VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

STUDIE PROVEDITELNOSTI INFORMAČNÍHO SYSTÉMU PRO NAKLÁDÁNÍ S UTAJOVANÝMI INFORMACEMI DO STUPNĚ UTAJENÍ DŮVĚRNÉ

Autor práce: Hana Huličová

Studijní obor: Bezpečnostně právní

Forma studia: Kombinované studium

Vedoucí práce: Mgr. Vladimír Čížek, DiS.

Katedra: Katedra právních oborů a bezpečnostních studií

2012

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47 b zákona č. 111/1998 Sb. v platném znění.

……..……

Vlastnoruční podpis autora bakalářské práce

Děkuji vedoucímu bakalářské práce Mgr. Vladimíru Čížkovi, DiS. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT V ČESKÉM JAZYCE

HULIČOVÁ, H. *Studie proveditelnosti informačního systému pro nakládání s utajovanými informacemi do stupně tajení důvěrné: bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2012. 100 s. Vedoucí bakalářské práce: Mgr. Vladimír Čížek, DiS.

Klíčová slova: informační systém, utajované informace, fyzická bezpečnost, personální bezpečnost, administrativní bezpečnost, průmyslová bezpečnost, bezpečnost IS, bezpečnostní dokumentace, analýza rizik.

Bakalářská práce se zabývá návrhem a vytvořením studie proveditelnosti informačního systému pro nakládání s utajovanými informacemi do stupně Důvěrné a následné aplikace vytčených podmínek a zásad na fiktivní firmě.

ABSTRAKT V ANGLICKÉM JAZYCE

HULIČOVÁ, H. A feasibility study of the information system for the handling of classified information to the instance classification confidential: Bachelor thesis. České Budějovice : The College of European and Regional Studies, o. p. s., 2012. 100 s. Supervisor: Mgr. Vladimír Čížek, DiS.

Key words: information system, classified information, physical security, personal security, administration security, industrial security, information system security, safety documentation, risk analysis.

This bachelor thesis deals with the design and a feasibility study of the information system for handling with classified information to the instance classification confidential and the subsequent application of the defined conditions and principles in a fictitious company.

OBSAH

ÚVOD

Ochrana utajovaných informací je specifickou oblastí bezpečnosti, která je pro ČR upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, a konkretizována prováděcími vyhláškami a bezpečnostními standardy, jejichž úkolem je zabránit vyzrazení nebo zneužití utajovaných informací a tím chránit zájmy České republiky.

Tématem bakalářské práce je vytvoření studie proveditelnosti informačního systému nakládajícího s utajovanými informacemi do stupně utajení Důvěrné, kde se propojují různé oblasti: informační a komunikační technologie, které jsou hlavními nositeli informací, s nimiž se setkáváme v dnešní době snad všude, dále charakterem samotných utajovaných informací, v našem případě stupně utajení Důvěrné, objekty, kde je s utajovanými informacemi nakládáno, lidmi, kteří s nimi pracují, lidmi, kteří zajišťují jejich provoz, bezpečnost a kontrolu a administrativními postupy, které popisují jednotlivé činnosti všech rolí informačního systému. Ochrana informací je v současnosti aktuálním tématem a stát ji považuje za velmi důležitou. Proto také stát zřídil Národní bezpečnostní úřad, který navrhuje potřebnou legislativu k ochraně utajovaných informací, projednává ji se státními organizacemi a předkládá ji k projednání a schválení parlamentem. Ministerstva za tímto účelem vydávají resortní prováděcí předpisy pro ochranu utajovaných informací. Legislativa k ochraně utajovaných informací stanovuje minimální standardy tj. minimální úroveň bezpečnostních opatření pro ochranu utajovaných informací, které mohou být vzorem pro privátní systémy organizací nebo fyzických osob, jež si uvědomují hodnotu svých informací, a jež si zároveň chtějí chránit svoje soukromí. Zde můžeme říci, že materiály pojednávající o informačním systému určeném k nakládání s utajovanými informacemi, mohou být velkým přínosem či vzorem pro kohokoliv, kdo má zájem eliminovat nebo snížit úroveň hrozeb směřujících vůči aktivům informačního systému. Informační systém určený k nakládání s utajovanými informacemi musí mít implementovány požadované bezpečnostní funkce a musí také poskytovat záruky, že bezpečnostní funkce správně fungují. Takový informační systém proto musí být certifikován Národním bezpečnostním úřadem před schválením provozu s utajovanými informacemi. Já sama jsem uživatel, který ví o možných rizicích moderních informačních technologií,

a snažím se je také v rámci svých možností eliminovat, nicméně nikdy jsem sama neřešila bezpečnost informací jako celek. Proto jsem se rozhodla svoje znalosti doplnit a zohlednit další rizikové faktory. Tímto by moje práce mohla být přínosem i pro další.

První část, nebo také „teoretická část“, je zaměřena na vymezení a definování obecných podmínek, které je nutno splnit, abychom vyhověli legislativním požadavkům pro vybudování informačního systému pro zpracování utajovaných informací. Výše jmenovaný zákon stanoví šest druhů zajištění ochrany utajovaných informací: 1) personální bezpečnost, 2) průmyslová bezpečnost, 3) administrativní bezpečnost, 4) fyzická bezpečnost, 5) bezpečnost informačních nebo komunikačních systémů a 6) kryptografickou ochranu. V průběhu studia jsem dospěla k závěru, že všechny výše uvedené podmínky, zásady a pravidla je možné rozdělit podle následujících kritérií:

- Právní determinace. Informační systém určený k nakládání s utajovanými informacemi je možné vybudovat pouze za dodržení platných právních předpisů vztahujících se k ochraně utajovaných informací a platných právních předpisů upravujících činnost organizace.
- Personální determinací rozumíme dostupnou kapacitu osob s odpovídající kvalifikací, splňující podmínky přístupu fyzické osoby k utajované informaci dané zákonem, a oprávněním k provozu informačního systému.
- Materiálně technická determinace je tvořena souhrnem materiálních zdrojů a fyzického prostředí, kterými se zajišťuje vlastní provoz a bezpečnost informačního systému. Jedná se o objekty, ve kterých bude informační systém provozován, jejich zabezpečení a vlastní informační systém, a z nich vycházející požadavky na informační a komunikační technologie.
- Systémově specifické determinace musí být zohledněny při promítání výše uvedených determinací do bezpečnostní dokumentace a do analýz.

Druhá část aplikuje všechny zmiňované podmínky, zásady a standardy uvedené v první části do prostředí fiktivní firmy. Je tvořena: 1) studií proveditelnosti, která se skládá z analýzy výchozího stavu informačního systému a jeho zabezpečení v organizaci a návrhu řešení a systémového projektu informačního systému IS-ATOBEZ-UI, a 2) bezpečnostní dokumentací.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem bakalářské práce je vymezit základní právní a věcné podmínky, jež jsou nutné pro vybudování informačního systému umožňujícího nakládat s utajovanými informacemi do stupně utajení Důvěrné a na základě získaných poznatků a podmínek uskutečnit aplikaci všech požadavků do prostředí fiktivní firmy.

Použitá metoda v první části vychází ze získání dat, studia dokumentů, jejich rozboru a vyhodnocení a postupů stanovených platnými právními předpisy, zejména zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dále prováděcími vyhláškami Národního bezpečnostního úřadu a bezpečnostními standardy. Výsledkem analýzy sebraných materiálů je v bakalářské práci takzvaná teoretická část, která interpretuje, formuluje a seskupuje danou problematiku do jednotlivých kapitol právní, personální, materiálně technické a systémové specifické determinace.

Obsahem druhé části jsou získané informace aplikovány na fiktivní firmu, tzn. vytvoření fiktivní firmy, která má potřeby vytvářet, zpracovávat a distribuovat utajované informace stupně utajení Vyhrazené a Důvěrné. Kapitola „Aplikace ve fiktivní firmě“ popisuje právní pozici vytvořené firmy, analyzuje potřeby a zdroje fiktivní firmy. Dále je práce zaměřena na samotnou tvorbu a schválení návrhu technického a bezpečnostního řešení informačního systému zpracovávajícího utajované informace, kde byly posouzeny a porovnány různé technické možnosti řešení s ohledem na potřeby firmy, s ohledem na bezpečnostní hodnocení tzv. Common Criteria[1], s ohledem na systémový projekt a bezpečnostní dokumentaci informačního systému pro zpracování utajovaných informací do stupně utajení Důvěrné, podle kterých by fiktivní firma postupovala při realizaci svého informačního systému. Jinými slovy: ve výše uvedené kapitole je vypracované bezpečnostní řešení. Při přípravě na vlastní bezpečnostní řešení jsem se seznámila se Studií proveditelnosti a systémovým projektem přebudování komunikační infrastruktury v objektech Vyšehradská a Na Děkance úřadu Ministerstva spravedlnosti. Tento projekt je však postaven na jiných

[1] *Common Criteria* [online]. Common Criteria Portal, 2011 [cit. 2011.09.23]. Dostupné z WWW: <http://www.commoncriteriaportal.org/>.

technologiích plynoucích z jejich potřeb a proto je rozepsán i v jiném technickém rozsahu zpracování. Projekt je majetkem Ministerstva spravedlnosti a není možné z něj cokoli citovat, byl však materiálem, který mně ukázal, jak by studie proveditelnosti měla vypadat a co by měla obsahovat (Projekt Ministerstva spravedlnosti není uveden mezi zdroji, protože z něj nebylo čerpáno.). Před zpracováním bezpečnostního řešení bylo nutno ověřit, zda funkcionalita informačního systému odpovídá požadavkům fiktivní firmy, a zda vybrané a následně použité informační technologie splní požadavky Národního bezpečnostního úřadu na provoz informačního systému zpracovávajícího utajované informace a zároveň bude kompatibilní s ostatními částmi řešení. Bakalářská práce v této části klade důraz především na vytvoření řešení počítačové bezpečnosti a řešení datového toku do informačního systému Státního úřadu pro jadernou bezpečnost. Proto bylo nejdříve potřebné zjistit, na jakých softwarových technologiích je možné počítačovou sít vybudovat, aby výsledné řešení prošlo certifikací, dále nastudovat a vyhodnotit jaké požadavky mají vybrané softwarové technologie na hardware. Výsledné poznatky sloužily jako zadání, podklad pro vyhledání a konfiguraci odpovídajícího hardware, který na jedné straně musel deklarovat podporu vybraným softwarovým technologiím, na straně druhé garantoval výkon, bezpečný provoz, do budoucna i rozšiřitelnost systému, obsahoval hardwarovou diagnostiku a energetickou úsporu a zároveň byl finančně dostupný pro vytvořenou firmu. Všemi výše uvedenými kroky jsme byli stále jen u softwarového a hardwarového řešení, u kterého bylo potřeba popsat bezpečné nastavení všech jeho funkcí a zohlednit všechny implementační a instalační požadavky, které na informační systém zpracovávající utajované informace klade zákon č. 412/2005 Sb. a prováděcí předpisy Národního bezpečnostního úřadu, jejichž popis a vysvětlení se nachází v právní, personální, materiálně technické a systémově specifické determinaci tj. v první obecné části bakalářské práce.

Bakalářské práce obsahuje v prvé části ucelený studijní materiál pro potřeby všech, kteří mají zájem informační systém pro zpracování utajovaných informací budovat a v části druhé pak vlastní projekt, studii proveditelnosti počítačové sítě pro zpracování utajovaných informací do stupně utajení Důvěrné, kde byly využity a aplikovány získané teoretické poznatky ve fiktivní firmě při vybudování reálného informačního systému se všemi svými prvky.

2 PRÁVNÍ DETERMINACE

Právní determinace definuje platnou legislativu (přehled je uveden v Seznamu platných právních předpisů) a vše, co tvůrce informačního systému pro zpracování utajovaných informací musí vzít v potaz, a za druhé třídí jednotlivé požadavky, podmínky a omezení do tematických celků.

Prvním krokem každé organizace – provozovatele budoucího informačního systému pro zpracování utajovaných informací dle § 139 zákona č. 412/2005 Sb., o ochraně utajovaných informací – je posouzení, zda informace, které bude organizace přijímat, zpracovávat, tvořit, vytvářet, evidovat atd. odpovídají nařízení vlády č. 522/2005 Sb. v aktuálním znění, kterým se stanoví sezam utajovaných informací. Tzn., že je nutné posoudit, zdali informace určené ke zpracování v informačním systému jsou uvedeny v přílohách nařízení vlády a jsou utajované, a jejich vyzrazení, zneužití by mohlo způsobit škodu, nebo újmu zájmům České republiky. Seznam utajovaných informací stanoví i stupeň nebo rozsah stupňů utajení informací. V případě, že organizace provozovatele budoucího informačního systému dojde k závěru, že posuzované informace spadají do seznamu utajovaných informací a jsou utajovanými informacemi určitého stupně, musí naplnit podmínky pro daný stupeň utajení stanovené v již zmiňovaném zákoně č. 412/2005 Sb.

2.1 Podmínky a zásady vycházející z obecně závazných právních předpisů

Informační systém, který nakládá s utajovanými informacemi, musí být certifikován Národním bezpečnostním úřadem ještě před zahájením zpracování utajovaných informací a jako takový musí splňovat podmínky, jež jsou stanoveny zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon upravuje zásady, podmínky a požadavky pro stanovení utajovaných informací, přístupu k nim, o jejich ochraně a ustanovuje činnosti a postupy pro práci s nimi. Od 1. ledna 2012 bude platit novela zákona upravující utajované informace a úpravy se budou týkat především: sloučení agend registrů, archivace, spisových služeb a žádostí fyzických a právnických osob o osvědčení.

Platné právní prostředí ČR pro oblast bezpečnosti komunikačních systémů a informačních systémů je uvedena v Seznamu platných právních předpisů a týká se: seznamu utajovaných informací, ochrany utajovaných informací, počítačové a komunikační bezpečnosti, fyzické bezpečnosti, personální bezpečnosti, administrativní bezpečnosti a organizačních opatření k zajištění bezpečnosti.

Z výše uvedeného vyplývá, že informační systém může zahájit ostrý provoz pouze po splnění celého komplexu vzájemně provázaných podmínek. Můžeme je rozdělit do 6 skupin. Zákon č. 412/2005 Sb. je nazývá „druhy zajištění ochrany utajovaných informací“:

- První skupinou jsou podmínky kladené na osoby, které budou přicházet do styku s utajovanými informacemi tzv. personální bezpečnost. Podmínky jsou kladeny na uživatele informačního systému, tak na správce informačního systému, ale i další osoby, které přicházejí do styku s utajovanými informacemi, mohou jimi být pracovníci spisovny, zaměstnanci zajišťující správu zabezpečených oblastí, údržbáři, uklízečky apod.
- Druhou skupinu tvoří fyzická bezpečnost, kterou se rozumí zajištění bezpečného prostředí pro umístění a provoz informačního systému určeného k nakládání s utajovanými informacemi tak, aby bylo znemožněno neoprávněné osobě získat přístup k provozovanému systému. Jedná se o zabezpečení vlastního objektu po technické stránce v oblasti budovy, místností, prostředků zabezpečení - uzamykání, mříží, trezorů, perimetrů, detekčního zařízení – čidel, kamer a jeho střežení za pomoci ostrahy, nebo elektronického zabezpečovacího systému – EZS, včetně kontroly vstupu osob do objektu skrze turnikety, nebo elektronické kontroly vstupu – EKV a protipožárního systému – EPS.
- Třetí skupinu představuje vlastní bezpečnost informačního systému. Zde se definuje, jaký informační systém bude provozován, kde bude instalován, za jakých podmínek bude provozován, jak je definována bezpečnostní politika, bezpečnostní provozní mód, způsob kryptografické ochrany a další.
- Čtvrtou skupinu tvoří nakládání s utajovanými dokumenty, např. s nosiči utajovaných informací a s informacemi vystupujícími z informačního systému. Jedná se o administrativní bezpečnost. Způsob ochrany dokumentů v listinné a nelistinné podobě, jejich označování, distribuce, ukládání, archivace a likvidace.

- Pátou skupinu tvoří legislativní požadavky kladené specificky na daný informační systém resp. na danou informační oblast. V tomto případě jsou to pravidla stanovená zákonem o mírovém využívání jaderné energie a ionizujícího záření - atomový zákon. Zde se definují podmínky specifikované daným zákonem.
- Šestá skupina je tvořena opatřeními odpovědné osoby organizace. Pojem „odpovědná osoba“ definuje zákon č. 412/2005 Sb., výkonem je zpravidla pověřen Bezpečnostní ředitel organizace a její součinnosti s příslušnými územními orgány pro řešení krizových situací. Zde se uvažuje s opatřeními v případě požáru, živelní pohromy jako vítr, povodeň, záplava, zemětřesení a teroristického útoku.

2.2 Platné technické normy a standardy

Legislativa pro ochranu utajovaných informací bez ohledu na to, zda jde o informace ČR, EU nebo NATO, stanovuje tzv. minimální rozsah bezpečnostních opatření, která musí být uplatněna ve stanovených případech. Tato legislativa zpravidla připouští nebo doporučuje, aby současně byly také zohledněny mezinárodní standardy a platné technické normy, někdy je označujeme jako standardy bezpečnosti informačních technologií. Obecně můžeme říci, že norma je psaný dokument, může být i nepsaný, ale to není náš případ, který vyžaduje určité chování, opatření nebo vlastnosti věcí, řešení, institucí, osob a situací a jako takové jsou závazné pro kohokoliv a to znamená, nejen pro tvůrce informačního systému pro zpracování utajovaných informací. Z těchto norem můžeme citovat určitě normy jako ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací nebo jednotlivá ISA, která jsou zárukou určité kvality a jakosti, v informatice se používají a jsou vyžadována ISO 9001, ISO 27001 a ISO 14001, do skupiny technických norem bude ale patřit i Nařízení vlády č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska elektromagnetické kompatibility, nebo Common Criteria pro jednotlivé technologie, či v informace používané jednotlivé standardy, i zde záleží na použitých technologiích jako ISA - Industry Standard Architecture, což je standard pro počítačovou sběrnice pro rozšiřující karty nebo v našem případě by to mohly být standardy z oblasti kryptografie jako DES - Data Encryption Standard pojednávající o kryptografické symetrické šifře, AES - Advanced Encryption Standard je v kryptografii označení pro symetrickou blokovou šifru, anebo nepsaný standard jako RSA, zkratka je vytvořena z prvních písmen autorů pana Rivesta, Shamira a Adlemana,

což je šifra s veřejným klíčem, jedná se o první algoritmus, který je vhodný jak pro podepisování, tak pro šifrování. Přehled některých technických norem a zásad je uveden v Seznamu technických norem a Seznamu zásad.

Při tvorbě informačního systému pro zpracování utajovaných informací organizace nesmí zapomenout na zapracování i svých vlastních interních normativních aktů organizace pro oblast bezpečnosti komunikačních systémů a informačních systémů, to je zpravidla politika bezpečnosti informací organizace, ale mohou to být i další instrukce, pokyny, metodiky a dílčí politiky. Příkladem mohou být „Směrnice organizace k ochraně utajovaných informací“ a „Spisový a skartační řád organizace“.

S přijetím zákona č. 412/2005 Sb. bylo nutno přijmout různé změny v mnoha dalších právních odvětvích, které se přímo problematikou utajovaných informací nezabývají, jednotlivé změny byly souborně vydány v zákoně č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon přináší změny v různých odvětvích práva, celkem je zde uvedeno 66 částí, kdy každá část je věnována změnám v jednom konkrétním zákoně, z těchto částí vybírám jednu změnu uvedenou v trestním zákoně - zákon č. 40/2009 Sb., zde najdeme v Hlavě IX: Trestné činy proti České republice, cizímu státu a mezinárodní organizaci, Díl 2 § 316 Vyzvědačství, § 317 Ohrožení utajované informace a § 318 Ohrožení utajované informace z nedbalosti. Aby nebylo vyloženo jinak, zákon č. 413/2005 nepřináší jen změny v sankcích, ale i změny týkající se provozu, činností, prací, postupů atd.

Veškerá zákonná ustanovení stanovující podmínky při ochraně utajovaných informací zpracovávaných, uchovávaných a přenášených pomocí informačních systémů by byla nedostatečná, kdyby nebyla zajištěna určitým sankčním mechanismem. V osmé části zákona č. 412/2005 Sb. v § 148 až 156 jsou taxativně vyjmenovány přestupky a správní delikty, kterých se mohou dopustit fyzické osoby, podnikající fyzické osoby, právnické osoby a podnikatelé v souvislosti s porušením pravidel a povinností v oblasti ochrany utajovaných informací. Zároveň jsou zde vyjmenovány pokuty za jednotlivé přestupky a správní delikty, které mohou být dle závažnosti protiprávního jednání ve výši od 50 000 Kč až do 5 000 000 Kč.

3 PERSONÁLNÍ DETERMINACE

Platné právní prostředí, popsané v části Právní determinace, upravuje i rámec týkající se osob, zejména zaměstnanců, jež v informačním systému mají pracovat, správců informačního systému, kteří zajišťují provozní funkcionalitu informačního systému a dále bezpečnostních správců, jejichž úkolem je zajišťovat bezpečný chod a bezpečnostní funkcionalitu informačního systému v organizaci sem řadíme i bezpečnostního správce informačního systému a bezpečnostního správce kryptografické ochrany.

Personální determinací se rozumí zajištění dostupné kapacity osob s odpovídající kvalifikací a oprávněním k užití a k zabezpečení provozu informačního systému. Přičemž oprávněné osoby musí splňovat podmínky seznamovat se s utajovanými informacemi příslušného stupně utajení a případně mít oprávnění k provozní obsluze kryptografického prostředku. Personální determinace ovlivňuje části: personální bezpečnosti, průmyslové bezpečnosti a administrativní bezpečnosti.

3.1 Personální bezpečnost

Personální bezpečnost stanovuje podmínky pro přístup fyzické osoby k utajované informaci. V této oblasti je nutné definovat[2]:

- Kdo bude mít přístup k utajovaným informacím, vyplývá většinou z funkce, pracovní nebo jiné činnosti zaměstnance nebo člena pracovního týmu. Fyzická osoba musí splňovat podmínky přístupu k utajované informaci. Zákon k personální bezpečnosti říká: „informaci nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti, je držitelem oznámení o splnění podmínek pro přístup k utajovaným informacím stupně utajení Vyhrazené nebo vlastní platné osvědčení fyzické osoby příslušného stupně utajení a zároveň je poučena výjimky stanovuje zákon“[3]. V našem případě rozlišujeme: bezpečnostního správce informačního systému, správce informačního systému, uživatele a vlastní kapitolu tvoří

[2] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7528-7531.
[3] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7528.

bezpečnostní správce kryptografické ochrany, správce kryptografického materiálu a pracovník kryptografické ochrany.

- Správcem kryptografické ochrany, správcem kryptografického materiálu a pracovník kryptografické ochrany může být osoba, která je držitelem osvědčení pro daný stupeň utajení a zároveň absolvovala zkoušku z odborné způsobilosti pracovníka kryptografické ochrany, ze způsobů a manipulací s kryptografickým materiálem, zkouška je skládána na Národním bezpečnostním úřadě, výsledkem zkoušky je hodnocení stupněm „prošel“ nebo „neprošel“, v případě úspěšného složení se daná osoba stává držitelem osvědčení o zvláštní odborné způsobilosti[4].
- Uživatelem, bezpečnostním správcem informačního systému, správcem informačního systému atd. mohou být pouze osoby, které splňují podmínky přístupu k utajované informaci jak bylo popsáno výše pro práci v daném stupni utajení a bezpečnostním provozním módu informačního systému, v kterém se s utajovanými informacemi nakládá, jež jsou proškoleni, jež se autorizovali jedinečným identifikátorem a postupovali stanoveným způsobem uvedeným v bezpečnostní dokumentaci a jež mají oprávnění provádět určité aktivity, přičemž všichni výše jmenovaní musí dodržovat postupy stanovené v bezpečnostní dokumentaci informačního systému, v případě, že tak nečiní, mohou být sankcionováni tzn., že mají odpovědnost za svoji činnost.
- Fyzická osoba:
  - pro stupeň utajení Vyhrazené nemusí mít prověrku Národního bezpečnostního úřadu, avšak musí splnit stanovené minimální požadavky, být řádně poučena zaměstnavatelem a poučení je potvrzeno písemně,
  - pro stupeň utajení Důvěrné musí být držitelem osvědčení fyzické osoby pro daný stupeň nebo stupně vyššího.
- Osvědčení vydává Národní bezpečností úřad, pokud žadatel splní všechny zákonné podmínky[5], kterými jsou:

[4] Česko. Vyhláška č. 524 ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9994-9995.

[5] Česko. Vyhláška č. 527 ze dne 14. prosince 2005 o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10045.

- žádost o vydání osvědčení fyzické osoby,
- dotazník fyzické osoby v elektronické podobě na technickém nosiči a listinné podobě, přičemž listinná podoba musí odpovídat elektronické podobě vyjma podpisu,
- doklad o poučení odpovědnou osobou,
- oznámení o splnění podmínek pro přístup fyzické soby k utajované informaci,
- prohlášení fyzické osoby o způsobilosti k právním úkonům,
- prohlášení k osobní způsobilosti,
- doklady dokazující údaje uvedené v dotazníku - rodný list, oddací list, doklad o nejvyšším dosaženém vzdělání, potvrzení o studiu v zahraničí, rozhodnutí orgánů činných v trestním řízení, potvrzení o příjmech od zaměstnavatele, doklady o právech třetích osob zatěžující žadatele, rozhodnutí soudu či jiného státního orgánu k nějakému výkonu.

- Fyzická osoba žádající o prověrku musí mimo výše uvedeného splňovat i obecné podmínky[6]:
  - je státním občanem České republiky, nebo státním občanem členského státu Evropské unie, nebo Organizace Severoatlantické smlouvy,
  - je způsobilá k právním úkonům v plném rozsahu,
  - je starší 18 let,
  - je bezúhonná, tj. nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu vztahující se k ochraně utajovaných informací,
  - je osobnostně způsobilá, tzn., že netrpí poruchou či jinými obtížemi, u vyšších stupňů je dokládáno odborným posudkem a
  - je bezpečnostně spolehlivá.

3.1.1 Personální bezpečnost ve fyzickém prostředí

Jak z názvu kapitoly vyplývá, je nutné při budování informačního systému pro zpracování utajovaných informací zajistit personální bezpečnost při ochraně objektu a samotného technického vybavení informačního systému a to především v oblasti kontroly vstupu a výstupu oprávněných osob do zabezpečené oblasti, ale i vjezdu

[6] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7528-7531.

a výjezdu vozidel do objektu, s tímto bodem souvisí zajištění režimových opatření, které jsou formálně upraveny v Provozním řádu, a jejich ověřování a vyhodnocování možných rizik v oblastech:

- stanovení seznamu oprávněných osob, dopravních prostředků, které mohou do objektu vstoupit, vjet,
- stanovení seznamu oprávněných osob, které mohou vstoupit do zabezpečené oblasti a jednací oblasti,
- manipulace s klíči a identifikačními prostředky a technickými prostředky, jejich označení, evidence, přidělení, odevzdání, úschova a uložení duplikátů,
- vedení provozního deníku a knihy návštěv,
- kontrola oprávnění pro vstup a vjezd ostrahou,
    - Ostraha objektu, ve kterém se nachází zabezpečená oblast kategorie Důvěrné, je typu 2[7] nebo vyšší. Ostrahu typu 2 zabezpečují zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníci ozbrojených sil nebo ozbrojených sboru anebo zaměstnanci bezpečnostní ochranné služby.
    - Ostraha technického zařízení obsahující utajované informace stupně utajení „Důvěrné“ se zpravidla nevztahuje na běžné informační systémy, je definována podle typu 4[8] nebo vyšší dle § 5 odst. 5 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, což znamená, že je zajištěna příslušníky ozbrojených sil nebo ozbrojených sborů a je vykonávána způsobem nepravidelných obchůzek, je zajištěna neustále nejméně jednou osobou, jež zajistí rychlý zásah, je-li ochrana utajované informace narušena a jež je určená pro výkon ostrahy.
- kontrola vynášených věcí a utajovaných informací,
- stanovení podmínek a způsobu kontroly pohybu osob v objektu,
- bezpečnostní, požární a návštěvní řád aj.

[7] Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 18 Přílohy č. 1.

[8] Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 18 Přílohy č. 1.

3.2 Průmyslová bezpečnost

Jestliže podnikatel, právnická osoba ke své práci nezbytně potřebuje přístup k utajované informaci, musí být držitelem platného osvědčení podnikatele pro daný stupeň utajení. K získání osvědčení žadatel musí předložit podle § 96 odst. 2 písmena c) zákona č. 412/2005 Sb.[9]:

1. úplný výpis z obchodního rejstříku a doklady o změnách, jež se zapisují do obchodního rejstříku,
2. výpis z evidence emise, nebo čestné prohlášení podnikatele se seznamem osob, mající vyšší jak 10 procentní podíl v podniku,
3. výpis z katastru nemovitostí a smlouvy o pronájmu prostor, budov a pozemků,
4. roční účetní uzávěrky a daňová přiznání - 5 let zpětně, včetně písemného ověření auditora týkající se příslušných uzávěrek,
5. potvrzení finančního úřadu o stavu osobních účtů a výpis z účtu vlastníka,
6. potvrzení správy sociálního zabezpečení a pojišťoven, že podnikatel nemá nedoplatky včetně penále,
7. podepsaný přehled závazků z podnikatelské činnosti, kde splatnost přesáhla 180 dnů s písemným vyjádřením o důvodech nezaplacení a potvrzení bank, či jiných věřitelů o plnění svých povinností,
8. čestné prohlášení s přehledem cenných papírů a vkladů do společností s ručením omezeným, družstev, obchodních společností či komanditních společností,
9. zdůvodnění nutnosti přístupu,
10. vyplněný dotazník
11. ovládací smlouvu nebo písemný doklad o vztazích 5 let zpětně.

Podnikatel, fyzická osoba, tzn. živnostník podle výše uvedeného zákona, musí předložit ve většině stejné písemnosti, nepředkládá písemnost z bodu 1, bod 2 je nahrazen bodem 13 a body 3 až 10 jsou stejné, k ověření splnění podmínek, živnostník dále předkládá[10]:

[9] Česko. Vyhláška č. 526 ze dne 14. prosince 2005 o stanovení používaných v průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10015-10016.

[10] Česko. Vyhláška č. 526 ze dne 14. prosince 2005 o stanovení používaných v průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání

12. živnostenské listy, koncesní listiny, živnostenská oprávnění, nebo osobou provozující zemědělskou výrobu včetně výpisu z evidence,
13. úplný výpis z obchodního rejstříku, je-li tam živnostník zapsán,
14. potvrzení ze živnostenského úřadu, že živnostníkovi nebyla pozastavena či přerušena živnost, že nezaniklo živnostenské oprávnění, nebo že není na živnostníka vyhlášen konkurz, nebo že neexistují překážky v provozování živnosti, nebo že neexistuje záznam o pokutách a sankcích uložených živnostníkovi souvislosti s podnikáním.

Podnikatel - zahraniční osoba dokládá stejné písemnosti jako české subjekty, s tím rozdílem, že body 1, 2, 10 a 11 dokládá formou obdobných dokladů z evidencí podle země původu.

Podnikatel žádající vydání osvědčení podnikatele musí splňovat i obecné podmínky[11]:

- podnik je ekonomicky stabilní, tzn., že podnik nebyl zrušen, není v konkurzu, není ochranné lhůtě, není na něj soudem povoleno nucené vyrovnání, není v nucené správě, nemá nedoplatek na pojistném a dani, plní všechny finanční povinnosti a není na jeho majetek uvalena exekuce,
- podnik je bezpečnostně spolehlivý, tzn., že podnik neuvádí nepravdivé informace, či nezamlžuje informace o skutečném stavu podniku, nenavazuje kapitálové a finanční vztahy s fyzickými a právnickými osobami cizí moci, jež by mohli jednat proti zájmu České republiky, je personálně stabilní, to se týká i statutárního orgánu, kontrolního orgánu a prokuristů, je-li podnik akciovou společnosti musí být jeho akcie psané na jméno, dále podnik v minulosti nikdy neporušil svoje povinnosti při ochraně utajovaných skutečností, žádný ze společníků podniku nebyl v minulosti pravomocně odsouzen za úmyslný čin a jednatelé podniku úmyslně neporušují právní předpisy, čímž by mohla vzniknout státu škoda,
- podnik je schopen zabezpečit ochranu utajovaných informací,

osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10016.

[11] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7528-7531-7532.

- odpovědné osoby podnikatele, prokuristé jsou držiteli platného osvědčení fyzické osoby nejméně pro takový stupeň, nebo jsou držiteli oznámení, pokud se žádá pouze pro režim práce ve stupni utajení Vyhrazené.

  Všechny výpisy, potvrzení a prohlášení nesmí být starší 60 dnů.

3.3 Administrativní bezpečnost

Administrativní bezpečnost se zjednodušeně zabývá: tvorbou, příjmem, evidencí, zpracováním, odesíláním, přepravou, přenášením, ukládáním, řízením, skartací, archivací a nakládáním s utajovanými informacemi včetně přístupů do registrů. Její podmínky jsou odvislé od stupně utajení a souvisí[12]:

- S označováním dokumentů v listinné a nelistinné formě:
  - Na každém utajovaném dokumentu musí být vyznačen stupen utajení podle § 5 vyhlášky č. 529/2005 Sb.
  - Utajovaný dokument musí být prokazatelným způsobem zaevidován podle § 7 vyhlášky č. 529/2005 Sb., musí být vyznačeno číslo jednací utajovaného dokumentu nebo jiné evidenční označení a další náležitosti.
  - Požadavky administrativní bezpečnosti kladené na zpracování a přenos utajovaných informací v informačním systému resp. kryptografických prostředcích stanovuje dokumentace certifikovaného informačního systému resp. kryptografického prostředku, která vychází z § 23 odstavce 3 zákona č. 412/2005 Sb. U dokumentů v tištěné podobě, které tvoří výstup z informačního systému, se musí zajistit:
    - název, původce informace, stupeň utajení musí být uveden vždy velkými písmeny, a to může být provedeno ručně, nebo razítkem, číslo jednací, které je tvořeno: zkratkou stupně utajení, pořadovým číslem z jednacího protokolu, lomítkem a rokem, vyhláška Národního bezpečnostního úřadu č. 529/2005 Sb. připouští uvedení dalších údajů za spojovníkem nebo jiné evidenční označení a datum vzniku utajovaného dokumentu, vyžaduje-li to charakter utajované informace je původce povinen vyznačit i dobu, po kterou bude tento dokument utajován a to za nápisem „UTAJOVAT DO“, po uplynutí této doby, utajení zaniká. Vyznačení

[12] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7532-7534.

stupně musí být zachováno po celou dobu trvání utajení. Utajovaný dokument jako takový je pak vedena v jednacím protokolu nebo v další administrativní pomůcce podle § 7 vyhlášky č. 529/2005 Sb. U označování rozlišujeme[13]:

- označování serverů, komunikačních technologií a stanic stanovuje dokumentace certifikovaného informačního systému resp. schváleného komunikačního systému,
- nosiče utajovaných informací například pevné disky, disket, CD/DVD média, flash - disky a jiná média se eviduji jako dokumenty v nelistinné formě dle § 5 odstavec 4 vyhlášky č. 529/2005 Sb.,
- označování bezpečnostní dokumentace.

- S administrativními pomůckami. Za administrativní pomůcky vyhláška Národního bezpečnostního úřadu č. 529/2005 Sb. považuje: jednací protokol, pomocný jednací protokol, manipulační knihu, doručovací knihu, zápůjční knihu, kontrolní list utajovaných informací a sběrný arch, který slouží k většímu počtu utajovaných informací k jedné věci, přičemž všechny listy pomůcek musí být číslovány, vyjma kontrolního listu a sběrného archu i řádně upraveny - autentizovány listy očíslovány a prošity a na vrchní stránce musí být uvedeno razítko, doložka o počtu listů, podpis bezpečnostního ředitele nebo osoby pověřené k podpisu odpovědnou osobou a datum přidělení pomůcky do užívání. Osoba odpovědná nesmí být zároveň osobou, jež danou pomůcku vede. Administrativní pomůcky mohou být vedeny i elektronicky, musí však obsahovat všechny předepsané položky a systém, v kterém je tato pomůcka vedena musí být zabezpečen proti neoprávněnému zásahu a přístupu osob bez oprávnění. Všechny administrativní pomůcky se evidují a ukládají takovým způsobem, aby nedošlo k jejich ztrátě, či poškození, mohou se vyřadit až tehdy, jestliže všechny utajované dokumenty v nich evidované a zaznamenané jsou vyřazeny.
- Se skartačním řízením a archivací. Skartace je postup, při kterém se dokumenty vyřazují, jsou to dokumenty, u kterých uplynula skartační doba, a pro původce jsou již nepotřebné. Utajovaný dokument v průběhu jeho skartační lhůty je možné zapůjčit fyzickým a právnickým osobám, nebo podnikající fyzické osobě, která je ve

[13] Česko. Vyhláška č. 529 ze dne 15. prosince 2005 o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10117-10124.

služebním poměru, či členském vztahu k orgánu státu. Za skartaci odpovídá původce nebo jeho právní nástupce[14].

- S opisem. Opis u klasifikované informace Důvěrné může být proveden pouze s písemným souhlasem nadřízené osoby.
- Se změnou klasifikace. Stupeň utajení se mění nebo ruší při zjištění, že pominul důvod pro utajení, nebo že důvody již neodpovídají danému stupni, změna stupně se musí vyznačit a původce musí písemně informovat všechny adresáty o změně klasifikace, adresáti po obdržení oznámení od původce změnu na utajované informaci vyznačí. Původce má povinnost utajované informace jednou za 5 let prověřit, zdali důvod utajení u dané informace trvá. Zanikl-li původce, provede změny právní nástupce, nesplňuje-li právní nástupce podmínky, pak je provede Národní bezpečnostní úřad. Změna se provede přeškrtnutím původního stupně, přičemž původní stupeň musí být čitelný a nový se vyznačí.
- S organizačními opatřeními, pod tímto bodem se nalézá: údržba technologií, řízení celého životního cyklu implementace, provozu, rozvoje nebo rušení provozu, plánování kapacit, instalace v souladu s dokumentacemi, servis, zálohování, obnova funkčnosti, zajištění bezpečného provozu a rozvoje systému, školení všech rolí vystupujících v systému, vyšetření a hlášení bezpečnostních incidentů, provádění kontrol systému a vyhodnocení.
- S přípravou zásilky k přepravě a přenosu. Utajované dokumenty je možné přepravovat a přenášet pouze v přenosných schránkách nebo v uzavřeném pevném obalu, ale také v aktovkách, kufřících, kufrech, bezpečnostních schránkách, nebo kurýrních vacích, které jsou zajištěny proti neoprávněné manipulaci s jejím obsahem a to zámkem, pečetí nebo plombou. Na zásilce se uvádí název státu, právnické osoby, jméno a příjmení fyzické osoby a stupeň utajení a zároveň je označena větou: "V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!"[15].

[14] Česko. Zákon č. 499 ze dne 30. června 2004 o archivnictví a o spisové službě a o změně některých zákonů. In *Sbírka zákonů, Česká republika*. 2004, částka 173, s. 9743-9753,9758,9761-9763.
[15] Česko. Vyhláška č. 55 ze dne 14. února 2008, kterou se mění vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2008, částka 16, s. 842 § 2.

- S přepravou. Dle § 22 vyhlášky č. 529/2005, o administrativní bezpečnosti a o registrech utajovaných informací může držitel poštovní licence[16] přepravovat zásilku s utajovanými informacemi stupně Důvěrné, jeli místo zásilky v České republice. Držitel poštovní licence písemně potvrzuje převzetí zásilky a adresát potvrzuje příjem zásilky. Odesílatel obdrží písemné potvrzení o doručení zásilky. Je-li zásilka s utajovanými informacemi stupně Důvěrné a vyšší poslána kurýrem, musí se kurýr prokázat platným osvědčením fyzické osoby pro příslušný stupeň utajení, u stupně utajení Tajné a Přísně tajné je zásilka kurýrem přepravována v doprovodu nejméně jedné osoby. Samotná zásilka je umístěna v přenosné schránce a i zde odesílatel dostává stvrzenku o převzetí utajované zásilky adresátem, tato stvrzenka se stává součástí výtisku utajovaného dokumentu. Držitel poštovní licence i kurýr odpovídá státu za poškození a úbytek obsahu zásilky. Kryptografický materiál se přepravuje jako kryptografická zásilka výhradně prostřednictvím kurýra kryptografického materiálu a její odesílání je upraveno vyhláškou č. 524/2005, o zajištění kryptografické ochrany utajovaných informací.
- S přenášením. Dle § 23 stejné vyhlášky je možné utajovaný dokument přenášet v obálce, pevném obalu a za splnění stejných podmínek jako v bodě s přepravou. Zásilku obsahující dokument Tajné a Přísně tajné je možné přenášet pouze s písemným souhlasem odpovědné osoby, nebo bezpečnostního ředitele, tento souhlas musí mít osoba přenášející zásilku u sebe a je součástí utajovaného dokumentu.
- S registry, to jsou centrální evidenční spisovny, kde je seznam, soupis, rejstřík utajovaných informací, členíme je podle mezinárodního styku mezi Českou republikou a Organizací Severoatlantické smlouvy, Evropskou unií a ostatními subjekty cizí moci. Přístup do registru je na základě písemné žádosti.

[16] Česko. Zákon č. 29 ze dne 18. ledna 2000 o poštovních službách a o změně některých zákonů (zákon o poštovních službách). In *Sbírka zákonů, Česká republika*. 2000, částka 10, s. 340 v § 19.

4 MATERIÁLNĚ TECHNICKÁ DETERMINACE

Platné právní prostředí ČR popsané v části „právní determinace“ upravuje i pravidla pro rámec materiálně technické determinace, jejímž cílem je blíže specifikovat technické a materiální podmínky a zdroje pro budování informačního systému. Materiální zdroje obecně umožňují zajistit bezpečné fyzické prostředí a potřebná aktiva vlastního informačního resp. komunikačního systému. Bezpečnostní požadavky v této oblasti je možné rozdělit na dvě části:

- podmínky v oblasti fyzické bezpečnosti a
- bezpečnostní požadavky na informační a komunikační technologie.

4.1 Fyzická bezpečnost

Fyzickým prostředím je objekt, budova nebo nějaký ohraničený prostor, ve kterých se nachází zabezpečená oblast anebo jednací oblast. Při výběru objektu je vhodné zvažovat vnější bezpečnostní prostředí - širší okolí, protože případné hrozby z vnějšího prostředí musí být pokryty protiopatřeními. Zabezpečená oblast anebo jednací oblast jsou prostorem, místem, kde je možné utajované informace uchovávat například v trezoru, uzamykatelné skříni atd., projednávat a zpracovávat. Zabezpečené oblasti se podle možnosti přístupu zařazují do tříd: třída I, zde vstupem do oblasti dochází k seznámení s utajovanými informacemi a třída II, kde vstupem do oblasti nedochází k seznámení. Samotné zabezpečené oblasti rozdělujeme podle stavební konstrukce, to se týká stěn, podlah a stropů do pěti typů[17]:

- Typ 4 musí mít zděnou konstrukci o tloušťce více jak 300 mm, tzn. cihly, vápencové bloky, pórobetonové tvárnice, nebo z vyztuženého betonu o tloušťce větší jak 150 mm. Bodové ohodnocení mechanických zábranných prostředků musí splňovat hodnotu SS3 = 4. Okna, dveře a další uzávěry musí splňovat bezpečnostní třídu 4 nebo 5 podle ČSN P ENV 1627, přičemž musí být odolná proti násilnému vniknutí.
- Typ 3 musí mít zděnou konstrukci o tloušťce větší jak 150 mm, nebo může být z vyztuženého betonu o tloušťce větší jak 100 mm. Bodové ohodnocení

[17] Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 11-13 Přílohy č. 1.

mechanických zábranných prostředků musí splňovat hodnotu SS3=3. Okna, dveře a další uzávěry musí vyhovět bezpečnostním požadavkům třídy 3 téže normy.

- Typ 2 musí mít zděnou konstrukci o tloušťce 100 - 150 mm, nebo může být z vyztuženého betonu o tloušťce větší jak 100 mm. Bodové ohodnocení mechanických zábranných prostředků musí splňovat minimálně SS3=2, okna dveře musí splňovat požadavky bezpečnostní třídy 2 podle téže normy a zároveň musí být umístěna alespoň 5,5 m nad terénem a nesmí se k nim proniknout ze střechy, hromosvodů, okapů, parapetů, či jiných staveb.
- Typ 1 je lehké stavební konstrukce jako sádrokarton, lehké zděné konstrukce, dřevotříska, plastické hmoty, vlnitý, nebo jinak profilovaný plech, nebo sklo opatřené certifikovanou bezpečnostní fólií, průlezové otvory musí být zabezpečeny mechanickými zábrannými prostředky, které odpovídají hodnotě SS92 = 3, nebo jsou chráněny certifikovanými zařízeními elektronické signalizace, anebo nemusí být zabezpečeny průlezové otvory atd., pokud jsou umístěny alespoň 5,5 m nad terénem a nesmí se k nim proniknout ze střechy, hromosvodů, okapů, parapetů, či jiných staveb.
- Typ 0 je lehké stavební konstrukce, průlezové otvory nemusí být zajištěny mechanickými zábrannými prostředky, ale musí umožňovat kontrolu osob a vozidel.

Aby tento odstavec byl úplný, tak je nutné ještě doplnit, že obdobným způsobem jsou charakterizovány a rozděleny na typy: úschovné objekty typu 4, 3, 2 a 1, hranice objektu typu 4, 3, 2, 1 a 0, systém kontroly vstupu do zabezpečené oblasti typu 4, 3, 2 a 1, ostraha typu 5, 4, 3, 2 a 1, systém elektrické zabezpečovací signalizace typu 4, 3, 2 a 1, zámky, uzamykací systémy, fyzické bariéry atd.

Jednotlivé technické prostředky zajišťující fyzickou bezpečnost mají certifikáty a přiřazené bodové ohodnocení. Příloha vyhlášky č. 528/2005 Sb. stanovuje způsob použití opatření fyzické bezpečnosti a strukturu „tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené a jednací oblasti“. Dále stanovuje „tabulky bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti“, totéž pro „jednací oblast“, pro kategorie dle stupně utajení a v závislosti na míře rizika.

Aktiva informačního systému musí být umístěna do prostoru, kde je zajištěna fyzická ochrana. V rámci certifikace informačního systému se stanovuje, jaké části

informačního systému musí být umístěny v zabezpečené oblasti nebo objektu, přičemž aktiva v zabezpečeném objektu musí být umístěna tak, aby nebylo možné samotné utajované informace nebo informace k identifikaci a autentizaci do informačního systému odposlouchávat a odezírat[18]. Zákon č. 412/ 2005 Sb. stanovuje mimo výše uvedeného i podmínky fyzické bezpečnosti a stanovuje technické prostředky, které mají zajistit zabezpečení oblastí proti úniku utajovaných informací. Po technické stránce hovoříme:

- o mechanických, nebo zábranných prostředcích například: zámky, dveře, mříže, fólie, rámy, skla aj.,
- o elektronickém zámkovém zařízení, které řeší elektronickou identifikaci a autentizaci,
- o zabezpečovací signalizaci zajišťující oblast požární, tísňovou a detekci látek například čidla, hlásiče, alarmy,
- o televizních a kamerových systémech a detekci pohybu,
- o zařízení na fyzické ničení nosičů informací - různé skartovače aj.,
- o zařízení proti aktivnímu a pasivnímu odposlechu utajovaných informací.

4.1.1 Fyzická bezpečnost do stupně Důvěrné

- Konstrukce objektu: určení typu zabezpečené oblasti je dána nejméně odolným prvkem její hranice, takže u nižších typů zabezpečených oblastí 0 a 1 je nutné bezpečnost doplnit vyšším typem mechanických zabraných prostředků.
- Mechanické zábranné prostředky:
  - v kategorii Vyhrazené je možné použít mechanické zábranné prostředky certifikované i necertifikované,
  - v kategorii Důvěrné je nutné použít certifikované mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace[19].
- Zajištění, aby v těchto prostorech, nedošlo k nedovolenému použití technických prostředků určených k získání informací – například dohled kamerovým systémem.
- Zajištění způsobu ukládání utajovaných informací v závislosti na stupni.

[18] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7534-7536.
[19] Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 12 Přílohy č. 1.

- Zajištění projektu fyzické bezpečnosti a její dokumentace, jejíž součástí je popis zabezpečení objektu, oblasti včetně kategorií a tříd, vymezení hranic a vstupů do těchto objektů a oblastí, popis použitých technických prostředků a způsob použití, opatření, provozní řád objektu, oblasti, seznam odpovědných osob, informace o provozovateli objektu, krizový plán pro mimořádné situace, hrozby a rizika.

4.2 Informační a komunikační technologie - ICT

Obecně informační a komunikační technologie se zabývají veškerými možnými technologiemi pro komunikaci a práci s informacemi. Bezpečnost informačních a komunikačních systémů uplatňuje opatření z těchto částí[20]:počítačové a komunikační bezpečnosti, kryptografické ochrany, ochrany proti úniku utajovaných informací prostřednictvím kompromitujícího vyřazování, administrativní bezpečnost a organizační opatření, personální bezpečnost, fyzické bezpečnosti informačního systému.

4.2.1 Informační systém a jeho požadavky

Pod pojmem informační systém, ve kterém jsou zpracovávány utajované informace, je nutné si představit soubor lidí, technologické prostředky tzn. jeden, nebo více počítačů, včetně periferních zařízení, které splňují technické podmínky pro práci v daném stupni utajení, dále programové vybavení a metody, jež zajišťují sběr, tvorbu, přenos, zpracování, uchovávání, ukládání a zobrazení utajovaných informací, ale i bezpečnostní dokumentace, metodiky, směrnice atd. Vše o informačním systému, o jeho částech, bezpečnostní politice, konfiguraci, nastavení a provozu musí být zohledněno v bezpečnostní dokumentaci informačního systému, která musí být zpracována pro každý informační systém pro zpracování utajovaných informací, proto této problematice je věnována vlastní samostatná kapitola číslo Bezpečnostní dokumentace informačního systému. Požadavky na formulaci bezpečnostní politiky informačního systému můžeme rozdělit na minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti pro daný stupeň utajení, na systémově závislé bezpečnostní

[20] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9979.

požadavky a na bezpečnostní požadavky bezpečnostní politiky nadřízeného orgánu, pokud byla zpracována[21]:

- Informační systém musí být vždy certifikován Národním bezpečnostním úřadem. Informační systém je řešen a provozován samostatně a je charakterizován: stupněm utajení, potřebami organizace, provozem, rozsahem zpracovávaných dokumentů a jejich počtem, reakcí tzn. odezvou na daný dokument, prostředky a možnostmi organizace a uživateli.
- Informační systém je provozován v odpovídajícím bezpečnostním provozním módu.
- Informační systém musí zajistit dostupnost požadované utajované informace na daném místě, v požadované formě a v časovém rozmezí, včetně stanovení minimálního rozsahu požadované funkčnosti, jež má být zaručena v době výpadku.
- V informačním systému mohou být použity pouze HW a SW komponenty odpovídající bezpečnostní dokumentaci informačního systému schválené Národním bezpečnostním úřadem, které jsou chráněny proti škodlivému kódu, které u stupně utajení Důvěrné a vyšší musí být zároveň zabezpečeny proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování. Národní bezpečnostní úřad hodnotí způsobilost daných komponent tak, že naměřené hodnoty vyzařování porovná s bezpečnostními standardy. V oblasti ochrany utajovaných informací před kompromitujícím vyzařováním se může použít i certifikovaná stínící komora. Tato část se tedy týká: serverů, počítačů, mobilních zařízení, psacího stroje s pamětí, šifrovacího zařízení, zálohovacího zařízení, UPS, aktivních prvků, tiskáren, kopírek, scannerů, čteček, skartovacích strojů i kabelů atd.
- U informačního systému musí být zajištěna bezpečnost nosičů utajovaných informací, jež jsou evidovány a odpovídají bezpečnostnímu provoznímu módu, evidovány jsou i nosiče utajovaných informací, jež jsou zabudované uvnitř PC a mobilních zařízení např. HDD, s tímto bodem pak souvisí i speciální zařízení fyzického ničení nosičů informací, zde se odlišuje typ nosičů papír, film s informací v originální velikosti, diskety, CD apod. od nosičů mikrofilm, čipové karty a obdobné nosiče, kdy Vyhláška Národního bezpečnostního úřadu č. 523/2005 v § 15 odst. 7 stanovuje: „zničení nosiče utajovaných informací informačního

[21] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9980-9986.

systému musí být provedeno tak, aby se znemožnilo utajovanou informaci z něho opětovně získat.“.

- Informační systém musí mít vypracovanou analýzu rizik, která stanoví seznam hrozeb s odpovídajícím rizikem, jež ohrožují aktiva informačního systému. Posuzují se zejména hrozby tedy zranitelná místa v systému, jež mají vliv na funkčnost a bezpečnost informačního systému a dle míry rizika se provedou vhodná protiopatření. U mobilních a přenosných informačního systému se posuzují i rizika spojená s dopravním prostředkem. Některé funkce informačního systému mohou být v odůvodněných případech nahrazeny použitím jiných prostředků personálních, administrativních či fyzických, musí být však plně realizována kvalita a úroveň bezpečnostní funkce.

4.2.2 Požadavky informační bezpečnosti do stupně Důvěrné

Minimální bezpečnostní požadavky z oblasti počítačové bezpečnosti pro stupně utajení Důvěrné a vyšší, v závislosti na zvoleném bezpečnostním provozním módu IS[22]:

- zajištění jednoznačné identifikace a autentizace uživatele, bezpečnostního správce, správce informačního systému a správce kryptografické ochrany, který je řešen těmito základními metodami a z nich kombinacemi:
  - toho, co uživatel zná například: PIN, heslo,
  - toho, co uživatel má například: hardwarové technické prostředky patří sem: hardwarový klíč, SmartCard, privátní klíč,
  - jaký uživatel je tj. jeho biometrické vlastnosti jako otisk prstu a
  - podle toho, co uživatel umí například nějaký náhodně vygenerovaný dotaz,
- zajištění bezpečnosti funkcí informačního systému, jež zajišťují identifikaci,
- zajištění povinného anebo volitelného řízení přístupu k objektům tj. rozlišení přístupových práv pro různé role: uživatel, bezpečnostní správce, správce informačního systému a případně správce kryptografického prostředku,
- zajištění nepřetržitého zaznamenávaní událostí například přes auditní záznamy,
- zajištění možnosti zkoumání auditních záznamů tj. stanovení odpovědnosti, kdo bude auditní záznamy vyhodnocovat,

[22] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9980-9986.

- zajištění ošetření paměťových objektů, zajištění obsahu paměťových objektu a jejich bezpečnost – například šifrováním,
- zavedení, nastavení a provoz bezpečnostních mechanismů,
- zajištění fyzické bezpečnosti informačního systému tzn. definování, kde mají jednotlivé komponenty informačního systému být umístěny v jaké bezpečnostní oblasti a jak tyto oblasti mají vypadat,
- zajištění personální bezpečnosti informačního systému tj. školení uživatelů, správců,
- zajištění administrativní bezpečnosti informačního systému,
- nastavení bezpečnostního provozního módu, zákon definuje provozní mód vyhrazený, s nejvyšší úrovní, nebo víceúrovňový,
- zajištění bezpečnosti v prostředí počítačových síti je rozepsáno v kapitole 4.2.4 Počítačové sítě,
- zajištění důvěrnosti informací, tj. zajištění informace takovým způsobem, aby bylo znemožněno její odhalení, zničení či pozměnění neoprávněnou osobou,
- zajištění dostupnosti utajované informace a informačního systému v určitém čase na určitém místě,
- pokrytí hrozeb identifikovaných analýzou rizik, u nichž rizika překračují provozovatelem akceptovatelnou úroveň - stanovení hrozeb, definování rizik a nasazení vhodného protiopatření,
- zajištění možnosti náhrady jiného bezpečnostního prostředku nebo skupiny mechanismů pro určitou funkci,
- zajištění požadavků na mobilní a přenosné informační systémy, to se týká například notebooků,
- zajistit otestování komponentů proti kompromitujícímu vyzařování, které je požadováno od stupně Důvěrné a výše, provádí Národní bezpečnostní úřad,
- zajistit bezpečnost nosičů informací, tj. evidenci, určení, uchování, stanovení stupně utajení, mazání, nebo ničení nosičů,
- zajistit požadavky na přístup k utajované informaci za pomocí autorizace a osvědčení osob,
- stanovení odpovědnosti pro uživatele, bezpečnostního správce, správce informačního systému a správce kryptografického prostředku a stanovení pracovních postupu a požadavků na jednotlivé role informačního systému,

- zajištění správy informačního systému, zavedením role správce informačního systému a definováním rozsahu jeho činnosti,
- zajištění testování a kontroly bezpečnosti informačního systému, to se týká testování před vydáním certifikátů, nutnost stanovení různých testů, jež se předkládají Národnímu bezpečnostnímu úřadu,
- zajištění instalace informačního systému oprávněnými osobami,
- zajištění bezpečnosti provozu informačního systému, to znamená zajištění prověřování a soustavné kontrolování informačního systému, nastavení antivirové ochrany proti škodlivému kódu, zálohování, UPS, údržba, servis, vyhodnocování auditních záznamů, logů, řešení krizových situací, likvidace následků, nouzový provoz a obnova informačního systému.

4.2.3 Komunikační systém a jeho požadavky

Obecně komunikační systémy zajišťují oboustrannou, nebo jednostrannou komunikaci jednotlivců, nebo skupin. Komunikační systém zajišťuje přenos utajovaných informací mezi koncovými zařízeními respektive jejich uživateli. Komunikační systém vyžaduje zajištění bezpečnosti v komunikačních zařízení, přenosového prostředí, kryptografických prostředků, obsluhy, provozních podmínek a postupů.

„Komunikační systém je systém zajišťující přenos informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy.“[23] Komunikační systém musí především zajistit důvěrnost, integritu, neodmítnutelnost odpovědnosti a dostupnost utajovaných informací. Jednotlivé požadované body jsou definovány v bezpečnostní politice, jsou zajištěny jak fyzickými prostředky, tak organizačními a provozními postupy, vhodnými opatřeními a provozními směrnicemi. Vlastní kapitolu komunikačního systému tvoří kryptografická ochrana, zde je definována instalace kryptografického prostředku, jeho nastavení, zajištění provozní obsluhy, používání kryptografických klíčů, zajištění výroby klíčových materiálů, odesílání kryptografické písemnosti v listinné a nelistinné podobě a dále zajištění servisu. Samotný

[23] Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7537.

kryptografický materiál, klíčový materiál, ale i kryptografická písemnost se označují slovem „KRYPTO“, evidenčním číslem, nebo číslem jednacím z administrativních pomůcek kryptografické ochrany, administrativní pomůcky v této oblasti jsou: evidenční karta, rejstřík evidenčních karet, provozní deník, evidenční kniha, jednací protokol, manipulační kniha, doručovací kniha a zápůjční kniha a stupněm utajení. Listinná podoba pak uvádí i název státu, právnické osoby, nebo fyzické osoby, místo a datum, kde kryptografická písemnost vznikla, číslo výtisku a počet listů včetně počtu stran příloh[24].

4.2.4 Počítačové sítě

Počítačová síť je celkové uspořádání technických prostředků, které umožňují a realizují spojení, zajišťující výměnu informací respektive kódovaných dat mezi počítači na určité ploše v určitém prostoru a tím umožňuje komunikaci mezi uživateli. Hned na začátku je však nutné napsat, že počítačovou sít, ve které se zpracovávají utajované informace, není možné jen tak napojit k jiným sítím. Připojení utajované sítě informačního systému k síti vnější, jež není pod kontrolou správy, musí být zajištěno vhodným certifikovaným bezpečnostním rozhraním tak, aby se zamezilo průniku do utajované sítě. Systémové požadavky na bezpečnost v prostředí počítačové sítě vychází z § 9 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stíněných komor, kde musí být zajištěna:

- fyzická ochrana pro lokální počítačovou síť v rámci zabezpečené oblasti včetně všech komponentů komunikačního kanálu,
- spolehlivá identifikace a autentizace komunikujících stran, včetně ochrany identifikační a autentizační informace,
- ochrana důvěrnosti a integrity utajované informace při přenosu utajované informace v systému, základním prostředkem pro zajištění důvěrnosti v komunikačním kanále je kryptografická ochrana, pro zajištění integrity je zavedení spolehlivé detekce, jež by odhalila záměrné a náhodné změny utajované informace,
- ochrana rozhraní počítačové sítě proti průniku do informačního systému,
- plná kontrola správy počítačové sítě.

[24] Česko. Vyhláška č. 524 ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9998-9998.

4.2.5 Podmínky ICT

V předcházejících částech je uvedeno, co je počítačová síť, informační a komunikační systém a jaké jsou na ně obecné požadavky, nyní se pokusím definovat jednotlivé požadavky v osmi krocích, které je nutné začlenit do projektu sítě, u samostatné stanice se mnohé části vynechají:

- Prvním krokem je definice systému - tj. zjištění určení daného systému z hlediska pokrytí uživatelských potřeb, rozhodnout o bezpečnostním provozním módu, stanovit klasifikaci a kategorii informací, jmenovat management a určení uživatelů.
- Druhým krokem je definování bezpečnostních požadavků - jmenování minimální funkcionality systému, zohlednění životního cyklu, stanovení požadavků z oblasti počítačové a komunikační bezpečnosti, definování požadavků na bezpečnost provozního prostředí a na dokumentaci.
- Třetím krokem je návrh samotného systému - jejím obsahem je bezpečnostní architektura systému.
- Čtvrtým krokem je navržení bezpečnostních opatření v informačních technologiích, zde je nutné zohlednit a zapracovat: autentizaci uživatelů; řízení přístupu; souborové a tiské služby; zpracování, registraci a vyhledávání dokumentů v systému; síťové uživatelské prostředí; správu pracovních stanic; antivirovou ochranu; vyhodnocování logů, či zálohování a archivaci dat.
- Pátým krokem je definování adresářových služeb v případě sítí - tj. jejich začlenění do Domain Name Systému, stanovení organizační a geografické struktury, zajištění služeb doménových řadičů, stanovení aplikace skupinových politik.
- Šestým krokem je definování komunikační infrastruktury - tzn. rozhodnout o typu lokální sítě o její topologii, o kategorii kabeláže, o aktivních prvcích; o použití kryptografické ochrany a o poskytovaných službách komunikační infrastruktury.
- Sedmým krokem je definování bezpečného propojení na jiné systémy / sítě a stanovení rozhraní, vstupů a výstupů.
- Osmým krokem je vlastní definování informačních technologií: kabeláže, aktivních prvků, rozvaděčů, šifrovacích zařízení, doménových řadičů, souborového a služebního serveru, kořenové certifikační autority, záložního napájecího zdroje a vlastních stanic.

5 SYSTÉMOVĚ SPECIFICKÉ DETERMINACE

Výše uvedené determinace právní, personální a materiálně technická musí být zohledněny v bezpečnostní dokumentaci a v analýzách.

5.1 Bezpečnostní dokumentace informačního systému

Bezpečnostní dokumentace informačního systému popisuje všechny oblasti informačního systému, zahrnuje: fyzickou bezpečnost, počítačovou a komunikační bezpečnost, personální bezpečnost, průmyslovou bezpečnost, administrativní bezpečnost, včetně organizačních opatření k zajištění celkové bezpečnosti vycházející z analýzy rizik, dále plány, směrnice, řády a seznamy atd., jako taková je posuzována Národním bezpečnostním úřadem před vydáním certifikátu informačního systému.

Bezpečnostní dokumentace informačního systému[25] je obecně písemným dokumentem popisujícím jednotlivé komponenty informačního systému, postupy, zásady a pravidla bezpečnosti při práci v daném informačním sytému, skládá se z:

- Projektové bezpečnostní dokumentace informačního systému, která obsahuje: bezpečnostní politiku a návrhy bezpečnosti informačního systému, jež mají zajistit bezpečnostní politiku včetně popisu a podmínky realizace.
- Provozní bezpečnostní dokumentace informačního systému, která obsahuje provozní bezpečnostní směrnice, to jsou pravidla, pokyny a zásady, které popisují určitou činnost, v tomto případě provoz v oblasti: činnosti bezpečnostních správců, činnosti správců informačního systému, správců kryptografické ochrany, činnosti uživatelů atd.

Výše uvedená Bezpečnostní dokumentace informačního systému dále obsahuje: popis servisních činností, popis údržby komponent, který je zajišťován správcem informačního systému, nebo externisty splňující podmínky zákona, tj. mají příslušná osvědčení pro práci v daném módu, nebo vyšším, které schválil bezpečnostní správce, popis řešení havárií komponent informačního systému a krizových situací, včetně

[25] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9979-9980.

stanovení opatření zaměřené na minimalizaci škod, zajištění obnovy systému do certifikovaného stavu, nouzový provoz, likvidaci následků a stanovení odpovědnosti za jednotlivé úkony.

5.1.1 Bezpečnostní politika

Bezpečnostní politika je obecně základní, nosný dokument, stanovující soubor zásad, norem, pravidel a postupů, způsob, jakým má být zajištěna důvěrnost, integrita a dostupnost utajované informace a odpovědnost uživatele, bezpečnostního správce a správce informačního systému za jeho činnost v informačním systému. Jinými slovy stanovuje základní aktiva informačního systému tj. HW a SW komponenty, data apod. a zásady k ochraně místa, majetku, osob a informací informačního systému. Jeho cílem je tedy zajištění kvality, dostupnosti, důvěrnosti a integrity informací, jež jsou zpracovávány v prostředí informačního systému a zajištění odpovědnosti uživatele za svou činnost v informačním systému. Úkolem bezpečnostní politiky je jasné, závazné definování a popis komponentů, koncepce, přístupů, vnitřních norem, bezpečnostních zásad, standardů, směrnic a postupů pro oblast informační bezpečnosti, jež se týkají uživatelů, administrátorů, bezpečnostních správců a dalších osob vstupujících do informačního systému. Bezpečnostní politika zahrnuje také oblast počítačové bezpečnosti, která je vypracována[26]:

- Z minimálních bezpečnostních požadavků definující:
  - jednoznačnou identifikaci a autentizaci uživatele, bezpečnostního správce a správce informačního systému, správce kryptografické ochrany a zajištění důvěrnosti a integrity autentizační informace,
  - volitelné řízení přístupu k objektům na základě přístupových práv včetně jejich identity a členství ve skupinách,
  - nepřetržité zaznamenávání událostí, jež mohou ovlivnit bezpečnost informačního systému a zabezpečení záznamů před neautorizovaným přístupem,
  - zkoumání záznamů a odpovědnosti jednotlivých uživatelů a všech správců,
  - ošetření paměťových objektů před jejich dalším použitím,

[26] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9980-9986.

- ochranu důvěrnosti dat během přenosu mezi zdrojem a cílem.

- Ze systémově závislých bezpečnostních požadavků, z požadavků uživatelů a výsledků analýzy rizik. Vyhláška Národního bezpečnostního úřadu č. 523/2005 v § 8 říká, že informační systém se musí provozovat pouze v některém z uvedených módů: bezpečnostní provozní mód vyhrazený, bezpečnostní provozní mód s nejvyšší úrovní, nebo bezpečnostní provozní mód víceúrovňový. Musí být splněny minimální bezpečnostní požadavky z oblasti počítačové bezpečnosti a opatření z oblasti administrativní, personální a fyzické bezpečnosti informačních systémů, u bezpečnostního provozního módu s nejvyšší úrovní a víceúrovňového módu jsou povinné mechanismy volitelného řízení přístupu subjektů informačního systému k objektům informačního systému. Požadavky personální bezpečnosti se odvozují od zvoleného bezpečnostního provozního módu.
- Z bezpečnostních požadavků nadřízeného orgánu resp. nadřízené bezpečnostní politiky pokud byla zpracována.

5.1.2 Další součásti bezpečnostní dokumentace

Bezpečnostní dokumentace mimo výše jmenovaného obsahuje[27]:

- Projekt fyzické bezpečnosti včetně krizového plánu objektu, je dokumentací popisující objekt po technické stránce, její součástí jsou plány, nákresy, popisující charakter a konstrukci objektu, jeho zabezpečení.
- Analýzu rizik informačního systému, včetně jejich ohodnocení a možných opatření.
- Krizový plán pro objekt, osoby, počítačovou síť a utajované informace. Obsahuje řešení a postupy při mimořádných událostech a krizových stavech, jeho částmi jsou: katalog krizových opatření, operační plány, výkresy, mapy, seznamy osob krizového řízení, seznam odpovědných osob, plán nezbytných dodávek a zdravotnického zařízení.
- Provozní, bezpečnostní, návštěvní a požární řád. To jsou soubory zásad, pravidel, uspořádání a pořádku, podle nichž se musí v dané oblasti postupovat, v našem případě v oblasti: provozu, bezpečnosti, návštěv a požáru.

[27] Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9979-9986.

- Seznam oprávněných uživatelů informačního systému s uvedením uživatelského identifikátoru a role v informačním systému, a to ke kontrolám a ke včasnému vyřazení uživatele při zániku jeho Osvědčení nebo Oznámení, změně jeho pracovního zařazení, odchodu z organizace apod.
- Seznam aktiv informačního sytému k zajištění správy konfigurace – vedení seznamu HW a SW bezpečnostním správcem informačního systému v přehledné formě, včetně údaje o zabudovaných utajovaných informací.
- Návrh bezpečnostních testů informačního systému.

5.2 Analýzy

Analýza je obecně rozbor, rozklad, vědecká metoda, pozorování a měření, je to postup od něčeho neurčitého k něčemu konkrétnímu v reálném čase. V oblasti informačního systému jsou využívány analýza potřeb a analýza stávajícího stavu, kterými jsou definovány samotné potřeby organizace a popis aktuálního stavu, a analýza možného ohrožení utajovaných informací u podnikatele, která je požadována zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti v § 98, který pojednává o bezpečnostní dokumentaci, v odstavci b, kdy organizace zpracovávající utajované informace má povinnost do bezpečnostní dokumentace začlenit analýzu možného ohrožení utajovaných informací včetně účinných ochranných opatření ke snížení rizik.

5.2.1 Analýza potřeb a analýza stávajícího stavu

Pod analýzou potřeb informačního sytému si můžeme představit nějaký logický rámec projektu nebo systematický rozbor projektu, studii, koncepci, definování potřeb a cílů organizace vycházející z nějakého skutečného stavu. Pokud skutečný stav není stanoven, je nutné provést i analýzu stávajícího stavu, což je metoda zkoumající skutečný stav v organizaci, při této analýze jsou zkoumána data minulá a stávající. Společně pak slouží jako podklad pro návrh počítačové sítě a jejího zabezpečení, protože: identifikuje potřeby a cíle organizace, vymezuje jednotlivé pojmy a jejich rozsah, respektive stanovuje kritéria, identifikuje platné právní prostředí ČR a požadavky organizace, definuje vlastní dokumentaci, politiky, směrnice, řády a popisuje stávající stav v organizaci týkající se samotné organizace, její struktury

a procesů, objektů organizace a jejího vybavení, technického vybavení hardware a software, komunikačního vybavení, samotných sítí a pracovníků.

5.2.2 Analýza rizik

Analýza rizik je metoda zabývající se rozborem rizik v organizaci. Rizika jsou identifikována a klasifikována do jednotlivých stupňů a v seznamu rizik jsou pak uvedena od největšího rizika k menšímu. Výsledkem analýzy rizik je dokument popisují rizika, jejich hodnocení a návrh možných opatření, kterými by se příslušná rizika snížila na akceptovatelnou úroveň, nebo eliminovalo. Setkáme se zde s pojmy jako: aktivum, dopad, riziko bezpečnosti informací, vyhnutí se riziku, komunikace rizik, odhad rizik, identifikace rizik, redukce rizik, podstoupení rizik, přenos rizik atd. Česká technická norma ISO/IEC 27005 o informační technologii – bezpečnostní politice a Řízení rizik bezpečnosti informací rozděluje danou problematiku do šesti kapitol: 1): identifikace jednotlivých aktiv informačního systému, 2): hodnocení daných aktiv informačního systému, 3): zvládání rizik informačního systému, 4): akceptace rizik informačního systému, 5): komunikace rizik informačního systému, 6) monitorování a přezkoumání rizik informačního systému. Z výše uvedeného vyplývá, že na začátku je nutné provést identifikaci[28] týkající se:

- Identifikace samotných aktiv, které rozdělujeme na primární a podpůrná aktiva, přičemž primární aktiva jsou samotné informace, obchodní procesy a činnosti, naproti tomu podpůrná aktiva představují technické a programové vybavení jako: hardware a software, komunikační techniku, sítě, kde se definuje typ přenosu: aktivní, nebo pasivní, komunikační rozhraní, dokumentaci informačního systému, pracovníky tj. manažeři - ti, co rozhodují, správci, uživatelé, pracovníci provozu / údržby, vývojáři, lokalitu a samotnou organizaci.
- Identifikace rizik. Účelem této identifikace je, co by se mohlo stát, kdyby něco byla způsobena potencionální ztráta.
- Identifikace hrozeb. Zde by měly být identifikovány hrozby a jejich zdroje. Hrozby se rozlišují podle typu, ke každému typu jsou pak přiřazeny samotné hrozby.
- Identifikace stávajících opatření. Zde jsou identifikovaná stávající a plánovaná opatření vycházející z různých dokumentací a implementačních plánů.

[28] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 9-18.

- Identifikace zranitelnosti, kterou definujeme v těchto oblastech: organizace, procesy a postupy, běžná praxe řízení, pracovníci, fyzické prostředí, konfigurace informačního systému, hardware, software, komunikační zařízení, a závislost na externích stranách.
- Identifikace následků. Následky se zde posuzují z hlediska: vyšetřování a doby nápravy, ztráty času, ztráty příležitosti, zdraví a bezpečnosti, finančních nákladů na zvláštní dovednosti nutné pro nápravu škody, pověsti a důvěryhodnosti.
- Identifikace a stanovení základních hodnotících kritérií, které zohledňují strategické hodnoty procesu informací a činnosti organizace, kritičnost informačních aktiv, platnou legislativu, regulační požadavky, smluvní povinnosti, dostupnost, důvěrnost a integritu, negativní následky ztráty důvěryhodnosti a pověsti aj., dále stanovují kritéria dopadu, zde hovoříme například o úrovni klasifikace daného aktiva, nebo o narušení bezpečnosti informací, poškození provozu, ztrátě činnosti, poškození pověsti aj. a samozřejmě musí být vytvořena a určena kritéria akceptace rizik s přihlédnutím k obchodu, legislativě, provozu, technologiím, financím aj. faktorům.
- Posledním bodem této části je pak stanovení rozsahu a hranice pro řízení rizik.

Druhým krokem je odhad rizika, v této oblasti se setkáme s metodou odhadování rizik, ty mohou být[29] 1) kvalitativní, k popisu velikosti se používá následků například nízkých, středních, vysokých a pravděpodobnosti, že se tyto následky vyskytnou při určitém atributu, nebo 2) kvantitativní, tato metoda používá stupnici a číselné hodnoty, dále hodnocením následků, určení pravděpodobnosti incidentu a úrovní odhadu rizik. Třetím krokem je pak vlastní vyhodnocení rizik[30], v tomto kroku jsou posuzovány shody aktuálního stavu ICT bezpečnosti s požadovanou bezpečností např. BS7799/ISO 17799 a dalšími dokumenty standardizační povahy. Nakonec jsou stanoveny závěry z analýzy rizik a interpretovány návrhy zásad vyplývajících z analýzy rizik, hovoříme zde o zvládání rizika, kdy dochází buď k redukci rizika, podstoupení rizika, vyvarování se rizika, nebo k přenosu rizika, které musí být začleněny do legislativy dané organizace, nebo implementovány cestou technických a netechnických opatření ke zvládání rizik a odstínění přetrvávajících a doznívajících, nebo také zbytkových rizik[31].

[29] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 18.
[30] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 18-20.
[31] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. s. 20-24.

6 APLIKACE VE FIKTIVNÍ FIRMĚ

Organizace ATOBEZ a. s. byla zřízena k zajištění bezpečnosti při manipulaci s jaderným materiálem. Dokumenty, které bude organizace vytvářet, zpracovávat a distribuovat jsou utajovanými informacemi stupně utajení Vyhrazené a Důvěrné, a musí proto být zabezpečeny podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

6.1 Studie proveditelnosti

Organizace si v prvním kroku nechává vypracovat studii proveditelnosti informačního systému s pracovním názvem IS ATOBEZ-UI pro zpracování utajovaných informací v dané organizaci. Studie zahrnuje analýzu potřeb, která definuje zákonné podmínky pro realizaci, analyzuje výchozí podmínky v organizaci, kde se má informační systém budovat a navrhuje způsob realizace s ohledem na požadavky včetně financí a výchozího stavu v organizaci.

6.2 Analýza potřeb

Analýza vychází z definovaných a odsouhlasených potřeb, zjištěného stavu v organizaci a možností organizace, jak dosáhnout vytčených cílů. Při této analýze se využívá studium všech dostupných dokumentů, fyzický průzkum stavu techniky a objektu na místě, konzultace zástupců zainteresovaných stran a doporučení Národního bezpečnostního úřadu. Výsledky analýzy jsou projednávány s vedením organizace formou oponentního řízení. Vlastní analýza je podkladem k návrhu realizace informačního systému IS ATOBEZ-UI pro zpracování utajovaných informací a jejího zabezpečení. Analýza vychází z definovaných potřeb a ze zjištěného stávajícího informačního systému ATOBEZ, který jen částečně řeší uživatelské potřeby a není způsobilý ke zpracování utajovaných informací.

6.2.1 Definované potřeby

Podrobnou analýzou definovaných potřeb docházíme k jednoznačně a detailně vymezenému cíli studie proveditelnosti. Takto vymezený cíl nebo cíle umožní při zjišťování stávajícího stavu vymezit potřeby, stanovit metody a nástroje pro vlastní

realizaci výstavby IS ATOBEZ-UI. Jednotlivé potřeby jsou definovány ve dvanácti bodech.

Bod první: ochrana utajovaných informací. Z charakteru dokumentů v listinné nebo nelistinné podobě, které mají být elektronicky zpracovávány, vyplývá, že se jedná o informace utajované ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v platném znění.

Bod druhý: stupeň utajení zpracovávaných informací. Stupeň utajení je stanoven na úrovni Vyhrazené nebo Důvěrné a odpovídá nařízení vlády č. 522/2005 Sb., ve znění nařízení vlády č. 240/2008 Sb., v kterém se v příloze č. 16 stanoví seznam utajovaných informací v oblasti působnosti Státního úřadu pro jadernou bezpečnost. Mimo toho se budou zpracovávat utajované informace Evropské unie stupně utajení Restreint UE - ekvivalent stupni Vyhrazené. V důsledku těchto podmínek a zjištěného požadavku na řízení přístupu k informacím je nezbytné stanovit, aby IS ATOBEZ-UI pracoval v bezpečnostním provozním módu s nejvyšší úrovní. Tento bezpečnostní provozní mód umožňuje zpracování utajovaných informací různého stupně utajení, ve kterém všichni uživatelé musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávnění pracovat se všemi utajovanými informacemi. Celkový objem zpracovaných informací je 98 % v úrovni Vyhrazené a zbývající dvě procenta jsou ve stupni Důvěrné.

Bod třetí: počet osob zpracovávajících utajované informace pomocí IS ATOBEZ-UI nebo se na zpracování podílejících. 30 osob bude utajované informace vytvářet nebo se podílet na jejich fyzickém zpracování, další 3 osoby se budou s utajovanými informacemi pouze seznamovat. Pro správu IS ATOBEZ-UI budou potřeba dvě další osoby, jedná se o bezpečnostního správce informačního systému a správce informačního systému. Do zabezpečených oblastí, kde bude IS ATOBEZ-UI provozován, bude mít, mimo výše jmenovaných osob, přístup i technická správa objektu, jedná se o tři osoby: údržbáře, uklízečku a provozovatele objektu, tyto osoby se přímo nebudou seznamovat s utajovanými informacemi, ale nelze vyloučit přístup k informačním technologiím a médiím IS ATOBEZ-UI.

Bod čtvrtý: distribuce utajovaných informací uvnitř organizace a mimo organizaci. Utajované informace budou primárně vznikat uvnitř organizace v jednom objektu v druhém patře samostatné třípodlažní budovy. Zde se budou utajované informace rovněž zálohovat a archivovat, v tomto prostoru bude též umístěna serverová část IS ATOBEZ-UI. Utajované informace se v některých případech budou přijímat, případně odesílat Státnímu úřadu pro jadernou bezpečnost.

Bod pátý: spolupráce v rámci Evropské unie. Distribuce utajovaných informací v rámci Evropské unie se přímo nepředpokládá, ale bude prováděna prostřednictvím SÚJB. Tzn., že IS ATOBEZ-UI nebude propojen s institucemi Evropské unie, pouze vybrané materiály budou přijímány, případně budou na SÚJB odesílány a označeny jako „EU“.

Bod šestý: množství zpracovaných dokumentů a jejich druh. Množství zpracovávaných dokumentů plyne z analýzy stávajícího stavu a studia rozvoje dané problematiky. IS ATOBEZ-UI bude navržen s 20% rezervou. Převážná část zpracovávaných dokumentů tj. 80 % je nelistinné povahy, zbytek 20 % je listinné povahy. Dokumenty nelistinné povahy jsou o kapacitě 40 kB na jednoho zpracovatele denně, odesílané dokumenty jsou o kapacitě cca 1100 kB.

Bod sedmý: počítačová síť a pracovní stanice. Z počtu zpracovatelů, rozsahu zpracovávaných dat a jejich distribuce vyplývá, že je potřebné vybudovat IS ATOBEZ-UI jako počítačovou sít. Počítačová síť musí umožnit zpracování informací tak, aby více uživatelů mohlo současně přistupovat k informacím týmu, informacím pracoviště a k dalším zdrojům. Materiál musí být možné distribuovat jakýmkoliv uživatelem jakémukoliv oprávněnému uživateli. Uživatel resp. skupina uživatelů má přístup jen k těm informacím v IS ATOBEZ-UI, které nutně potřebují ke své práci. Uživatelé buď samostatně, nebo skupina uživatelů společně vytváří dokument, který je následně předán vedoucímu střediska, který materiál buď odsouhlasí, nebo vrátí k dopracování. Po schválení materiálu vedoucím střediska se materiál postupuje řediteli organizace. Ředitel organizace materiál schválí a prostřednictvím svého asistenta se materiál buď vytiskne, nebo zašle na SÚJB, nebo se archivuje. Asistent vede jednací protokol. Pro

výše uvedený model zpracování dat je dostatečné vybavení uživatelů standardními počítači. Činnost asistenta ředitele je nutné zajišťovat na výkonnější pracovní stanici.

Bod osmý: Komunikační bezpečnost při přenosu utajovaných informací mezi ATOBEZ a SÚJB. ATOBEZ a. s., na základě dohody se SÚJB, zřídí ve svém objektu vzdálenou pracovní stanici informačního systému SÚJB. Utajované informace budou mezi oběma systémy přenášeny na vyjímatelném nosiči utajovaných informací v prostoru ATOBEZ a. s. Za zajištění komunikační bezpečnosti mezi svým systémem a jeho vzdálenou pracovní stanici bude odpovědný SÚJB. Správa této pracovní stanice bude v působnosti správy informačního systému SÚJB, provozní obsluhou budou pověřeni určení zaměstnanci ATOBEZ a. s., kteří budou postupovat podle bezpečnostní směrnice pro obsluhu / užití informačního systému SÚJB.

Bod devátý: aplikační programové vybavení. Činnosti uživatelů IS ATOBEZ-UI spočívají v analýze provozních dat technického zařízení s jaderným obsahem. Jsou zaznamenány toky dat, porovnávány s normativy a vyhodnocovány odchylky. Data z technického zařízení jsou předávána na DVD ve formě souborů v programu MS Excel. Výstupem se primárně požaduje materiál ve formátu: DOCX, XLSX a PDF, předpokládá se možnost zpracování i dalších dat, které mají nativní formáty operačního systému nebo kancelářského balíku (obrázky, videosekvence, prezentace, apod.).

Bod desátý: opatření počítačové bezpečnosti. IS ATOBEZ-UI je potřebné – mimo fyzickou bezpečnost ve smyslu vyhlášky 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků – zajistit hardwarově, softwarově a organizačními opatřeními. V oblasti počítačové bezpečnosti je třeba zajistit:

- jednoznačnou identifikaci a autentizaci uživatele,
- zajistit ochranu důvěryhodnosti a integrity utajované informace,
- volitelné řízení přístupu k objektům na základě rozlišování příslušných práv uživatele a identity uživatele nebo jeho členství ve skupině uživatelů,
- nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením,

- možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele,
- ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu,
- zajištění integrity,
- zajištění dosažitelnosti informací a služeb,
- zajištění antivirové ochrany.

Bod jedenáctý: zálohování a archivace dat. Na základě požadavku dostupnosti zpracovaných dat a celého informačního systému musí IS ATOBEZ-UI umožnit provádění záloh, archivaci dat a zálohování systémových prostředků.

Bod dvanáctý: Internet. Organizace by ráda připojení k Internetu; po konzultaci s Národním bezpečnostním úřadem organizace překvalifikovala svůj požadavek a IS ATOBEZ nebude připojen k Internetu. Uživatelská potřeba využívat Internet bude řešena v rámci stávajícího firemního informačního systému.

6.2.2 Stávající informační systém ATOBEZ

Analýza stávajícího stavu provedla průzkum v těchto oblastech: bezpečnost stávajícího stavu informačního systému, využitelnost stávajícího informačního systému, personální bezpečnost, fyzickou bezpečnost, administrativní bezpečnost a krizové řízení.

V oblasti bezpečnosti stávajícího informačního systému bylo zjištěno: v organizaci je v současné době provozován informační systém, který představuje 48 pracovních stanic a tři servery. Existuje připojení na Internet. Je instalován poštovní server. Je instalován antivirový program Symantec Endpoint Protection, ten je aktualizován a upgradován 1x za týden. Uživatelská data nejsou zálohována ani archivována. Základním výstupem informačního systému je tisková sestava, ta je evidována a je s ní nakládáno jako s dokumentem dle zákona o archivní službě.

V oblasti využitelnosti stávajícího informačního systému k uspokojení potřeb definovaných v předchozí kapitole bylo zjištěno: stávající informační systém byl

pořízen před pěti roky a technicky je zastaralý. Bezpečnostní standardy na ochranu utajovaných informací nesplňuje. Serverová část je pro potřeby zvažovaného systému nedostatečná. Připojení systému k Internetu vylučuje zpracování utajovaných informací v tomto systému.

Oblast personální bezpečnosti. Základní podmínkou přístupu k utajovaným informacím je personální bezpečnost. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti přesně stanoví, za jakých podmínek se fyzická osoba může seznamovat s utajovanými informacemi. Odstavec 1 § 11 zákona stanoví, že fyzické osobě lze umožnit přístup k utajované informaci stupně Důvěrné, jestliže jej nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti, je držitelem platného osvědčení fyzické osoby příslušného stupně utajení a je poučena, nestanoví-li zákon nebo jiný právní předpis jinak. Do současné doby se utajované informace zpracovávaly v organizaci na ručních psacích strojích, proto je v organizaci v současné době dostatečný počet uživatelů budoucího informačního systému s platným osvědčením fyzické osoby příslušného stupně utajení a to včetně bezpečnostního správce, a budoucího správce informačního systému. Organizace má zpracován personální projekt dle § 72 zákona, tento projekt však neuvažoval s funkcemi správce informačního systému. Organizace nepotřebuje pracovníky kryptografické ochrany, protože správcem kryptografického prostředku umístěného v pracovní stanici v místnosti číslo 11 v zabezpečeném objektu firmy ATOBEZ a. s. bude pracovník SÚJB.

Oblast fyzické bezpečnosti. Fyzická bezpečnost představuje systém opatření, nástrojů a podmínek, kterými se zamezuje nebo ztěžuje fyzický přístup neoprávněných osob k utajovaným informacím, popřípadě takový přístup nebo pokus o neoprávněný přístup zaznamenat pomocí ostrahy, režimových opatření a nasazených technických prostředků. Organizace má zpracován projekt fyzické bezpečnosti, kterým je definován objekt a zabezpečené oblasti, včetně jejich hranic, jsou určeny kategorie a třídy zabezpečených oblastí. Projekt obsahuje vyhodnocení rizik, způsob použití příslušných opatření fyzické bezpečnosti a je zpracován provozní řád objektu. Je zpracován plán zabezpečení objektu a zabezpečení oblastí v krizových situacích. Projekt fyzické bezpečnosti neuvažuje o možnosti provozu informačního systému pro zpracování

utajovaných informací, není tedy popsán způsob zabezpečení tras strukturované kabeláže, místností pro servery a případné stínění k ochraně před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování. Fyzické zabezpečení objektu odpovídá zabezpečení definovanému v projektu fyzické bezpečnosti, tzn., že v objektu organizace je vybudováno 16 zabezpečených oblastí kategorie Důvěrné, patnáct zabezpečených oblastí se využívá pro zpracování utajovaných informací a jedna zabezpečená oblast je využívaná jako úložiště utajovaných informací. Místnost pro servery je v projektu označena jako zabezpečená oblast.

Oblast administrativní bezpečnosti. Administrativní bezpečnost tvoří systém při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informace. Administrativní bezpečnost je v organizaci zajištěna v souladu s příslušnými ustanoveními zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění a vyhlášky Národního bezpečnostního úřadu č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací v platném znění. Utajované informace jsou řádně označovány, evidovány v jednacím protokolu. Pro přepravu utajovaných informací jsou k dispozici bezpečnostní zavazadla. Odpovědnou osobou organizace je jmenována osoba odpovědná za vedení jednacího protokolu. Je zpracován vnitřní předpis o zajištění administrativní bezpečnosti v organizaci.

Oblast kryptografické ochrany. Partnerem je SÚJB, který provozuje svůj vlastní certifikovaný informační systém. Existuje písemná dohoda mezi SÚJB a ATOBEZ a. s. o vytvoření vzdáleného samostatného pracoviště SÚJB, které bude umístěno v zabezpečeném prostoru ATOBEZ a. s., o tuto pracovní stanici bude informační systém SÚJB doplněn. Informace mezi oběma systémy budou přenášeny na vyjímatelném nosiči utajovaných informací. Za zajištění komunikační bezpečnosti při přenosu mezi systémem SÚJB a jeho vzdálenou pracovní stanicí umístěnou v objektu ATOBEZ a. s. bude odpovědný SÚJB.

Oblast krizového řízení. Krizovým řízením se rozumí souhrn řídících činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik,

plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace. Organizace má způsob řešení krizových situací zapracován jako přílohu k projektu fyzické bezpečnosti, součástí jsou požární poplachové směrnice a evakuační plán.

6.3 Návrh řešení a systémový projekt: IS ATOBEZ-UI

Po provedené analýze výchozího stavu informačního systému a jeho zabezpečení v organizaci, jejím projednáním v oponentním řízení je zpracován návrh realizace počítačové sítě a jejího zabezpečení. Návrh směřuje k vybudování certifikovaného IS ATOBEZ-UI. Z výše definovaných potřeb a zjištěného stávajícího stavu plynou dvě možná řešení:

Řešení první. Utajované informace jsou z 98 % zpracovávány ve stupni Vyhrazené. Nabízí se možnost danou problematiku rozdělit do dvou informačních systémů, resp. podsystémů, kdy by byl jeden informační systém vybudován pouze pro zpracování utajovaných informací Vyhrazené a druhý samostatný informační systém pro stupeň Důvěrné, pro který by byl vyčleněn pouze jeden počítač sdílený menším počtem uživatelů. Řešení oddělením stupňů utajení nabízí snížení požadavků personální bezpečnosti na většinu uživatelů a možné snížení nákladů na zajištění fyzické bezpečnosti Stupeň Důvěrné by byl jen pro jednu vlastní stanici a pro vzdálenou stanici SÚJB.

Řešení druhé. Zde by problematika byla řešena v jediném informačním systému v bezpečnostním provozním módu s nejvyšší úrovní pro stupeň utajení Důvěrné, dle § 8 odst. 3 vyhlášky č. 523/2005 Sb., tzn., že všichni uživatelé by museli mít prověrku nejvyššího stupně, který se v systému nachází, tedy stupně Důvěrné, a celé řešení by muselo splnit požadavky na ochranu před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování. V systému musí být použity mechanismy volitelného řízení přístupu k informaci, které jsou běžnou součástí OS MS Windows.

Pro účely této práce bylo vybráno druhé řešení, a to z následujících důvodů:

- organizace preferuje řešení v jediném informačním systému;

- organizace preferuje prověření všech uživatelů systému na stupeň utajení Důvěrné;
- organizace preferuje zajištění fyzické bezpečnosti na stupeň utajení Důvěrné pro celý IS ATOBEZ-UI;
- objekt s budoucím IS ATOBEZ-UI má kolem sebe dostatečný perimetr kontrolovaný ATOBEZ a. s., aby mohlo být vyhověno požadavkům na ochranu proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování.

6.3.1 Počítačová sít

Počítačová síť se navrhuje typu lokální síť LAN. Vyčleněná LAN, v angličtině se pro tento případ používá pojem „dedicated“, bude propojovat požadovaný počet pracovních stanic tak, aby uživatelé mohli sdílet informace a zdroje v oblasti pamětí, výpočetní kapacity apod., účastníci sítě budou moci být trvale a přímo propojeni s datovými uložišti, proto bude nejlépe vyhovovat síťová architektura Klient/Server. Výhodou tohoto řešení je dobrá výkonnost, snadné nastavení a rozšíření, snadné nalezení a odstranění závad, přičemž při poruše jednoho počítače ostatní fungují.

V druhém patře budovy ATOBEZ a. s. se podle projektu fyzické bezpečnosti nachází 16 zabezpečených oblastí kategorie Důvěrné, jsou to místnosti označené 1 až 16, kde bude umístěn IS ATOBEZ-UI. Místnost číslo 12 bude vyčleněna pro samostatnou serverovnu pro servery a zařízení rozhraní sítě. Do této místnosti povede kabeláž kategorie 6 vyčleněná pouze pro IS ATOBEZ-UI. Rozvaděč kabeláže, ve kterém budou umístěny technologie informačního systému určené ke zpracování utajovaných informací, bude umístěn v zabezpečené oblasti. V systému bude použita rodina síťových protokolů TCP/IP a síťové prostředí Microsoft Windows založené na protokolu NetBIOS. Aktivní prvek Juniper bude vyhrazen jen pro IS ATOBEZ-UI a nebude sdílen se zbytkem organizace.

6.3.2 Datové toky

Z hlediska bezpečnosti, ale i efektivnosti, je nezbytné optimalizovat v organizaci datové toky:

1. Analyzovaná data od obsluhy technického zařízení s jaderným odpadem jsou předávána na médiu DVD ve formátu souborů XLSX, přebírá je osoba pověřená vedením jednacího protokolu.

2. Kontrola převzatých dat zahrnuje: kontrolu antivirovým programem a kontrolu čitelnosti média, provádí je osoba pověřená vedením jednacího protokolu.
3. Předání dat vedoucímu střediska znamená: zavedení dat do IS ATOBEZ-UI; distribuce vybraných dat referentovi nebo referentům, zpracovateli nebo zpracovatelům analýzy s pokynem ke zpracování dílčí analýzy a stanovení rozsahu osob, které budou s daty seznámeny a stanovení termínů zpracování dílčí analýzy.
4. Zpracování dílčí analýzy dat. Jednotliví referenti zpracovávají analyzovaná data v certifikovaném IS ATOBE-UI; materiál se zpracovává ve formátu XLSX a DOCX; výsledný dílčí materiál je referentem postoupen zpracovateli výsledného dokumentu, podílelo-li se na dokumentu více zpracovatelů; koncový zpracovatel vyhotovuje celkovou zprávu, kterou doplní o závěrečné shrnutí výsledků z analýzy dat; materiál se distribuuje vedoucímu střediska.
5. Vedoucí střediska materiál buď odsouhlasí, nebo vrátí k dopracování; odsouhlasený materiál je postoupen řediteli organizace ke schválení.
6. Ředitel organizace dokument schválí; dokument distribuuje svému asistentovi s pokynem k vytištění a expedici na SÚJB, nebo archivaci.
7. Asistent vytiskne příslušný dokument; dokument označí příslušným stupněm utajení; dokument označí číslem jednacím z jednacího protokolu; dokument nechá podepsat odpovědnou osobou.
8. Elektronickou verzi dokumentu schváleného odpovědnou osobou asistent uloží na příslušné médium tj. na DVD, případně USB Flash-disk a prostřednictvím pracovní stanice určené na přenos utajovaných informací IS SÚJB elektronicky odešle dokument SÚJB. V případě poruchy IS SÚJB dokument uloží do přepravního zavazadla, které stanoveným způsobem zabezpečí; bezpečnostní zavazadlo asistent předá proti podpisu kurýrovi s pokynem pro předání Státnímu úřadu pro jadernou bezpečnost.

6.3.3 Bezpečnostní provozní mód

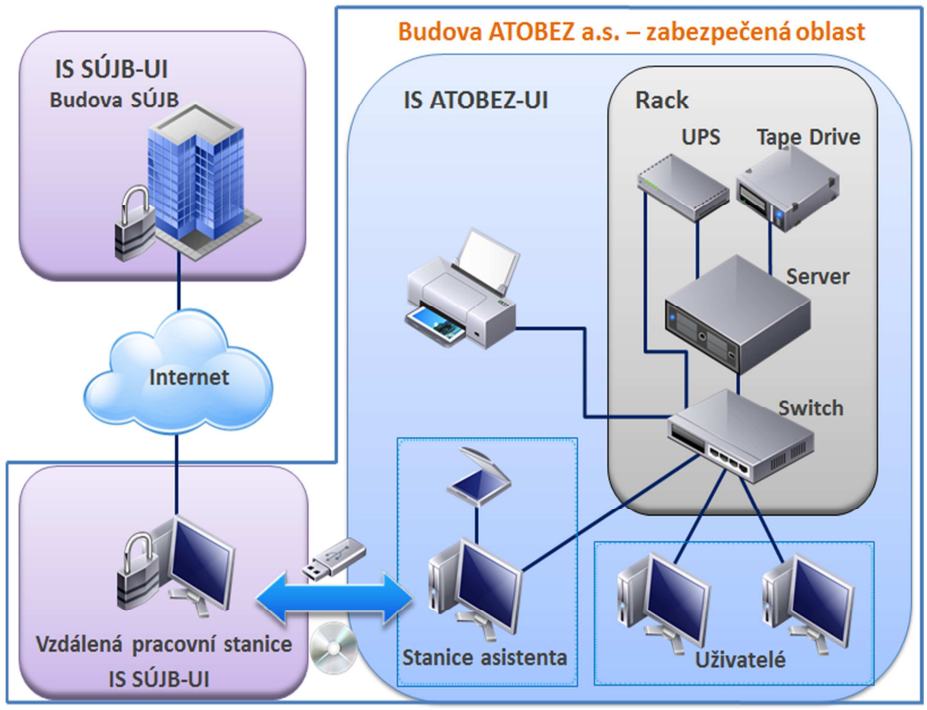
Vyhodnocením požadavků na řízení přístupu k utajovaným informacím a stupňů utajení se stanoví bezpečnostní provozní mód s nejvyšší úrovní dle § 8 odst. 3 vyhlášky Národního bezpečnostního úřadu č. 523/2005. Sb. o bezpečnosti informačních a komunikačních systému a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stíněných komor. Na základě něho bude možné zpracovávat

utajované informace různého stupně utajení, v našem případě do stupně Důvěrné, a všichni uživatelé informačního systému IS ATOBEZ-UI nemusí být oprávnění pracovat se všemi utajovanými informacemi v systému obsaženými.

6.3.4 Technické požadavky počítačové sítě

Informační systém bude založen na klasickém řešení Klient/Server, které spolu budou komunikovat skrze počítačovou síť (obrázek číslo 1 – zámečky v obrázku představují šifrování pro zajištění důvěrnosti dat při přenosu komunikačním kanálem). Tzn., že pracovní stanice budou přes switch Juniper WX2200 24 port připojeny k jednomu serveru kabeláží, mezi serverem a switchem budou 4 fyzické síťové karty. Na switch pak bude připojena ještě síťová tiskárna. Záložní zdroj elektřiny tj. UPS bude napájet switch a server. Server, aktivní prvek, UPS a zálohovací zařízení budou v provedení rack a budou umístěny do 19“ uzamykatelného 25 U velkého racku s ventilátorem, celý rackový komplet pak ještě bude doplněn o výsuvnou polici na klávesnici, 1U 17“ Flat Panel Monitor, patch panel, UTP kabely, dostatečně dimenzovanými zdroji elektřiny a čtečkou čipových karet pro přihlášení správce informačního systému.

Obr. 1 Počítačová síť IS ATOBEZ-UI



6.3.4.1 Kabeláž, rozbočovač, aktivní prvek a UPS

Kabeláž informačního systému bude postavena na produktech značek Belden a Panduit v kategorii 6. Belden vyrábí kabely a vodiče do průmyslové výroby a zabezpečovacích systémů a Panduit nabízí komplexní řešení síťové infrastruktury jako například: zásuvky, instalační krabice, RJ45 moduly, rozvaděče, propojovací a UTP kabely, patch panely, kabelové lišty a žlaby, vázací materiál, značení a bezpečnost sítě[32] Samotný uzamykatelný 19“ rack byl vybrán v provedení 25U od společnosti IBM, jelikož má perforované přední a zadní uzamykatelné, ocelové dveře, chlazení pro vysokou hustotu instalací, hloubku 100 cm a je doporučován pro servery řady IBM Systems x a všech jeho dalších komponent. Aktivní prvek Juniper byl vybrán z konfigurační nabídky IBM[33], riziko proti výpadku bude u něj eliminováno druhým záložním switchem se zakoupenou doživotní zárukou, který bude uložen také v racku, obdobným způsobem byla v systému IBM vybrána i síťová, racková UPS.

Tab. 1 Kabeláž, rozbočovač, UPS a Switch

Množství	Popis
1x	Kabeláž Belden a Panduit v kategorii 6 včetně žlabů
1x	IBM 25U Standard Rack Cabinet - RACK
1x	IBM Keyboard with integrated Poiting Device 3m cable/black/USB/ CZ
1x	IBM 1U 17 in Flat Panel Monitor
4x	IBM 1,5m Blue Cat 6e Cable
5x	IBM 1.5m, 10A/100-250V, C13 to IEC 320 - C14
1x	IBM 1500 LCD 2U Rack - UPS
2x	Juniper 24 port 1GB WX2200 Ethernet Switch for IBM Systém X
2x	Juniper 3 Year Onsite Repaier 22x7 4 Hour Response
1x	IBM 19-inch Rack Mount Kit - pro Switch

[32] *Panduit* [online]. Kassex 1995-2009 [cit. 2011-10-04]. Dostupné z WWW: <http://www.kassex.cz/produkty/panduit>.

[33] *IBM System x: IBM System x iCat - (Internet Interactive Catalogue) - interaktivní katalog* [online]. DNS, 2011 [cit. 2011-10-04]. Dostupné z WWW:<http://www.dns.cz/main.aspx?cls=art&base_tre_id=58&base2_tre_id=94&tre_id=368&vyrid=1002&menuactive=%3bml368%3b&art_id=1859>.

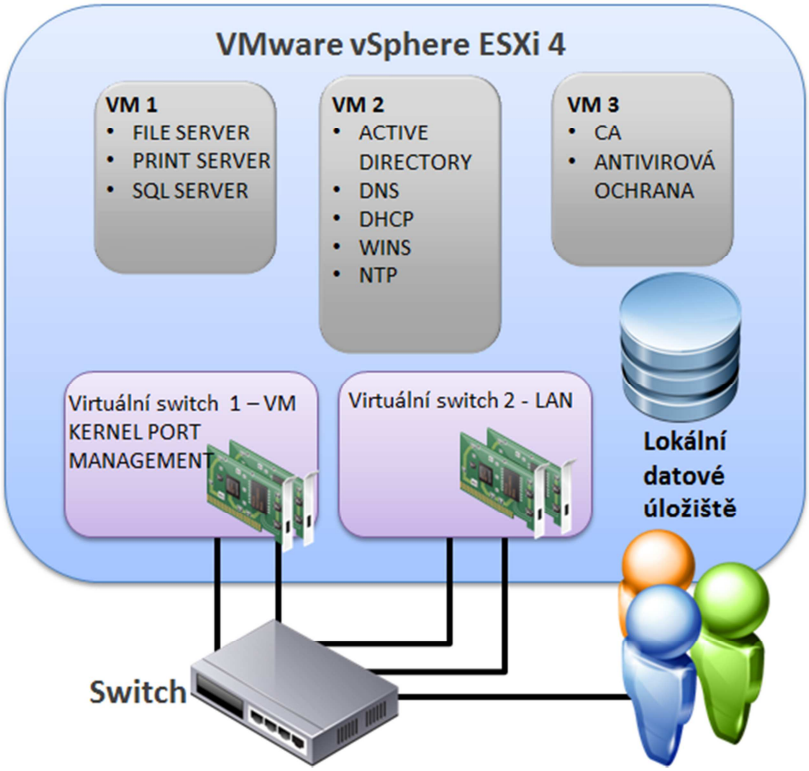
6.3.4.2 Server

Na fyzickém serveru budou ve virtuálním prostředí (obrázek číslo 2) provozovány 3 virtuální Microsoft servery: první virtuální server bude obsahovat: souborový tzv. File Server, tiskový tzv. Print Server, SQL server a MonitorWare Console, druhý virtuální server bude obsahovat: doménový řadič pro: Active Directory, DNS, DHCP, WINS a NTP a na třetím virtuálním serveru bude umístěna certifikační autorita. Na samotnou virtualizaci bude použit free produkt VMware ESXi ve verzi 4.0. Antivirová ochrana, cestovní profily a veškerá uživatelská data budou uložena na souborovém serveru, to znamená, že na lokálních discích stanic budou ukládány pouze dočasné soubory aplikací. S ohledem na tento fakt bude server plně redundantní, to se týká: CPU, HDD, sítových karet a zdrojů napájení. Z hlediska větší provozní spolehlivosti a bezpečnosti by bylo vhodnější řešení v provedení dvou serverů propojených v clusteru s jedním diskovým polem, vezme-li se však v potaz, že práce v informačním systému firmy ATOBEZ a. s. neběží v režimu 7x24 a nepracují zde zaměstnanci 5x8 dní v týdnu, pak postačí výpadek serveru respektive výpadek základní desky pokrýt dobrým servisem serveru. Uvnitř serveru budou umístěny čtyři HDD o velikosti 300 GB v provedení SAS v režimu RAID 5, to znamená, že jeden disk bude použit jako hotspare disk, zbývající tři disky budou tvořit lokální datové uložiště o efektivní kapacitě n-1 tj. 600 GB, z toho 100GB bude použito na CA, 100GB na druhý virtuální server a zbytek na první virtuální server. Server bude dále vybaven hardwarovým RAID řadičem a DVD-RW. Pro splnění výše uvedených podmínek byl vybrán IBM server x3550 M3 v provedení 1U Rack postavený na procesorové technologii Intel Xeon, který může mít až dva šestijádrové procesory, je rozšiřitelný ze 4 HDD na 8 HDD SAS/SATA, kapacita RAM až 192 GB modulů RDIMM nebo 48 GB modulů UDIMM, obsahuje i rozšířenou diagnostiku a přitom je energeticky úspornější. Server má vestavěný hypervizor VMware ESXi 4.0 s volitelnou pamětí flash 2 GB pro virtualizaci[34] a [35].

Obr. 2 Virtualizační prostředí

[34] *IBM Systém x3550 M3: Servery rack* [online]. IBM, 2011 [cit. 2011-09-30]. IBM. Dostupné z WWW: <http://www-03.ibm.com/systems/cz/x/hardware/rack/x3550m3/index.html>.

[35] *IBM System x: IBM System x iCat - (Internet Interactive Catalogue) - interaktivní katalog* [online]. DNS, 2011 [cit. 2011-10-04]. Dostupné z WWW: <http://www.dns.cz/main.aspx?cls=art&base_tre_id =58&base2_tre_id=94&tre_id=368&vyrid=1002&menuactive=%3bml368%3b&art_id=1859>.



Tab. 2 Server

Množství	Popis
1x	IBM Server x3550 M3, Xeon 4C 2,4 GHz/1066 MHz, 1x4 GB
1x	Intel Xeon 4C Processor 2,4 GHz/1066 MHz - druhý CPU
5x	IBM 4 GB
6x	IBM 2 GB
4x	IBM 300 GB HDD
1x	IBM 3550 M2 R2 ODD Kit - rozšíření na autoloader
1x	IBM 3 GB SAS HBA Controller v2
1x	IBM Dual Port 1GB Ethernet Daughter Card
1x	IBM 675 Redundant Power Supply
1x	IBM Ultraslim Enhanced SATA Multi-Bunner - DVD
1x	IBM 3Year Onsite Repair 24x7, 24 Hour Committed Service
1x	HID Omnikey 3121 USB - čtečka čipových karet
1x	Crescendo C700 - čipová karta
1x	VMware Server ESXi verze 4.0 - tato verze je zdarma

Množství	Popis
3x	MS Windows Serveru 2008 Standard Edition
1x	MS SQL Server Standard
1x	Symantec Endpoind Protection 12 - antivirová ochrana
1x	Adiscon MonitorWare Console

6.3.4.3 Zálohování a archivace dat

Uživatelská data budou ukládána na souborovém serveru vyčleněnému pro tento účel, pracovní stanice nebudou sloužit k ukládání dat uživatelů, a proto lokální HDD nebudou centrálně zálohovány. Zálohování a archivace bude prováděna automaticky programovým vybavením na externí storage TS2250, která má připojení přes SAS, je rozšiřitelná, funguje na technologii LTO Ultrium s fyzickou kapacitou 1,5 TB nativních dat a 3,0 TB v komprimovaných datech s přenosovou rychlostí 140 Mbps native[36]. Pro zálohování a archivaci je navržen software Symantec Backup Exec a to pro Windows Servery a pro SQL Server. Zálohovací kopie budou ukládány v odděleném prostoru, aby se předešlo haváriím a škodám, navrhuje se udržovat minimálně 3 generace záloh.

Tab. 3 Zálohování

Množství	Popis
1x	IBM Storage TS2250 Tape Drive Model H5S
1x	IBM 19-inch Rack Mount Kit
5x	IBM Ultrium 5 Data Cartridge - 5-pack
1x	IBM Mini-SAS/mini-SAS 1x Cable
1x	IBM 3 roky Onsite Repair 9x5 Same Business Day
1x	Symantec Backup Exec 2010 for Windows Server
2x	Symantec Backup Exec 2010 for Agent for Windows Server
1x	Symantec Backup Exec 2010 Agent for Microsoft SQL Server

[36] *IBM Systém Storage TS2250 Tape Drive Express: Páskové systémy* [online]. IBM, 2011 [cit. 2011-09-30]. Dostupné z WWW: <http://www-03.ibm.com/systems/cz/storage/tape/ts2250/index.html>.

6.3.4.4 Pracovní stanice

Pracovní stanice v celkovém množství 13 kusů budou umístěny v zabezpečených oblastech v kategorii Důvěrné a budou zabezpečeny tak, aby uživatelé neměli možnost měnit jejich konfiguraci a instalovat aplikace, přičemž konfigurace uživatelského prostředí bude prováděna pomocí skupinových politik v Active Directory. Takto navržené síťové uživatelské prostředí umožní, aby uživatelé nebyli vázáni na konkrétní stanici a mohli se vzhledem na režim práce dělit o pracovní stanice. Úložiště uživatelských dat budou směrována výhradně na datový server. Operační systém bude nastaven tak, aby pracovní soubory vznikající při zpracování utajovaných informací v žádném případě nebyly ukládány na HDD. Swapování OS bude zakázáno. Stanice po vypnutí nebude obsahovat utajované informace! Stanice nebudou obsahovat CD ani DVD a jejich USB vstupy budou softwarově zakázány pomocí produktu OptimAccess[37]. Součástí všech pracovních stanic je: klávesnice, 19“ monitor a USB čtečka čipových karet. Operačním systémem stanice bude MS Windows 7 Enterprise, který má certifikát NIST.

Tab. 4 Pracovní stanice

Množství	Popis
13x	Lenovo IdeaCentre AIO A320-1
13x	Lenovo ThinkVision L1951p - LCD display - TFT - 19"
13x	HID Omnikey 3121 USB - čtečka čipových karet
13x	HID Crescendo C700 - čipová karta
13x	MS Windows CAL 2008 Device - klient k serveru
13x	MS Windows 7 Enterprise
13x	Symantec Endpoind Protection 12 - antivirová ochrana
13x	Sodatsw OptimAccess
13x	ICZ Protect for Windows
13x	Microsoft Office Standard 2010
13x	Adobe Acrobat X Standard

[37] *OptimAccess: Technické řešení* [online]. Sodatsw, 1997-2012 [cit. 2011-10-03]. Dostupné z WWW: <http://www.sodatsw.cz/personalni-audit-jak-optimaccess>.

6.3.4.5 Kryptografický prostředek

Kryptografický prostředek bude součástí řešení komunikační bezpečnosti IS-SÚJB. Instalaci, konfiguraci a klíčové hospodářství bude zajišťovat SÚJB. Určený zaměstnanec ATOBEZ zajistí provozní obsluhu kryptografického prostředku, pokud to systém bude potřebovat. SÚJB dodá vlastní vzdálenou pracovní stanici certifikovaného IS SÚJB. Pracovní stanice bude obsahovat: počítač včetně kryptografického prostředku, monitor, tiskárnu, čtečku čipových karet a 3 čipové karty, dále SW vybavení: operační systém stanice, antivirovou ochranu, SW na šifrování disku, SW na ochranu USB vstupů, Office Standard 2010 a Adobe Acrobat X, kterou budou užívat určení zaměstnanci ATOBEZ při dodržení požadavků a postupů stanovených Bezpečnostní směrnicí pro uživatele IS-SÚJB. ATOBEZ se bude finančně podílet na nákladech na pořízení a provoz této stanice a rovněž na nákladech za přenosovou linku. Kryptografický prostředek bude umístěn v pracovní stanici v místnosti č. 11 v zabezpečené oblasti kategorie Důvěrné vedle místnosti serverovny, do této místnosti bude mít výhradní přístup pouze obsluha (pracovník ATOBEZ) a správce kryptografického prostředku, tj. pověřený pracovník SÚJB, který složil odbornou zkoušku odborné způsobilosti pracovníka kryptografické ochrany[38].

6.3.4.6 Řízení přístupu, souborové a tiskové služby

Souborový server bude využíván k těmto účelům: veškerá uživatelská data a cestovní profily budou uloženy na souborovém serveru. Profil bude upraven pomocí skupinové politiky tak, že se ze souborového serveru budou při přihlášení kopírovat pouze registry, ostatní části profilu uživatele budou přístupné přes namapované sdílené adresáře, výjimkou budou pouze dočasná data aplikací, která se budou ukládat na lokální disk stanice umístěné v zabezpečené oblasti kategorie Důvěrné a při odhlášení uživatele budou smazána. Souborový server bude dále využit pro sdílené adresáře pracovních podskupin pro společnou práci a správce informačního systému na něm bude mít uloženy instalační balíčky aplikací pro jejich instalaci pomocí skupinových politik. Pro řízení přístupu uživatelů k těmto výše uvedeným službám budou použity autorizační mechanizmy integrované v MS Windows a Active Directory.

[38] Česko. Vyhláška č. 524 ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9994-9995.

Veškeré tisky budou prováděny na sdílené tiskárně HP LaserJet Enterprise 500 Color M551 XH, rovněž umístěné v zabezpečené oblasti v kategorii Důvěrné u pracovních stanic. V odpovědnosti uživatelů bude zajistit v nejkratším čase evidenci utajovaných výtisků a manipulaci s nimi včetně skartace vadných nebo nadbytečných výtisků.

6.3.4.7 Autentizace uživatelů

Autentizace uživatelů využije metodu autentizace pomocí SmartCard Logon, což je dvoufaktorová metoda typu: co mám - SmartCard a co vím - PIN, využívající čipové karty standardu SmartCard a X.509 certifikáty. Její výhodou je bezpečnější proces autentizace, jednoduché PIN ze šesti číslic, které se nemusí měnit tak často jako heslo, a nutnost použít SmartCard při přihlášení. Tuto technologii je možné využít i pro další aplikace využívající X.509 certifikáty, jako například elektronický podpis dokumentů. Jestliže čipová karta bude zakoupena v duálním provedení, potom může být bezkontaktní část použita jako identifikační klíč pro kontrolovaný vstup do zabezpečených oblastí. Navrhovanou čipovou kartou je Crescendo C700 od společnosti HID, která podporuje operační systémy Windows XP 2000 / Vista / 7 a Windows Server 2003 a 2008, Windows Mobile, Mac OS X Linux, Solaris a Unix a využívá standardů ISO 7816 1 - 4, X.509, PFX, DER, PKCS 12, PCSC/CCID, Crypto API/MSCAP[39]. Pro autentizaci uživatelů bude použit Kerberos, který je integrován do MS Windows a Active Directory, Kerberos umožní uživatelům využít identitu získanou při přihlášení ke stanici k přístupu do všech aplikací informačního systému. Jako PKI pro SmartCard Logon bude využita kombinace Active Directory a Microsoft Certifikační autority. Certifikáty CA, certifikáty uživatelů a CRL budou publikovány v Active Directory a budou přístupné pomocí protokolu LDAP. Certifikační autorita bude vydávat certifikáty s platností jeden rok pro přihlášení uživatelů do systému a pro server a stanice pro zabezpečení přenášených informací. Správu čipových karet a jejich obsluhu bude provádět bezpečnostní správce informačního systému.

[39] *Logical Access Solutions: Documents* [online]. Haidglobal, 2010-10-03 [cit. 2011-10-03]. Dostupné z WWW: <http://www.hidglobal.com/documents/20101203-crescendo-ds-en.pdf>.

6.3.4.8 Zabezpečení disku stanice

Jednotlivé stanice umístěné v informačním systému IS ATOBEZ-UI budou zabezpečeny proti krádeži, či odnesení pevného disku tak, že všechny pevné disky stanic budou šifrovány komerčním krypto-grafickým prostředkem Protect for Windows pro pokrytí zbytkových rizik, který spolupracuje s přihlašovacím autentizačním zařízením od firmy HID čipová karta Crescendo C700 a čtečky Omnikey 3121.

6.3.4.9 Antivirová ochrana

Antivirová ochrana bude zajištěna antivirovými programy Symantec Endpoint Protection na zranitelném serveru a pracovních stanicích, tato ochrana musí zajistit: ochranu souborového systému pracovních stanic, ochranu souborového systému doménového serveru a off-line aktualizací virových bází, off-line proto, že informační systém nebude připojen k Internetu. Správce informačního systému bude provádět pravidelnou aktualizaci systému antivirové ochrany.

6.3.5 Umístění informačního systému v objektech organizace

Informační systém bude instalován u ATOBEZ a. s., Nové Jedle 23 v objektu „A“ v druhém patře samostatné třípodlažní budovy v jeho levé části, která je od ostatních prostor budovy oddělena železobetonovou zdí o síle 25 cm. Vstup do prostor je vymezen bezpečnostními dveřmi vybavenými elektrickým zámkovým zařízením a systémem kontroly vstupu certifikovaným pro stupeň utajení Důvěrné a na oknech jsou zabudovány mříže. Takto zabezpečená oblast plně splňuje požadavky uvedené ve vyhlášce Národního bezpečnostního úřadu č. 528/2005 Sb. Vymezený objekt obsahuje 16 zabezpečených oblastí kategorie Důvěrné, z toho:

- Jedna zabezpečená oblast - místnost číslo 12 bude vyčleněna pro umístění serveru.
- Jedna zabezpečená oblast bude vyčleněna pro úložiště utajovaných informací a úložiště utajovaných informací nelistinného charakteru.
- Jedna zabezpečená oblast bude vyčleněna pro bezpečnostního správce.
- Jedna zabezpečená oblast místnost číslo 11 bude vyčleněna pro umístění pracovní stanice IS SÚJB se zabudovaným kryptografickým prostředkem.
- Jedna zabezpečená oblast bude vyčleněna pro správce informačního systému.
- Zbývajících 11 oblastí bude vyčleněno pro uživatele.

Celý objekt s instalovanými komponentami IS ATOBEZ-UI splňuje požadavky na ochranu před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování. Do okruhu 90m od objektu jsou prostory ATOBEZ a. s., které je možno kontrolovat. Konečné splnění těchto požadavků bude před certifikací IS posouzeno Národním bezpečnostním úřadem.

6.3.6 Dostupnost služby

Informační systém musí zajistit, aby požadovaná utajovaná informace byla přístupná ve stanoveném místě, v požadované formě a v určeném časovém rozmezí dle § 10 odst. 1 vyhlášky Národního bezpečnostního úřadu č. 523/2005 Sb., proto byly zapracovány následující opatření:

- Informační systém musí být vybaven nepřerušitelným napájecím zdrojem UPS, který zajistí provoz i v době výpadku elektrického proudu po dobu nejméně 2 hodin a zároveň musí zajistit požadavky na ochranu před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování do napájecí sítě.
- Server musí být zakoupen s rozšiřující podporou garantující dodávku náhradního dílu do 2 dnů v režimu 7x24.
- V systému musí být dva stejné switche s doživotní zárukou.
- Uživatelská data musí být ukládána na servery, kde bude zajištěno jejich zálohování v pravidelných termínech a následně budou archivovány, to se týká i operačních systémů serverů.
- Součástí bezpečnostní směrnice správce informačního systému musí být zpracován plán obnovení činnosti po havárii.
- Sledování stability informačního systému a jeho údržba musí být smluvně zajištěna systémovou a technickou podporou.

6.3.7 Správa informačního systému

Pro zajištění správy bezpečnosti informačního systému se zavádí role Bezpečnostní správce informačního systému. Pro zajištění spolehlivého provozu informačního systému se zavádí role Správce informačního systému. Obě výše uvedené role nejsou slučitelné, tj. musí být vykonávány různými osobami.

6.3.7.1 Vyhodnocování logů

Události zaznamenané v provozním auditním logu na serverech a stanicích budou po prvotní filtraci zaznamenány na serveru, pro vyhodnocení logů v SQL databázi, kterou bude bezpečnostní správce pravidelně vyhodnocovat. Pro vyhodnocení logů budou k dispozici pravidla pro odfiltrování záznamů o legálních operacích. Pro centrální vyhodnocení logů bude použit Adiscon MonitorWare Console, což je aplikace pro analýzu protokolů a událostí MS Windows, firewallu a událostí v síti, a proto je vhodný pro bezpečnostní analýzy[40].

6.3.7.2 Správa pracovních stanic

Samotná správa pracovních stanic musí zajistit bezpečné prostředí, ve kterém budou zpracovávány utajované informace:

- Instalace operačního systému bude probíhat formou instalace z připravených obrazů operačního systému pro daný hardware.
- Instalace aplikací bude probíhat pomocí skupinových politik.
- Uživatelské prostředí se nakonfiguruje při prvním přihlášení uživatele pomocí skupinových politik.
- Aktualizace aplikací včetně antivirové ochrany a operačního systému, změny jejich konfigurace a zabezpečení se budou provádět pomocí skupinových politik.
- Pokud dojde k nefunkčnosti programového vybavení pracovní stanice, bude provedena její reinstalace.
- Konfigurace spolehlivě zajistí, že na lokálním disku stanice se nebudou vyskytovat žádná uživatelská data.

6.3.8 Návrh organizačních opatření

Základní podmínkou pro schválení provozu informačního systému pro zpracování utajovaných informací je certifikace informačního systému Národním bezpečnostním úřadem. Informační systém může být provozován pouze za podmínek stanovených ve vydaném certifikátu, vlastní provoz informačního systému je řízen bezpečnostní dokumentací schválenou Národním bezpečnostním úřadem. Bezpečnostní dokumentaci rovněž schvaluje odpovědná osoba organizace a vnitřním předpisem nebo

[40] *MonitorWare-Console* [online]. DLMASS, March 20 2008 [cit. 2011-10-04]. Dostupné z WWW: <http://www.dlmass.com/downloads/czech/MonitorWare-Console/>.

pokynem se stává závazná pro všechny zaměstnance organizace. Dalším dokumentem nezbytným pro schválení provozu informačního systému je zpracovaný projekt fyzické bezpečnosti objektu, který je schvalován Národním bezpečnostním úřadem. Tímto projektem se stanoví technická opatření nezbytná pro bezpečnost informačního systému, režimová opatření v objektu, režim manipulace s klíči a identifikačními daty a ostraha objektu. Odpovědná osoba organizace stanoví vnitřním předpisem činnost pracovníků organizaci v době vyhlášení krizového stavu. Bezpečnostní opatření, jež budou uplatněny v informačních technologiích:

- Všechny utajované informace budou bezpečně uchovávány na serverech.
- Vynucení bezpečné autorizace pracovních stanic, uživatelů a služeb zajištěno pomocí protokolu Kerberos a PKI.
- Rozdělení rolí pro jednotlivé administrační úkony tzv. dělení privilegií.
- Důsledné zabezpečení serverů a pracovních stanic za pomoci skupinových politik.
- Jednotný model automatické instalace a aktualizace programového vybavení na stanicích za pomoci skupinových politik.
- Centrálně spravovaná antivirová ochrana pro servery a stanice.
- Řízení přístupu uživatelů k objektům.
- Ošetření paměťových objektů před jejich dalším použitím.
- Veškeré konfigurace uživatelských profilů a data jsou uloženy na souborovém serveru, tzv. cestovní profily.
- Komunikace budou probíhat ve vyčleněné bezpečné LAN.
- Důvěrnost utajovaných informací při přenosu mezi lokalitami musí být zajištěna certifikovanými kryptografickými prostředky.

6.3.9 Časový harmonogram prací

Časový harmonogram prací na vybudování informačního systému pro zpracování utajovaných informací zahrnuje období od zpracování dokumentace po zkušební provoz, včetně.

Tab. 5 Časový harmonogram prací

Pořadí	Činnost	Počet pracovních dnů
1	Zpracování dokumentace	5
2	Výběrové řízení pro dodavatele	25

Pořadí	Činnost	Počet pracovních dnů
3	Zpracování návrhu bezpečnostní dokumentace (žádost o certifikaci IS a bezpečnostní dokumentace IS se předkládá NBÚ k certifikaci)	20
4	Přepracování projektu fyzické bezpečnosti (předkládá se ke schválení NBÚ)	5
5	Realizace strukturované kabeláže	10
6	Dodávka a instalace serveru	5
7	Oživení serveru	5
8	Dodávka a instalace pracovních stanic	2
9	Dodávka a instalace UPS	1
10	Přeorganizování zabezpečených oblastí	3 souběžně
11	Oživení informačního systému	3
12	Konfigurace virtuálních serverů a vytvoření uživatelských účtů	4
13	Školení uživatelů a správců	2
14	Zkušební provoz, provedení bezpečnostních testů a doložení jejich výsledků Národnímu bezpečnostnímu úřadu.	10
15	Certifikace Národním bezpečnostním úřadem (provozovatel zajistí součinnost s Národním bezpečnostním úřadem tak, aby certifikát byl vydán před termínem požadovaným pro zahájení ostrého provozu)	-
16	Schválení ostrého provozu odpovědnou osobou organizace	5
	Celkem (bez doby na certifikaci od NBÚ)	105

6.3.10 Podmínky realizace:

Informační systém pro zpracování utajovaných informací se bude realizovat dodavatelky a to jak dodávka techniky hardware a software, tak dodávka bezpečnostní dokumentace a školení uživatelů a správců. Subdodavatelsky bude zajištěna dodávka, instalace a přebudování stávajících zabezpečených oblastí do nových zabezpečených

oblastí. Vlastními pracovníky organizace bude provedena úprava projektu fyzické bezpečnosti.

6.3.11 Rozpočet nákladů

V tabulce jsou zaneseny celkové náklady za jednotlivé logické celky, rozpis položek je uveden v Příloze II: Kalkulace k rozpočtu.

Tab. 6 Rozpočet nákladů

Kapitola	Popis	Kusy	Cena bez DPH
6.3.4.1	Kabeláž, rozbočovač, aktivní prvky a UPS	1	717.909 Kč
6.3.4.2	Server	1	189.311 Kč
6.3.4.3	Zálohování	1	190.958 Kč
6.3.4.4	Pracovní stanice	1	635.037 Kč
6.3.4.5	Platba SÚJB za certifikovanou stanici s kryptografickým prostředkem	1	144.438 Kč
6.3.4.6	Sítová tiskárna	1	24.700 Kč
	Fyzická bezpečnost	1	574.482 Kč
	Instalace	1	943.000 Kč
	Školení	1	412.500 Kč
	Instalační dokumentace	1	450.000 Kč
	Celkem bez DPH a s DPH: 4.282.335 Kč		5.138.802 Kč

6.4 Bezpečnostní dokumentace a certifikace

Po schválení studie proveditelnosti informačního systému organizací ATOBEZ a. s. bude zpracována bezpečnostní dokumentace informačního systému a po jejím projednání s Národním bezpečnostním úřadem může být provedena vlastní výstavba informačního systému. Takové projednání není stanoveno legislativou. Pokud jej však provozovatel informačního systému neuskuteční, hrozí, že Národní bezpečnostní úřad nebude akceptovat řešení nebo jeho některé části a proces certifikace se protáhne nebo dokonce znemožní.

ZÁVĚR

Legislativa pro oblast utajovaných informací je velice rozsáhlá. Nebylo cílem této práce provést detailní analýzu všech právních norem, které definují různé oblasti fyzické, personální, administrativní bezpečnosti atd. V první části je uveden přehled základních právních předpisů, pojednávajících o utajovaných informacích, včetně některých základních pravidel a podmínek. Druhá část obsahuje aplikaci zjištěných informací na fiktivní firmě. Kde bylo nutné ověřit, zdali dané řešení bezpečnosti a funkcionality informačního systému je reálné, vhodné pro danou organizaci a její požadavky, a zda použité bezpečnostní technologie poskytují požadované záruky, zda vyhovují požadavkům Národního bezpečnostního úřadu na provoz informačního systému zpracovávající utajované informace a je kompatibilní s dalšími částmi řešení. Proces získání certifikátu informačního systému výrazně usnadňuje použití klíčových prvků informačního systému, pro které je k dispozici hodnocení bezpečnosti dle metodiky Common Criteria[41]. U bakalářské práce je stanoven maximální rozsah stran, takže samotná aplikace vybudování informačního systému pro zpracování utajovaných informací nemůže danou problematiku vylíčit do posledního detailu. Proto jsem důraz položila na řešení počítačové bezpečnosti a řešení datového toku do dalšího infomačního systému SÚJB. Tzn., že jsem nejdříve zjistila, jaké software mají hodnocení bezpečnosti, na kterých mohu informační systém založit, následně jaké mají hardwarové požadavky, to se týkalo systémů VMware Serveru ESXi verze 4.0 a MS Windows 2008 Serveru a aplikačního vybavení jakým je například MS SQL Server atd., pak jsem hledala hardware, které podporuje výše uvedené systémy a aplikace. Zde se jednalo především o kompatibilitu s VMwarem. K výsledkům softwarových požadavků jsem připočetla rezervu 20% pro případný rozvoj informačního systému a přes serverové konfigurátory počítačových firem IBM a Dell jsem získala přesné hardwarové konfigurace serverů z vybraných řad, oba výsledné servery jsem porovnala a výhodnější řešení jsem do bakalářské práce zapracovala. Dané serverové řešení jsem postavila, pokud možno v redundantním provedení, čímž jsem eliminovala riziko výpadku, mimo samotného serveru, protože pak by řešení bylo velmi drahé. Vezme-li se však v potaz, že práce v informačním systému firmy ATOBEZ a. s. neběží v režimu 5x8, pak postačí

[41] *Common Criteria* [online]. Common Criteria Portal, 2011 [cit. 2011.09.23]. Dostupné z WWW: <http://www.commoncriteriaportal.org/>.

výpadek serveru pokrýt dobrým servisem. Po konfiguraci serveru, zálohovacího zařízení, UPS, aktivních prvků, racku, výběru stanic včetně bezpečnostních doplňků a sítové tiskárny jsem pokračovala s přesnou identifikací software, tzn., že bylo nutné v cenících firem Microsoft, Symantec atd. vyhledat odpovídající licence, které řeší požadovanou problematiku a zároveň jsou vhodné pro typ naší fiktivní firmy. Další práce se týkaly již samotného bezpečnostního nastavení tak, aby byly zohledněny a splněny všechny podmínky, které na informační systém nakládající s utajovanými informacemi klade zákon, například v oblasti řízeného přístupu, identifikace a autentizace atd. Samotnou kapitolou pak byla kryptografická ochrana, kde jsem nejdříve vypracovala řešení se zajištěním kryptografické ochrany uvnitř IS ATOBEZ-UI a až poté jsem si uvědomila, že jej vlastně nemohu v bakalářské práci prezentovat, informace ohledně certifikovaných kryptografických prostředků jsou vydávány na vyžádání oprávněným osobám, to sice splňuji já jakožto fyzická osoba, ale práce s těmito informacemi by nemohla být veřejná, takže jsem musela pozměnit potřeby fiktivní firmy tak, aby daná oblast v bakalářské práci řešena byla, a zároveň jsem neporušila zákon. Přes veškerou snahu o přehlednost textu jsem nemohla v předkládané práci příliš zestručnit popis technického řešení informačního systému. Musela jsem vzít v úvahu, že studie proveditelnosti, aby byla správným základem pro vybudování informačního systému, musí důkladně popsat kritéria, současný stav a požadovaný stav informačního systému. Právě detailní popis technického řešení informačního systému dává předpoklad pro jeho kontrolu a následně certifikaci Národním bezpečnostním úřadem. Pro dodavatele slouží popis technického řešení jako závazné vodítko při vlastní realizaci projektu. Jiné části informačního systému jako například kabeláž, či fyzická bezpečnost objektu, byly pak pojaty v bakalářské práci s větší volností, jednak proto, že po obsahové stránce by například fyzická bezpečnost mohla být samostatnou bakalářskou prací a jednak i proto, že nebyly definovány přesné údaje o objektu sídla fiktivní společnosti ATOBEZ a. s., tyto práce by v obou případech vyžadovaly technické a stavební plány. Cílem bakalářské práce bylo vytvoření studie proveditelnosti počítačové sítě pro zpracování utajovaných informací do stupně utajení Důvěrné, která měla danou problematiku v obecné rovině vymezit a následně je reálně aplikovat na fiktivní firmě, aby si případný čtenář udělal představu, co vše se pod tímto pojmem skrývá, jaké podmínky musí být splněny a jaké zásady musí být dodrženy, domnívám se, že předloženou prací byl zadaný cíl snad splněn.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. DOČKAL, J. Bezpečnost WLAN v souladu se standardy. *DATA SECURITY MANAGEMENT*. 17. června 2010, roč. XIV, č. 2, s. 40. ISSN 1211-8737.
2. KINDL, J. *Projektování bezpečnostních systému I. Díl.* Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. 134 s. ISBN 80-7318-165-7.
3. LAUCKÝ, V. *Bezpečnostní futurologie*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 93 s. ISBN 978-80-7318-560-2.
4. LAUCKÝ, V. *Speciální bezpečnostní technologie*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.
5. LAUCKÝ, V. *Technologie komerční bezpečnosti I.* Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. 64 s. ISBN 80-7318-194-0.
6. PEKAREK, O., ČÍŽEK, V. *Práce s agenturními a elektronickými informacemi.* Vyd. 1. České Budějovice : Vysoká škola evropských a regionálních studií, 2007. 138 s. ISBN 978-80-86708-40-9.
7. PIPER, F., MURPHY, S. *Kryptografie.* Přeložil Pavel Mondschein. Vyd. 1. Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5.
8. POŽAR, J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.
9. ROELTGEN, C. *ITś hidden face: Everything you always wanted to know about Information Technology*. A look behind the scenes. CreatesSpace, 2009. 286 s. ISBN 978-1442152311.
10. STEINER, O. Úskalí při nasazování elektronického podpisu. *DATA SECURITY MANAGEMENT*. 17. června 2010, roč. XIV, č. 2, s. 48. ISSN 1211-8737.
11. TUČEK, P. TMP aneb důvěryhodný počítač. *DATA SECURITY MANAGEMENT*. 17. června 2010, roč. XIV, č. 2, s. 34. ISSN 1211-8737.
12. VACCA, J. R. *Computer and Information Security Handbook.* Vyd. 1. Morgan Kaufmann, 2009. 928 s. ISBN 978-0123743541.

13. VOLNER, Š. *Bezpečnosť v 21. storočí*. Vyd. 1. Bratislava : Iris, 2009. 387 s. ISBN 978-80-89256-36-5.
14. WILLIAMS, B., SAWYER, S. *Using Information Technology*. Vyd. 9. Career Education, 2010. 608 s. ISBN 978-0073516776.
15. ŽILKA, R. Utajování dat v souborových systémech. *DATA SECURITY MANAGEMENT*. 18. června 2009, roč. XIII, č. 2, s. 34. ISSN 1211-8737.

Elektronické zdroje

1. *Bezpečnost v kostce* [online]. Gity, 18. 10. 2011 [cit. 2011-10-19]. Dostupné z WWW: <http://www.chrantesidata.cz/cs/art/1039-hlavni-strana/>.
2. *Common Criteria* [online]. Common Criteria Portal, 2011 [cit. 2011.09.23]. Dostupné z WWW: <http://www.commoncriteriaportal.org/>.
3. ČERMÁK, M. *Analýza rizik: jemný úvod do analýzy rizik* [online]. CLEVER AND SMART, 2008-2012 [cit. 2011-09-22]. Dostupné z WWW: <http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>.
4. *IBM Systém Storage TS2250 Tape Drive Express: Páskové systémy* [online]. IBM, 2011 [cit. 2011-09-30]. Dostupné z WWW: <http://www-03.ibm.com/systems/cz/storage/tape/ts2250/index.html>.
5. *IBM System x: IBM System x iiCat - (Internet Interactive Catalogue) - interaktivní katalog* [online]. DNS, 2011 [cit. 2011-10-04]. Dostupné z WWW: <http://www.dns.cz/main.aspx?cls=art&base_tre_id=58&base2_tre_id=94&tre_id=368&vyrid=1002&menuactive=%3bml368%3b&art_id=1859>.
6. *IBM Systém x3550 M3: Servery rack* [online]. IBM, 2011 [cit. 2011-09-30]. Dostupné z WWW: <http://www-03.ibm.com/systems/cz/x/hardware/rack/x3550m3/index.html>.
7. *Logical Access Solutions: Documents* [online]. Haidglobal, 2010-12-03 [cit. 2011-10-03]. Dostupné z WWW: <http://www.hidglobal.com/documents/20101203-crescendo-ds-en.pdf>.
8. *MonirWare-Console* [online]. DLMASS, March 20 2008 [cit. 2011-10-04]. Dostupné z WWW: <http://www.dlmass.com/downloads/czech/MonitorWare-Console/>.

9. *OptimAccess: Technické řešení* [online]. Sodatsw, 1997-2012 [cit. 2011-10-03]. Dostupné z WWW: <http://www.sodatsw.cz/personalni-audit-jak-optimaccess>.
10. *Panduit* [online]. Kassex, 1997-2009 [cit. 2011-10-04]. Dostupné z WWW: <http://www.kassex.cz/produkty/panduit>.
11. PSZCZOLKA, M. *Objektová bezpečnost: úvod do problematiky* [online]. Specialista.info, 2005.10.02 [cit. 2011-09-18]. Dostupné z WWW: <http://magazin.specialista.info/view.php?cisloclanku=2005100201>.

Legislativní dokumenty

1. Česko. Nařízení vlády č. 522 ze dne 25. prosince 2005, kterým se stanoví seznam utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9950-9977. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=522/2005&typeLaw=zakon&what=Cislo_Zákona_smlouvy>. ISSN 1211-1244.
2. Česko. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9978-9993. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=523/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
3. Česko. Vyhláška č. 524 ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 9994-10008. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=524/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
4. Česko. Vyhláška č. 525 ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 1009-10014. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=525/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
5. Česko. Vyhláška č. 526 ze dne 14. prosince 2005 o stanovení vzorů používaných v průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání

žádosti podnikatele (vyhláška průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10015-10044. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=526/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.

6. Česko. Vyhláška č. 527 ze dne 14. prosince 2005 o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10045-10078. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=527/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
7. Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10079-10115. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=528/2005&typeLaw=zákon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
8. Česko. Vyhláška č. 529 ze dne 15. prosince 2005 o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, částka 179, s. 10116-10151. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=529/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
9. Česko. Vyhláška č. 55 ze dne 25. února 2008, kterou se mění vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2008, částka 16, s. 842-844. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=55/2008&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
10. České. Zákon č. 29 ze dne 18. ledna 2000 o poštovních službách a o změně některých zákonů (zákon o poštovních službách). In *Sbírka zákonů, Česká republika*. 2000, částka 10, s. 336-352. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=29/2000&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

11. Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7526-7576. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=412/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
12. Česko. Zákon č. 413 ze dne 21. září 2005 o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti (tiskový zákon). In *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7577-7591. Dostupný také z WWW:<http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.Aspx q=413/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy>. ISSN 1211-1244.
13. Česko. Zákon č. 499 ze dne 30. června 2004 o archivnictví a o spisové službě a o změně některých zákonů. In *Sbírka zákonů, Česká republika*. 2004, částka 173, s. 9742-9780. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=499/2004&typeLaw=zakon&what=Cislo_zakona_smlouvy>.

Ostatní zdroje

1. ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 52 s.
2. *Freeware*: *Freeware* [online]. JULIS-MD, 2011 [cit. 2011-09-27]. Dostupné z WWW: <http://www.julis-mb.de/free-console>.
3. *IBM System x: Servery: Rack*: *IBM System x3550 M3* [online]. IBM, 2011 [cit. 2011-09-26]. Dostupné z WWW: <http://www-03.ibm.com/systems/cz/x/hardware/rack/x3550m3/index.html>.
4. *IBM: Servery: Rackové servery* [online]. TECH DATA, 2011 [cit. 2011-09-26]. Dostupné z WWW: <http://intouch.techdata.com>.
5. *Identifikační systémy*: *Čtečky čipových karet OMNIKEY* [online]. GOLDCARD, 2009 [cit. 2011-09-26]. Dostupné z WWW: <http://www.identifikacnisystemy.com/ctecky-cipovych-karet-omnikey/>.
6. *Mechanické zábranné prostředky*. [online]. Národní bezpečnostní úřad, 1.2.2012 [cit. 2012-02-06]. Dostupné z WWW: <http://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/mechanicke-zabranne-prostredky/>.

7. *Microsoft: Serverové aplikace* [online]. TECH DATA, 2011 [cit. 2011-09-26]. Dostupné z WWW: <http://intouch.techdata.com>.
8. *Symantec: Antivirový a bezpečnostní software* [online]. TECH DATA, 2011. [cit. 2011-09-26]. Dostupné z WWW: <http://intouch.techdata.com>.
9. *Symantec: Zálohovací software* [online]. TECH DATA, 2011 [cit. 2011-09-26]. Dostupné z WWW: <http://intouch.techdata.com>.
10. *Tiskárny*: *Tisková technologie - Laserová* [online]. eD' system Czech, 2007-2011 [cit. 2011-10-11]. Dostupné z WWW: <http://edlink.edcz.cz/main.aspx?cls=ProductDetail&pro_id=359717>.
11. *Zařízení elektrické zabezpečovací signalizace a tísňové systémy*. [online]. Národní bezpečnostní úřad, 1.2.2012 [cit. 2012-02-06]. Dostupné z WWW: <http://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/zarizeni-elektricke-zabezpecovaci-signalizace-a-tisnove-systemy/>.

SEZNAM POUŽITÝCH ZKRATEK

Tab. 7 Seznam zkratek

Název zkratky	Celý název
AD	Active Directory
AES	Šifrovací algoritmus - Advanced Encryption Standard
AM	Administrativní pomůcka
CA	Certifikační autorita
CD	Compact Disc
CPU	Procesor - Central Processing Unit
CRL	Certificate Revocation List
DC	Doménový řadič - Domain Controller
DER	DER zakódovaný certifikát
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Versatile Disc nebo Digital Video Disc
EKV	Elektronická kontrola vstupu
EPS	Elektronický protipožární systém
EZS	Elektronický zabezpečovací systém
FO	Fyzická osoba
FS	Souborový server - File Server
GB	Gigabite
HDD	Pevný disk - Hard disk drive
HTML	Hyper Text Markup Language
http	Hypertext Transfer Protocol
HW	Hardware
ICT	Informační a komunikační technologie
IP	Internet Protocol

Název zkratky	Celý název
ISA	Industry Standard Architecture
IT	Informační technologie
KS	Komunikační systém
LDAP	Lightweight Directory Access
Mbps	Megabit za sekundu
MS	Microsoft
NATO	Severoatlantická aliance - North Atlantic Treaty Organization
NBÚ	Národní bezpečnostní úřad
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCR	Optické rozpoznávání znaků - Optical Character Recognition
OEM	Original Equipment Manufacturer
PBS	Provozní bezpečnostní směrnice
PDF	Portable Document Format
PFX	Personal inFormation eXchange
PIN	Personal identification number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PO	Právnická osoba
PS	Tiskový server - Print Server
SSL	Secure Sockets Layer
SÚJB	Státní úřad pro jadernou bezpečnost
SW	Software
TB	Terabyt
TCP	Transmission Control Protocol
Úřad	Národní bezpečnostní úřad
WINS	Windows Internet Naming Service

SEZNAM POJMŮ

Tab. 8 Seznam pojmů

Pojem	Výklad
Active Directory	Active Directory je adresářová služba společnosti Microsoft, která umožňuje administrátorům, mimo jiné, nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře.
Advanced Encryption Standard	Advanced Encryption Standard je v kryptografii označení pro symetrickou blokovou šifru.
Aktivum informačního systému	Je definovaný hardware, software, dokumentace informačního systému a samotné utajované informace, jež jsou v informačním systému uloženy.
Autentizace	Je v informatice ověření identity. Ke zjištění identity se používá: co uživatel zná: hesla nebo PIN; co uživatel má: hardwarový klíč, SmartCard, privátní klíč; čím uživatel je - biometrické vlastnosti jako otisk prstu, snímek oční duhovky nebo sítnice a podle toho co uživatel umí – třeba nějaký kontrolní dotaz.
Autorizace subjektu	Je udělení, přidělení nějakých práv subjektu pro výkon jeho činností.
Bezpečnostní správce	Je pracovník správy informačního systému nebo komunikačního systému v roli zajišťující řízení, kontrolu bezpečnosti a zajištění bezpečnosti zabezpečených systémů.
Bezpečnostní standard	Je utajovaný soubor pravidel, který stanovuje postupy, technická řešení, bezpečnostní parametry, organizační opatření pro zajištění ochrany utajovaných informací.
Certifikace	Je potvrzení, nebo také veřejná listina a ověření splnění podmínek při udělování certifikátů a jejich vlastní přidělení. V textu se setkáme s certifikací informačního systému - to znamená, že daný systém splňuje všechny podmínky vymezené zákony pro práci s utajovanými informacemi v daném stupni, jako takový prošel kontrolou, kterou vykonal Národní bezpečnostní úřad, který daný certifikát vydal, v takovém informačním systému mohou být následně zpracovávány utajované informace daného stupně. Certifikát musí mýt i kryptografický prostředek, jež je určen ke kryptografické ochraně pro daný stupeň. Certifikát – osvědčení fyzické osoby musí mít i uživatel pracující s utajovanými

Pojem	Výklad
	informacemi v daném informačním systému, tak jako správce informačního systému, nebo bezpečnostní správce.
Certifikační autorita	Certifikační autorita je v asymetrické kryptografii subjekt, který vydává digitální certifikáty - elektronicky podepsané veřejné šifrovací klíče, čímž usnadňuje využívání PKI.
Common Criteria	Bezpečnostní hodnocení IT - Common Criteria for Information Technology Security Evaluation, September 2006, Version 3.1, Revision 1, CCMB-2006-09-001, starší verze byla vydána jako ČSN ISO/IEC_15408-2 a 3, česká technická norma, Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT, Český normalizační institut, 2002.
CRL	Certificate Revocation List je seznam zneplatněných certifikátů.
Data Encryption Standard	Data Encryption Standard je v kryptografii symetrická šifra.
DHCP	Dynamic Host Configuration Protocol, je protokol z rodiny TCP/IP, přiděluje počítačům IP adresu, masku sítě, implicitní bránu a jméno DNS serveru.
DNS	Domain Name System - hierarchický systém doménových jmen.
Dopad	Nepříznivá změna ovlivňující úroveň dosažených cílů organizace.
DoS	Denial of Service nebo také Distributed Denial of Service je distribuované odmítnutí služby.
Důvěrnost	Je vlastnost informací, která znemožňuje odkrytí informace neoprávněné osobě, jinými slovy tzn., že systém je zajištěn před neautorizovaným přístupem.
DVD	Digital Versatile Disc nebo Digital Video Disc je formát digitálního optického datového nosiče.
Fyzická bezpečnost	Fyzická bezpečnost je ve starší terminologii označována jako objektová bezpečnost.
Hrozba	Je jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva.
HTML	Hyper Text Markup Language, označovaný zkratkou HTML, je značkovací jazyk pro hypertext.
http	Hypertext Transfer Protocol je Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML.
Identifikace	Obecně můžeme říci, že je to zjištění a stanovení totožnosti na

Pojem	Výklad
	základě shodných charakteristik.
Identifikace rizika	Je proces hledání, sepsání a charakterizování prvků rizika.
Informace	Dnes široký pojem, informace jako vědění, informace jako nositel genomu DNA, informace jako místo, kde se je možné o něčem informovat, informace jako nehmotná skutečnost, informace jako zpráva, nebo údaj a informace v informatice jako kódovaná data, které je možné vysílat, přijímat, uchovávat a zpracovávat. Dělíme je dle jejich nosiče na hlas, zvuk, písmo, obraz, disk, ale setkat se můžeme i s rozdělením listinné a nelistinné.
Integrita	Zjednodušeně můžeme říci, že je to zajištění vlastností: celistvosti, soudržnosti a neporušenosti. Datová integrita nám dává záruku, že daná data, informace byla přijata a přečtena bez chyb.
IP	Internet Protocol je datový protokol používaný pro přenos dat přes paketové sítě.
ISA	Industry Standard Architecture je počítačová sběrnice pro rozšiřující karty.
Kerberos	Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu.
Komunikace rizik	Výměna nebo sdílení informací o riziku mezi tím, kdo rozhoduje a ostatními zúčastněnými stranami.
Kryptografický prostředek	Je technický prostředek nebo softwarový produkt používaný ke kryptografické ochraně, nebo je to zařízení používané k výrobě, nebo k testování klíčového materiálu. Jako takový musí být certifikován Národním bezpečnostním úřadem.
LDAP	Lightweight Directory Access Protocol je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru.
NTP	Network Time Protocol je protokol pro synchronizaci vnitřních hodin počítačů po paketové síti s proměnným zpožděním.
Objekt informačního systému	Je pasivní prvek informačního systému, který obsahuje nebo přijímá informaci.
Odhad rizik	Je proces k ukončení hodnot pravděpodobnosti a následků rizika.
OEM	Original Equipment Manufacturer je obchodní termín, který označuje výrobce zařízení v našem případě je spojen s produkty

Pojem	Výklad
	Microsoft.
Opatření	Můžeme říci, že je to ustanovení, zařízení nebo postup v nějakém jednání, jehož úkolem je předcházet, zabraňovat či nouzově zajistit mimořádnou situaci. Opatření je bezpečnostní prostředek, jehož nasazením eliminuje riziko.
PDF	Portable Document Format – přenosný formát dokumentů je souborový formát vyvinutý firmou Adobe pro ukládání dokumentů nezávisle na softwaru i hardwaru.
PFX	Personal inFormation eXchange - znamená výměnu osobních informací, přípona.
PIN	Personal identification number - znamená osobní identifikační číslo.
PKCS	Je standard pro podepsané nebo šifrovaná data.
PKI	Public Key Infrastructure je v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly.
Podstoupení rizika	Znamená, že přijetím bereme ztráty nebo prospěch ze zisku vyplývajícího z nějakého rizika, v rámci informatiky jsou uvažovány pouze negativní rizika.
Provozní mód	Technický termín, označuje nějaký režim, prostředí, ve kterém se pracuje, stanovuje způsob práce.
Přenos rizik	Je sdílení nákladů ze ztrát s jinou stranou nebo sdílení prospěchu ze zisku vyplývajícího z rizika, v rámci informatiky jsou uvažovány pouze negativní dopady.
Redukce rizik	Je činnost ke snížení pravděpodobnosti, negativních následků nebo obou těchto parametrů spojených s rizikem.
Riziko bezpečnosti informací	Je možnost, že určitá hrozba využije zranitelnost aktiva nebo skupiny aktiv a způsobí škodu organizaci. Je stanoveno na základě kombinace pravděpodobnosti dané události a jejich následků.
Role	Je souhrn činností, funkcí, poslání, potřebných autorizací pro subjekt působící v zabezpečených systémech.
Řízený přístup	Je vlastně omezení, kdy do systému má přístup jen autorizovaný subjekt. Jeho funkce: 1) Trvalé spojení subjektu a objektu

Pojem	Výklad
	s bezpečnostním atributem, jež pro subjekt vyjadřuje úroveň oprávnění. 2) Ochrana integrity bezpečnostního atributu. 3) Bezpečnostní správce může pouze provádět změny bezpečnostních atributů subjektů a objektů. 4) Zachovávání atributů při kopírování objektu systému. 5) Subjekt může číst v objektu pouze tehdy, má-li oprávnění stejná, nebo vyšší než je stupeň utajení objektu. 6) Subjekt může zapisovat do objektu pouze tehdy, má-li stejná nebo nižší oprávnění než stupeň utajení objektu.
Skupinové politiky	Jsou to principy a zásady, které můžete uplatnit na určitou skupinu. Skupinové politiky umožňují přiřadit zásady skupiny pro malý počet objektů domény, aniž by ovlivňovaly zbytek domény. To umožňuje spravovat odděleně jednotlivé části organizace podle její hierarchie.
Správce informačního systému	Je pracovník správy informačního nebo komunikačního systému zajišťující požadované funkčnosti systémů a řízení jejich provozů.
SSL	Secure Sockets Layer, SSL je doslova vrstva bezpečných socketů, protokol, resp. vrstva vložená mezi vrstvu transportní například TCP/IP a aplikační například HTTP.
Stupně utajení	Utajované informace jsou klasifikované stupněm utajení: PŘÍSNĚ TAJNÉ zkratka „PT“, TAJNÉ „T“, DŮVĚRNÉ „D“ a VYHRAZENÉ „V“. Obdobným způsobem rozdělujeme i zabezpečené oblasti, ty jsou následně děleny na třídy: třída I - zde dochází k seznámení s utajovanými informacemi a třída II - v této oblasti nedochází k seznámení.
Subjekt informačního systému	Je aktivní prvek informačního systému, který zajišťuje předání informací mezi objekty daného systému.
TCP	Transmission Control Protocol je jedním ze základních protokolů sady protokolů Internetu.
Utajované informace	Utajovaná informace je jakákoliv informace označená v souladu se zákonem 412/2005 Sb., jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky a je uvedena v seznamu utajovaných informací.
Uživatel	Je fyzická osoba nakládající s utajovanými informacemi v informačním systému, nebo zajišťující přenos utajovaných informací v komunikačním systému.
Volitelný řízený	Je omezení přístupu subjektů do systémů, je založený na kontrole

Pojem	Výklad
přístup	přístupových práv, přičemž každý, kdo má přístupová práva může zvolit, na které další subjekty tato přístupová práva budou přenesena.
Vyhnutí se riziku	Rozhodnutí nedopustit zapojení se do rizikových situací, nebo je sloučit.
WINS	Windows Internet Naming Service - WINS je MS implementace NetBIOS Name Serveru - NBNS pro Windows.
X.509	V kryptografii je **X.509** standard pro systémy založené na veřejném klíči PKI.

SEZNAM PLATNÝCH PRÁVNÍCH PŘEDPISŮ

Obecně závazné předpisy upravující oblast ochrany utajovaných informací

Tab. 9 Právní předpisy upravující oblast ochrany utajovaných informací

	Název právních předpisů
1	Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, v platném znění, aktuálním znění - nařízení vlády 240/2008 Sb.
2	Vyhláška Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.
3	Vyhláška Národního bezpečnostního úřadu č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací.
4	Vyhláška Národního bezpečnostního úřadu č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.
5	Vyhláška Národního bezpečnostního úřadu č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), v platném znění, aktuálním znění - vyhláška 11/2008 Sb.
6	Vyhláška Národního bezpečnostního úřadu č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí - vyhláška o personální bezpečnosti.
7	Vyhláška Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, v platném znění, aktuálním znění - vyhláška č. 19/2008 Sb.
8	Vyhláška Národního bezpečnostního úřadu č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, v platném znění, aktuálním znění - vyhláška č. 55/2008 Sb.
9	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v platném znění, v aktuálním znění - zákon 119/2007, 177/2007, 296/2007, 32/2008, 255/2011 Sb.
10	Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti - změnový zákon.

Ostatní obecně závazné právní předpisy mající vztah k dané problematice

Tab. 10 Ostatní obecně závazné právní předpisy mající vztah k dané problematice

Pořadí	Název právních předpisů
1	Bezpečnostní strategie České republiky ze dne 8. Září 2011.
2	MP-USB Metodický pokyn Národního bezpečnostního úřadu, o používání Firmware a USB portů a bezpečnostní aspekty paměti typu „flash“.
3	Nařízení vlády č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska elektromagnetické kompatibility.
4	Zákon 89/1995 Sb., o státní statistické službě.
5	Zákon č. 1/2000 Sb., o ochraně osobních údajů a změně některých zákonů.
6	Zákon č. 106/1999 Sb., o svobodném přístupu k informacím.
7	Zákon č. 110/1998 Sb., o bezpečnosti české republiky ve znění zákony č. 300/2000 Sb.
8	Zákon č. 133/1985Sb., o požární ochraně.
9	Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, v platném znění.
10	Zákon č. 222/1999 Sb., o zajišťování obrany České republiky.
11	Zákon č. 227/2000 Sb., o elektronickém podpisu.
12	Zákon č. 239/2000 Sb., o integrovaném záchranném systému.
13	Zákon č. 240/2000 Sb., o krizovém řízení (krizový zákon) a o změně některých zákonů.
14	Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy.
15	Zákon č. 254/2000 sb., o auditorech.
16	Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.
17	Zákon č. 283/1991 Sb., o Policii České republiky.
18	Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů.
19	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
20	Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.
21	Zákon č. 513/1991 Sb., obchodní zákoník - Díl V: obchodní tajemství.

Pořadí	Název právních předpisů
22	Zákon č. 59/2006 Sb., o prevenci závažných havárií.

Seznam technických norem

Tab. 11 Seznam technických norem

Pořadí	**Název technických norem**
1	ČSN BS 7799-2 Systém managementu bezpečnosti informací - Specifikace s návodem pro použití.
2	ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace.
3	ČSN CLC/TS 50131-7. Poplachové systémy – Poplachové zabezpečení a tísňové systémy – Část 7: Pokyny pro aplikace.
4	ČSN EN 50131-1. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky.
5	ČSN EN 50131-7. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace.
6	ČSN EN ISO 9001 Systém managementu kvality.
7	ČSN ISO/IEC 13335-1 Informační technologie: Směrnice pro řízení bezpečnosti IT - část 1. : Pojetí a modely bezpečnosti IT.
8	ČSN ISO/IEC 13335-2 Informační technologie: Směrnice pro řízení bezpečnosti IT - část 2. : Řízení a plánování bezpečnosti IT.
9	ČSN ISO/IEC 13335-3 Informační technologie - Směrnice pro řízení bezpečnosti IT - část 3. : Techniky pro řízení bezpečnosti IT.
10	ČSN ISO/IEC 13335-4: Informační technologie – Směrnice pro řízení bezpečnosti IT – část 4. – Ochranná opatření.
11	ČSN ISO/IEC 14001 Systémy environmentálního managementu - Požadavky s návodem pro použití - pro oblast informačních technologií.
12	ČSN ISO/IEC 15408-1 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a všeobecný model.
13	ČSN ISO/IEC 15408-2 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční požadavky.
14	ČSN ISO/IEC 15408-3 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Požadavky na záruky bezpečnosti.
15	ČSN ISO/IEC 17799 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

Pořadí	Název technických norem
16	ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní politiky - Systémy managementu bezpečnosti informací – Požadavky.
17	ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní politiky - Řízení rizik bezpečnosti informací.
18	ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní politiky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
19	ČSN P ENV 1627 Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Požadavky a klasifikace.

Seznam zásad

Tab. 12 Seznam zásad

Pořadí	Název zásady
1	Advanced Encryption Standard - AES je standard pro symetrickou blokovou šifru.
2	Common Criteria for Information Technology Security Evaluation http://www.commoncriteriaportal.org/.
3	Data Encryption Standard – DES je standard pro symetrické šifry.
4	Industry Standard Architecture – ISA je standard počítačové sběrnice.
5	Standard Generalized Markup Language - SGML, nebo také Extensible Markup Language XML.

Seznam mezinárodních standardů

Tab. 13 Seznam mezinárodních standardů

Pořadí	Název mezinárodního standardu
1	External Networks managed by the General Secretariat of the Counsil of the E. U., General description, Version 1.0, 28/02/2003 o správě externích sítí.
2	ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management, českým překladem je ČSN ISO/IEC 27005.
3	Regulation (EC) No 1049/2001 of the European Parliament and of the Counsil of 30 May 2001 regarding public assess to European Parliament,

Pořadí	Název mezinárodního standardu
	Council and Commission documents. Nařízení ohledně přístupu veřejnosti k informacím.
4	Rozhodnutí rady EU ze dne 10. února 2004, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady 2004/194/ES.
5	Rozhodnutí rady EU ze dne 12. července 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady 2005/571/ES.
6	Rozhodnutí rady EU ze dne 18. Června 2007, kterým se mění rozhodnutí rady 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady 2007/438/ES.
7	Rozhodnutí rady EU ze dne 19. března. 2001, kterým se přijímají bezpečnostní předpisy 2001/264/ES - Council Decision of 19 March 2001 adopting the Counsil's security regulations.
8	Rozhodnutí rady EU ze dne 20. prosince 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady 2005/952/ES.
9	Rozhodnutí Rady o bezpečnostních pravidlech na ochranu utajovaných informací EU 6952/2/2011.
10	Rules and Procedures applicable to the transmission of Official Document (via the U32MAIL systém), V1.3, 23/09/2003 Pravidla a postupy použitelné pro předávání oficiálního dokumentu prostřednictvím systému U32MAIL.
11	Sdělení generálního tajemníka C-M(2002)49 - Bezpečnost v rámci organizace Severoatlantické smlouvy ze dne 17. června 2002. Tento dokument byl novelizován a doplněn C-M(2002)49-COR3, C-M(2002)49-COR7, C-M(2002)49-COR8. Součástí C-M(2002)49 jsou Směrnice k otázkám personální bezpečnosti AC/35-D/200, Směrnice k otázkám fyzické bezpečnosti – AC/35-D/2001, Směrnice k otázkám bezpečnosti informací – AC/35/D/2002, Směrnice průmyslové bezpečnosti – AC/35-D/2003, Směrnice k otázce INFOSEC – AC/35-D/2004 a Řídící směrnice INFOSEC pro CIS – AC/35-D/2005.

SEZNAM OBRÁZKŮ, TABULEK A PŘÍLOH

Seznam obrázků

Seznam tabulek

Seznam příloh

PŘÍLOHY

PŘÍLOHA I: Seznam provozní dokumentace

Tab. 14 Seznam provozní dokumentace

Číslo	Svazek	Název dokumentu	Stupeň utajení
0	A	Seznam dokumentů	N
		Provozní bezpečnostní dokumentace	
I	A	Základní dokument	N
II	A	Výsledky analýzy rizik	V
III	A	Bezpečnostní politika	D
IV	A	Provozní bezpečnostní směrnice pro bezpečnostního správce	N
V	A	Provozní bezpečnostní směrnice pro správce IS	N
VI	A	Provozní bezpečnostní směrnice pro obsluhu kryptografického prostředku	D
VII	A	Provozní bezpečnostní směrnice pro uživatele IS	N
VIII	A	Provozní směrnice správce IS	N
IX		Provozní směrnice pro obsluhu kryptografického prostředku	N
X	A	Provozní směrnice uživatele	N
XI	A	Seznam příloh k provozním bezpečnostním směrnicím	N
01	A	Formulář A k PBS správce: Provozní a bezpečnostní správa I	N
02	A	Formulář B k PBS správce: Žádost o zřízení / zrušení účtů	N
03	A	Formulář C k PBS správce: Prohlášení uživatele o seznámení a porozumění provozní bezpečnostní směrnici informačního systému.	N
04	A	Formulář D k PBS správce: Hlášení bezpečnostního incidentu	N
05	A	Formulář E k PBS správce: Seznam aktiv	N
06	A	Formulář F k PBS správce: Seznam čísel pečetí na zařízeních	N

Číslo	Svazek	Název dokumentu	Stupeň utajení
07	A	Formulář G k PBS správce: Záznam o provedení auditu na zařízeních	N
08	A	Formulář H k PBS správce: Záznam o provedeném školení	N
09	A	Formulář I k PBS správce: Záznam o provedené kontrole IS	N
10	A	Formulář J k PBS správce: Protokol o převzetí čipové karty s klíči	N
11	A	Formulář L k PBS správce: Pokyny k protokolu převzetí čipové karty s klíči	N
12	A	Příloha A k PBS Uživatele: Tabulka pro převod označování informací z EU	N
		Projektová dokumentace	
XII	B	Bezpečná doména	N
XIII	B	Server v bezpečné doméně	N
XIV	B	Pracovní stanice bezpečné domény	N
XV	B	Komunikační infrastruktura bezpečné domény	N
XVI	B	Infrastruktura PKI	N
XVII	B	Antivirová ochrana	N
XVIII	B	Vyhodnocení logů	N
XIX	B	Evidence a změna hesel lokálních administrátorů	N
XX	B	Zálohování a archivace	N
XXI	B	Bezpečnostní testy	N
		Projektová dokumentace IS-ATOBEZ-UI	
XXII	C	IS-ATOBEZ-UI Základní dokument	N
XXIII	C	IS-ATOBEZ-UI Příručka uživatele	N
XXIV	C	IS-ATOBEZ-UI Příručka administrátora	N
XXV	C	IS-ATOBEZ-UI Instalační administrátorská příručka	N
XXVI	C	IS-ATOBEZ-UI Konfigurační list serveru	N
XXVII	C	IS-ATOBEZ-UI Konfigurační list Switch	N
XXVIII	C	IS-ATOBEZ-UI Konfigurační list pracovní stanice	N

Číslo	Svazek	Název dokumentu	Stupeň utajení
XXIX	C	IS-ATOBEZ-UI Konfigurační list tiskárny	N
XXX	C	Popis uživatelských rolí	N
		Podpora certifikace	
XXXI	C	Žádost o certifikaci informačního systému	N

PŘÍLOHA II: Kalkulace

Ceny v kalkulacích jsou uvedeny v korunách bez DPH. Všechny kalkulace, vyjma kalkulace fyzické bezpečnosti, byly vytvořeny dne 26. 9. 2011. Pokud ceny byly výrobcem nebo distributorem uvedeny EURu, byl pro přepočet na koruny použit kurz ČNB ze dne 26. 9. 2011, který činil 24,68 Kč za 1 EUR, tento kurz byl zaokrouhlen na 25,00 Kč, obdobným způsobem byl použit kurz pro USD, který dle ČNB ve výše uvedeném dni byl 18,29 Kč za 1 USD, tento kurz byl zaokrouhlen na 18,50 Kč. Kalkulace fyzické bezpečnosti byla vytvořena až 6. 2. 2011, podle nového platného seznamu certifikovaných technických prostředků NBÚ.

PŘÍLOHA III: Kalkulace kabeláže, rozbočovače, aktivních prvků

Tab. 15 Kalkulace kabeláže, rozbočovače a aktivních prvků

P/N	Název	Cena za kus	Cena bez DPH
	1x Belden, zásuvky, žlaby*	450.000 Kč	450.000 Kč
	1x Elektrické rozvody**	120.000 Kč	120.000 Kč
93072PX	1x IBM S2 25U Standard Rack Cabinet	24.024 Kč	24.024 Kč
40K5376	1x IBM Keyboard with Integrated Poiting Device – 3m Cable – Black – USB	3.336 Kč	3.336 Kč
1723E7X	1x IBM 1U 17in Flat Panel Monitor Console Kit w/o keyboard	24.830 Kč	24.830 Kč
40K8785	1x IBM 1,5m Blue Cable	546 Kč	2.184 Kč
39Y7937	1x IBM 1,5m, 10A/100-250V Rack Power Cable	338 Kč	1.690 Kč

P/N	Název	Cena za kus	Cena bez DPH
53951KX	1x IBM 1500VA LCD 2U Rack UPS 230V	14.950 Kč	14.950 Kč
66300100	2x Juniper 24 Port 1GB EX2200 Ethernet Switch for IBM Systém X	32.410 Kč	64.820 Kč
51J8899	2x 3 Year Onsite Repair 24x7 4 Hour Responze	4.809 Kč	9.618 Kč
96P1565	1x IBM 19inch Rack Mount Kit	2.457 Kč	2.457 Kč
Celkem			**717.909 Kč**

*Na každý počítač je vymezeno 30 m kabelu, žlabu a jedna zásuvka s dvěma vývody, tzn. 45 Kč za 1 m obyčejného bílého žlabu, 10 Kč za 1 m kabelu a 15 Kč za 1 m práce to se rovná 70 Kč na 1 m, tj. 2.100 Kč na jeden počítač, tj. 273.000 Kč na všechny PC. Plně osazená zásuvka je cca za 400 Kč, celkem to je 5.200 Kč. Zbytek do celé částky položky 450.000 Kč, tj. 171.800 Kč je bráno jako rezerva do kabeláže.

**V každé budově většinou nějaký elektrický rozvod je, takže suma 120.000 Kč je na případné rozšíření a úpravu elektrického rozvodu.

PŘÍLOHA IV: Kalkulace serveru

Tab. 16 Kalkulace serveru

P/N	Název	Cena za kus	Cena bez DPH
7944K3G	1x IBM x3550 M3, Xeon 4C E5620 80w 2.40GHz/1066MHz/12MB, 1x4GB, O/Bay HS 2.5in SAS/SATA, SR M5014, 675W p/s, Rack	33.542 Kč	33.542 Kč
49Y3744	1x IBM Intel Xeon 4C Processor Model E5620 80W 2.40GHz/1066MHz/12M	11.804 Kč	11.804 Kč
49Y3757	5x IBM 4GB (1x4GB, Dual Rankx8) PC3-10600 CL9 ECC DDR3-1333MHz LP RDIMM	2.571 Kč	12.855 Kč
90Y4550	6x IBM 2GB (1x2GB, 1Rx8, 1.35V) PC3L-10600 CL9 ECC DDR3 1333MHz LP RDIMM	1.638 Kč	9.828 Kč
44W2193	4x IBM 300 GB 2.5in SFF Slim-HS 10K 6Gbps SAS HDD	6.120 Kč	24.480 Kč

P/N	Název	Cena za kus	Cena bez DPH
59Y3952	1x IBM System x3550 M3 R2 ODD Kit	1.014 Kč	1.014 Kč
49Y3725	1x IBM 3Gb SAS HBA Controller v2	3.900 Kč	3.900 Kč
49Y3717	1x IBM Dual Port 1Gb Ethernet Daughter Card	1.365 Kč	1.365 Kč
49Y3704	1x IBM 675W Redundant Power Supply	4.836 Kč	4.836 Kč
49Y3715	1x IBM Ultraslim Enhanced SATA Multi-Burner	1.924 Kč	1.924 Kč
41W9368	1x IBM 3 Year Onsite Repair 24x7 24 Hour Committed Service CS	4.073 Kč	4.073 Kč
OM3121	1x HID Omnikey 2121 USB	690 Kč	690 Kč
C700	1x HID Crescendo C700	650 Kč	650 Kč
P73-04982	3x WinSvrStd 2008R2 SNGL OLP NL	17.700 Kč	53.100 Kč
228-09421	1x SQL SvrStd 2008R2 SNGL OLP NL	21.900 Kč	21.900 Kč
0E7IOZF0-BI1EA	1x Symantec Endpoint Protection 12.1 per user BNDL STD LIC Express Band A Basic 12 Months	1.150 Kč	1.150 Kč
	1x Adiscon MonirWare Console	2.200 Kč	2.200 Kč
Celkem			**189.311 Kč**

PŘÍLOHA V: Kalkulace zálohování

Tab. 17 Kalkulace zálohování

P/N	Název	Cena za kus	Cena bez DPH
3580S5E	1x IBM System Storage TS2250 Tape Drive Express Model H5S	52.104 Kč	52.104 Kč
96P1565	1x IBM 19inch Rack Mount Kit	2.457 Kč	2.457 Kč
46C2084	5x IBM Ultrium 5 Data Cartridge 5 – pack	15.002 Kč	75.010 Kč
95P4713	1x IBM 2M Mini-SAS/Mini-SAS 1x	1.911 Kč	1.911 Kč

P/N	Název	Cena za kus	Cena bez DPH
	Cable		
44T5892	1x IBM 3 Year Onsite Repair 9x5 Same Business Day	13.171 Kč	13.171 Kč
20095933	1x Symantec Backup Exec 2010 Server WIN per Server BNDL XGRD LIC from BEQS Band S Basic 12 Months	11.500 Kč	11.500 Kč
20056831	2x Symantec Backup Exec 2010 Agent for Windows Systems WIN per Server BNDL STD LIC Band S Basic 12 Months	9.468 Kč	18.936 Kč
20057903	1x Symantec Backup Exec 2010 Agent for MSFT SQL WIN per Server BNDL STD LIC Express Band S Basic 12 Months	15.869 Kč	15.869 Kč
Celkem			**190.958 Kč**

PŘÍLOHA VI: Kalkulace pracovní stanice

Tab. 18 Kalkulace pracovní stanice

P/N	Název	Cena za kus	Cena bez DPH
57300376	13x Lenovo IdeaCentre AIO A320-1 i3-2310M/2GB/500GB/21,5" FHD/WIN7HP64bit	18.999 Kč	246.987 Kč
T48HNEU	13x Lenovo ThinkVision L1951p - LCD display - TFT - 19" - široká obrazovka - 1440 x 900 / 75 Hz - 250 cd/m2 - 1000:1 - 5 ms - 0.285 mm - DVI-D, VGA - obchodní čerň – TopSeller	3.500 Kč	45.500 Kč
OM3121	13x HID Omnikey 2121 USB	690 Kč	8.970 Kč
C700	13x HID Crescendo C700	650 Kč	8.450 Kč
R18-02729	13x WinSvrCAL 2008 SNGL OLP NL DvcCAL	720 Kč	9.360 Kč
0E7IOZF0-	13x Symantec Endpoint Protection 12.1 per user BNDL STD LIC Express BAND	1.150 Kč	14.950 Kč

P/N	Název	Cena za kus	Cena bez DPH
BI1EA	A Basic 12 Months		
SodatwOpt	13x OptimmAccess	1.150 Kč	14.950 Kč
ICZPW	13x Protect for Windows	4.500 Kč	58.500 Kč
021-09707	13x Office Std. 2010 SNGL OLP NL	9.100 Kč	118.300 Kč
65086209	13x Adobe Acrobat X Standard	8.390 Kč	109.070 Kč
Celkem			**635.037 Kč**

PŘÍLOHA VII: Kalkulace stanice s kryptografickým prostředkem

Tab. 19 Kalkulace stanice s kryptografickým prostředkem

P/N	Název	Cena za kus	Cena bez DPH
	1x Faktura od SÚJB a proměřenou stanic včetně kryptografického prostředku a včetně SW	144.438 Kč	144.438 Kč
Celkem			**144.438 Kč**

PŘÍLOHA VIII: Kalkulace síťové tiskárny

Tab. 20 Kalkulace síťové tiskárny

P/N	Název	Cena za kus	Cena bez DPH
CF083A#B19	1x HP LaserJet Enterprise 500 color M551xh, A4, 32/32str./min, USB 2.0, Ethernet, Duplex, 500GB HD	24.700 Kč	24.700 Kč
Celkem			**24.700 Kč**

PŘÍLOHA IX: Kalkulace fyzické bezpečnosti

Tab. 21 Kalkulace fyzické bezpečnosti

Identifikační číslo TP dle NBÚ	Název, označení a výrobce	Cena za kus	Cena bez DPH
T0072/2009	16x OMO 1K/3 Ocelová mříž jednokřídlová pro běžné okno od výrobce AŽD Praha s.r.o.	12.000 Kč	192.000 Kč

Identifikační číslo TP dle NBÚ	Název, označení a výrobce	Cena za kus	Cena bez DPH
T0045/2009	3x MRB Sazovice Bezpečnostní dveře BEDEX Vario V3 s jednokřídlové 900x2000	13.290 Kč	39.870 Kč
	3x Rozvorový zámek MUL-T-LOCK typ lock case 235	3.135 Kč	9.405 Kč
T0022/2010	3x Cylindrická vložka MUL-T_LOCK Typ 7x7 30x45	805 Kč	2.415 Kč
	3x Sjednocení vložek 7x7	185 Kč	555 Kč
	3x Samozavírač MUL-T-LOCK – model HE 24, včetně ramene	1.220 Kč	3.660 Kč
T0081/2010	3x Bezpečnostní přídavné kování R1 od firmy ROSTEX Vyškov	2.385 Kč	7.155 Kč
T0093/2010	3x Bezpečnostní zárubeň pro dveře BEDEX Vario V3 k zabetonování nebo zazdění	2.330 Kč	6.990 Kč
TP090/2009	1x Ústředna EZS – TP- 4-20 GSM od výrobce Tecnoalarm	11.888 Kč	11.888 Kč
T1092/2009	16x Detektor pohybu IR 2000 od výrobce Tecnoalarm	736	11.776 Kč
	4x TP-020-LCD Klávesnice s indikací LED a LCD Displejem od výrobce Tecnoalarm	3.462 Kč	13.848 Kč
	4x záložní baterie 7Ah	450 Kč	1.800 Kč
	480x 1m Lankový kabel s napájecím párem pro rozvody EZS, 6 vodičů od výrobce Tecnoalarm*	15 Kč	7.200 Kč
T00978/2009	1x Mobilní skříňový trezor TLA 13 od výrobce P-KOVO Brno s.r.o.	49.920 Kč	49.920 Kč
	1x Instalace	216.000 Kč	216.000 Kč
Celkem			**574.482 Kč**

*Na každé čidlo je počítáno 30 m kabelu.

PŘÍLOHA X: Kalkulace instalace a podpory

Tab. 22 Kalkulace instalace a podpory

P/N	Název	Cena za kus	Cena bez DPH
	1x Položení a proměření kabeláže	150.000 Kč	150.000
	1x Instalace a konfigurace Switche	60.000 Kč	60.000
	1x Instalace Serveru a jeho zahoření	20.000 Kč	20.000
	1x Instalace VMware a Windows a SQL včetně bezpečnosti	250.000 Kč	250.000
	1x Instalace CA a PKI	150.000 Kč	150.000
	1x Instalace zálohování	80.000 Kč	80.000
	1x Instalace pracovních stanic	3.000 Kč	39.000
	1x Instalace síťové tiskárny	20.000 Kč	20.000 Kč
	1x Instalace bezpečnostních testů	120.000 Kč	120.000 Kč
	1x Podpora od SÚJB k počítačové stanici s kryptografickým prostředkem 12 měsíců	54.000 Kč	54.000 Kč
Celkem			**943.000 Kč**

PŘÍLOHA XI: Kalkulace školení

Tab. 23 Kalkulace školení

P/N	Název	Cena za kus	Cena bez DPH
	33x Školení uživatelů	8.500 Kč	280.500 Kč
	1x Školení bezpečnostního správce	60.000 Kč	60.000 Kč
	1x Školení správce informačního systému	60.000 Kč	60.000 Kč
	1x Školení obsluhy pracovní stanice s kryptografickým prostředkem	12.000 Kč	12.000 Kč
Celkem			**412.500 Kč**

PŘÍLOHA XII: Kalkulace instalační dokumentace

Tab. 24 Kalkulace instalační dokumentace

P/N	Název	Cena za kus	Cena bez DPH
	1x Instalační dokumentace ke kabeláži	60.000 Kč	60.000 Kč
	1x Instalační dokumentace ke switchi	20.000 Kč	20.000 Kč
	1x Instalační dokumentace k CA a PKI	80.000 Kč	80.000 Kč
	1x Instalační dokumentace k serveru	150.000 Kč	150.000 Kč
	1x Instalační dokumentace k zálohování	40.000 Kč	40.000 Kč
	1x Instalační dokumentace k pracovním stanicím	20.000 Kč	20.000 Kč
	1x Dokumentace od SÚJB k pracovní stanici s kryptografickým prostředkem	80.000 Kč	80.000 Kč
Celkem			**450.000 Kč**

PŘÍLOHA XIII: Seznam hrozeb

Tab. 25 Seznam hrozeb

Typ	Hrozby
Fyzické poškození	Požár, poškození vodou, znečištění, závažná nehoda, zničení zařízení nebo médií, prach, koroze, zamrznutí.
Přírodní události	Klimatický jev, seizmický jev, sopečný jev, meteorologický jev, povodeň.
Ztráta základních služeb	Selhání klimatizace, přerušení dodávky elektřiny, selhání telekomunikačního zařízení.
Poruchy způsobené zářením	Elektromagnetické záření, termální záření, elektromagnetické impulzy.
Ohrožení informací	Zachycení kompromitujících interferenčních signálů, vzdálená špionáž, odposlech, krádež médií nebo dokumentů, krádež zařízení, zprovoznění recyklovaných nebo vyřazených vybavení, vyzrazení, data pocházející z nedůvěryhodných zdrojů, falšování

Typ	Hrozby
	pomocí technického vybavení, falšování pomocí aplikačního vybavení.
Technická selhání	Selhání zařízení, chybné fungování zařízení, přetížení informačního systému, chybné fungování aplikačního programového vybavení, chyba údržby.
Neoprávněné činnosti	Neoprávněné použití zařízení, podvodné kopírování aplikačního programového vybavení, použití padělaného nebo zkopírovaného aplikačního vybavení, poškození dat, nezákonné zpracování dat.
Ohrožení funkčnosti	Chyba v používání, zneužití oprávnění, falšování zpráv, odepření činnosti, nedostatek personálu.
Hacker, cracker	Hacking, sociální inženýrství, narušení a prolomení systému, neoprávněný přístup do systému.
Počítačová kriminalita	Počítačový zločin například kybernetické pronásledování, podvodné jednání například odpovídání, imitace, zachycení), získání informací za úplatu, spoofing, průnik do systému.
Terorismus	Bombové útoky/terorismu, informační válka, útok na systém například útok odmítnutí služby - DoS, průnik do systému, porušení systému.
Průmyslová špionáž - zpravodajské služby, společnosti, zahraniční vlády, ostatní vládní zájmy	Vojenské zvýhodnění, politické zvýhodnění, ekonomické zvýhodnění, krádež informací, průnik do soukromí, sociální inženýrství, neoprávněný přístup do systému - přístup ke klasifikovaným aktivům a technologickým informacím.
Interní pracovníci - špatně zaškolení, nespokojení, škodolibí, nedbalí, nečestní nebo zaměstnanci s ukončeným pracovním poměrem	Napadení zaměstnance, vydírání, prohlížení chráněných informací, zneužití počítačů, podvod, krádež, získání informací za úplatu, vložení falešných nebo upravených dat, narušení komunikace, škodlivý kód například virus, logická bomba, trojský kůň, prodej osobních počítačů, chyby v systému, průnik do systému, sabotáž systému, neoprávněný přístup do systému.