JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Katedra aplikované matematiky a informatiky

DIPLOMOVÁ PRÁCE

SROVNÁVACÍ STUDIE PROVEDITELNOSTI INFORMAČNÍCH SYSTÉMŮ PRO NAKLÁDÁNÍ S UTAJOVANÝMI INFORMACEMI DO STUPNĚ UTAJENÍ DŮVĚRNÉ V OBLASTI INFORMAČNĚ TECHNOLOGICKÉ A EKONOMICKÉ

Vypracoval: Hana Huličová
Vedoucí práce: doc. Ing Ladislav Beránek. CSc.
České Budějovice 2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

PROHLÁŠENÍ

Prohlašuji, že svoji diplomovou práci jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce a to – v nezkrácené podobě – elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Dne:……. ……

Hana Huličová

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc. Ing. Ladislavu Beránkovi, CSc. za cenné rady, připomínky a metodické vedení práce. Děkuji za specializované konzultace Ing. Marie Švarcové, PhD. a Ing. Antonína Šmejkala PhD.

ABSTRAKT V ČESKÉM JAZYCE

HULIČOVÁ, H. (2015). Srovnávací studie proveditelnosti informačních systému pro nakládání s utajovanými informacemi do stupně utajení důvěrné v oblasti informačně - technologické a ekonomické: diplomová práce. In: Jihočeská univerzita v Českých Budějovicích: Ekonomická fakulta. (pp. 131). České Budějovice: Jihočeská univerzita.

Klíčová slova: studie proveditelnosti, informační systém, utajované informace, fyzická bezpečnost, personální bezpečnost, administrativní bezpečnost, lidské zdroje, průmyslová bezpečnost, bezpečnost IS, bezpečnostní dokumentace, analýza rizik, ekonomická analýza, finanční analýza, náklady, investiční náklady, provozní náklady.

Diplomová práce se zabývá návrhem a srovnávací studie proveditelnosti informačního systému pro nakládání s utajovanými informacemi do stupně utajení důvěrné v oblasti informačně technologické a ekonomické tj. ekonomické a finanční analýze.

ABSTRAKT V ANGLICKÉM JAZYCE

HULIČOVÁ, H. (2015). Comparative study of feasibility of information systems handling classified information up to the CONFIDENTIAL level in the area of information-technological and economical: thesis. In: South Bohemian University in České Budějovice: Faculty of Economics. (pp. 131). České Budějovice: Bohemian Univerzity.

Keywords: feasibility study, information system, classified information, physical security, personnel security, administrative security, human resources, industrial safety, IS security, security documentation, risk analysis, economic analysis, financial analysis, costs, capital costs, operating costs.

This thesis deals with the design of a comparative study of the feasibility of an information system handling classified information up to the Confidebtial level in the information-technological and economic area - i.e. economical and financial analysis.

OBSAH

1 ÚVOD

Diplomová práce se zabývá srovnávací studií proveditelnosti informačních systémů pro nakládání s utajovanými informacemi do stupně utajení Důvěrné v oblasti technologické a ekonomické. Toto téma jsem si vybrala proto, že oblast bezpečnosti obecně je v poslední době vysoce aktuální a v oblasti informačních systémů obzvláště. Některé organizace a společnosti se přesto stále domnívají, že opatření v boji proti potenciálním hrozbám a rizikům jsou přehnaná a opatření, která vyžaduje např. zákon o kybernetické bezpečnosti, jsou pro ně překážkou v práci a přináší jim zvýšené náklady. Mezinárodní společenství a organizace jako je Evropská unie a NATO, včetně jejich jednotlivých členských států proto normativně stanovují podmínky pro využívání informačních systémů k nakládání s utajovanými informacemi. Systém takovýchto pravidel zajišťuje bezpečné zpracování, přenos a úschovu elektronických dat komplexně, tj. nejen z pohledu bezpečnosti informačních a komunikačních systémů a systému kryptografické ochrany, ale i z pohledu bezpečnosti personální, průmyslové, administrativní a fyzické. Takovýmto způsobem je zajištěn komplexní systém ochrany utajovaných informací. Tyto normativní podmínky však mohou být vodítkem a inspirací pro všechny, komu záleží na ochraně dat i neutajovaného charakteru - organizací, společností, tak domácností. Protože, jak bylo naznačeno, takováto opatření znamenají i zvýšené náklady na pořízení a provozování daného informačního systému je účelné zpracovat před realizací takovéhoto bezpečného informačního systému srovnávací studii proveditelnosti. Ve studii proveditelnosti se definují různé možnosti řešení a jejich socioekonomickým posouzením se navrhne nejefektivnější řešení pro daný případ.

Srovnávací studie proveditelnosti se musí stát hlavním zdrojem informací v oblasti technologické, organizační a ekonomické pro rozhodování o nejvhodnějším řešení dané problematiky, které bude splňovat normativně dané podmínky pro zpracování utajovaných informací příslušného stupně utajení. Základním předpokladem pro vytvoření efektivního funkčního a bezpečného informačního systému je detailní popis stávajícího stavu, požadovaného cíle a jednotlivých variant řešení. Dobře zpracovaná srovnávací studie je předpokladem bezproblémové certifikace informačního systému Národním bezpečnostním úřadem a ekonomického zajištění akce nejen v období pořízení systému, ale i jeho provozování po celý jeho životní cyklus.

2 CÍLE DIPLOMOVÉ PRÁCE

Hlavním cílem diplomové práce je vypracování srovnávací studie proveditelnosti pro vytvoření informačních systémů pro nakládání s utajovanými informacemi do stupně utajení Důvěrné v oblasti informativně technologické a ekonomické, která má sloužit jako podklad pro rozhodování v oblasti finanční a ekonomické a v oblasti technologických a bezpečnostních požadavků, které po informačním systému jsou požadovány. Jinými slovy práce má za úkol vymezit podmínky požadované legislativou v oblasti personální, průmyslové, administrativní a fyzické bezpečnosti, bezpečnosti infomačních a komunikačních systémů a kryptografické ochrany. Dílčím cílem studie proveditelnosti je provedení analýzy stávajícího stavu a analýzy potřeb organice Správy úložišť radioaktivního odpadu a na základě zjištěných skutečností, potřeb a podmínek navrhnout dvě vhodná a vyhovující technická řešení, která by prošla úspěšnou certifikací u Národního bezpečnostního úřadu.

Obě navržená technická řešení informačního systému jsou v práci podrobně popsána a jejich jednotlivé hardwarové a softwarové prvky jsou oceněny, a to jak z pohledu investičních, tak provozních nákladů. Získané výsledné hodnoty jsou dále analyzovány po stránce ekonomické a finanční. Z pohledu úplnosti a komplexnosti informací srovnávací studie proveditelnosti je práce doplněna o analýzu rizik a o slovní hodnocení silných a slabých míst jednotlivých řešení.

Úkolem diplomové práce bylo tedy vytvořit ucelený dokument, obsahující v tomto případě dvě možná řešení dané problematiky, provést ekonomickou a finanční analýzu jednotlivých variant a navrhnout nejefektivnější řešení, které umožní provozovat daný informační systém v požadovaném rozsahu, splňující kritéria pro zpracování utajovaných informací. V neposlední řadě, aby navržené řešení bylo ekonomicky výhodné.

Dílčími cíli bylo především:

1. Definovat nezbytné podmínky pro provozování informačního systému pro nakládání s utajovanými informacemi do stupně utajení Důvěrné tak, jak jsou definované v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

2. Provést detailní analýzu stávajícího stavu informačního systému provozovaného organizací, která byla použita pro potřeby této práce. Jedná se o organizační složku státu Správu úložišť radioaktivních odpadů (dále jen „SÚRAO“).
3. Provést důkladnou analýzu všech známých potřeb pro každou variantu možného řešení a souhrn všech normativních požadavků na provozování informačního systému pro zpracování utajovaných informací. Jedná se o platné právní předpisy (zákony a vyhlášky), technické normy a standardy.
4. Navrhnout dvě vhodná technická řešení zohledňující podmínky definované v bodě prvém, stávající stav v bodě druhém a potřeby organizace v bodě třetím.
5. Ocenit náklady (investiční a provozní) potřebné na vybudování a provoz navržených technických řešení a vypracovat propočet nákladů ekonomické a finanční analýzy.
6. Definovat rizika projektu, způsob jejich eliminace a slovní formulace silných tj. výhod a slabých tj. nevýhod jednotlivých technických řešení.

3 METODIKA DIPLOMOVÉ PRÁCE

Cílem diplomové práce je vytvoření studie proveditelnosti vymezující právní a věcné podmínky, jež jsou potřebné pro vybudování informačního systému umožňujícího nakládání s utajovanými informacemi do stupně utajení Důvěrné. Na základě získaných informací se navrhují dvě možná technická řešení proveditelnosti do prostředí organizace Správy úložišť radioaktivního odpadů. Výsledná technická řešení jsou podrobena finanční a ekonomické analýze, analýze rizik a slovnímu hodnocení silných a slabých míst obou řešení. Diplomovou práci dle použité metodiky je možné logicky rozdělit do pěti částí:

V první části jsou použity metody vycházející ze sběru dat, studia dokumentů, jejich rozboru a vyhodnocení a postupů stanovených platnými právními předpisy. Výsledkem analýzy sebraných materiálů v diplomové práci je teoretická část, která formuluje a zařazuje jednotlivé podmínky do příslušných částí personální, průmyslové, administrativní, fyzické bezpečnosti, bezpečnosti informačních a komunikačních systémů a kryptografické ochrany.

V druhé části mohly být získané informace aplikovány do fiktivní firmy, tuto cestu jsem však nezvolila a vybrala jsem si skutečnou organizaci Správy úložišť radioaktivního odpadu (SÚRAO), což znamenalo získané informace implementovat do živého prostředí, které samo je determinováno dalšími podmínkami, potřebami, zdroji a činnostmi. Aby práce mohla být publikována pro veřejnost, jsou některé informace v této části obecné a neodpovídající skutečné realitě organizace SÚRAO (například skutečné rozmístění zabezpečených oblastí apod.). Výsledkem této části je vytvoření analýzy stávajícího stavu (kapitola 7) a analýzy potřeb Správy úložišť radioaktivního odpadu (kapitola 8).

V třetí části jsou navrženy dvě vhodná technická řešení zohledňující podmínky definované legislativou, stávající stav a potřeby organizace s ohledem na bezpečnostní hodnocení tzv. Common Criteria (The Common Criteria, 2015). Výsledkem této části jsou: kapitola 9 Technická řešení obecně, kapitola 10 Technické řešení I. – samostatné stanice a kapitola 11 Technické řešení II. – serverové řešení. Jinými slovy v této části jsou vypracována dvě technická řešení, kde práce klade hlavní důraz na zajištění počítačové bezpečnosti a řešení datového toku do informačního systému Státního úřadu

pro jadernou bezpečnost. Z tohoto důvodu bylo nejdříve potřebné zjistit na jakých hardwarových a softwarových technologiích je možné vhodné řešení vybudovat tak, aby navržená a popsaná technická řešení mohla být zdárně certifikována Národním bezpečnostním úřadem.

Část čtvrtá definuje náklady v investiční a provozní fázi pro jednotlivá řešení. Tyto náklady jsou pak v diplomové práci analyzovány po stránce finanční a ekonomické. Výsledkem jsou: kapitola 13 Náklady (náklady v investiční fázi, náklady v provozní fázi) a kapitola 14 Ekonomická a finanční analýza, kde byly použity následující metody:

- Výpočet ekonomických přínosů a újmy.
- Diskontované DCF podle vzorce (Přehled vztahů k problematice spoření, důchody, anuitní splácení úvěrů: Pro SVŠE Znojmo):

$$v_r = \frac{1}{1+i} \; a\ rok\ následující\ v_{r+1} = \frac{v_r}{1+i}$$

- Kumulované DCF, čistá současná hodnota, v práci byly použity vzorce:

1) (Synek, 2011):

$$NPV = \sum (CF \times v)^n$$

2) (Trhfirem.cz: Partner pro prodej a akvizice malých a středních firem, 2015):

$$NVP = \frac{CF}{(1+i)^n}$$

- Index ekonomické rentability podle vzorce (Synek, 2011):

$$index\ ekonomické\ rentability = \frac{výsledek\ hospodaření\ (DCF)}{investice}$$

- Výnosnost investice ROI získáme podle vzorce (Synek, 2011):

$$výnosnost\ investice\ ROI = \frac{průměrný\ roční\ zisk}{investice} \times 100$$

- Doba návratnosti byla získána podle vzorce (Synek, 2011):

$$doba\ návratnosti = \frac{investice}{roční\ cash\ flow}$$

- Metoda diskontovaných hodnot nákladů podle vzorce (Synek, 2011):

$$diskontovaná\ hodnota\ nákladů = \frac{1 - \left(\frac{1}{1+i}\right)^{n}}{i}$$

- Metoda převedených nákladů
- Metoda součtu pořadí

Část pátá definuje rizika projektu, způsob jejich eliminace a slovní formulaci silných a slabých míst jednotlivých řešení. Výsledkem této práce je analýza rizik projektu (kapitola 15) a silná a slabá místa technických řešení (kapitola 16).

4 STUDIE PROVEDITELNOSTI

Studie proveditelnosti (Feasibility Study) je podkladová podpora pro ekonomické rozhodování, je hlavním informačním zdrojem, komplexním dokumentem projektu, jehož účelem je připravit objektivní, analýzou podložené podklady pro rozhodování. Studie proveditelnosti analyzuje investiční nebo podnikatelský záměr, jeho součástí je textová analýza projektu, analýza efektivnosti, předpověď stability projektu v čase, finanční náročnost projektu. Velké projekty obsahují i předpověď stability žadatele o úvěr. Studie proveditelnosti může obsahovat různé tematické části:

- úvodní informace,
- popis podstaty projektu a jeho etap,
- popis stávajícího stavu,
- technologické a technické řešení,
- řízení lidských zdrojů (organizace), management projektu včetně personálního řešení,
- analýza trhu, odhad poptávky, marketingová strategie a marketingový mix, tj. otázka poptávky po službě a produktu a jeho nabídky, substituty poskytované služby či produktu, samotný popis produktu a jeho cena,
- dopad projektu na životní prostředí (vyhodnocení vlivů na životní prostředí – EIA),
- ostatní podstatné charakteristiky projektu a jeho okolí (právní řešení, politická podpora…),
- zajištění finančního majetku, řízení pracovního kapitálu (oběžný majetek),
- finanční plán a analýza projektu,
- analýza společensko-ekonomických přínosů, nákladů projektu, hodnocení efektivity a udržitelnosti projektu (kvalitativní hodnocení, kvantitativní hodnocení, analýza efektivity nákladů - CEA, analýza nákladů a přínosů - CBA), zhodnocení připravenosti firmy změnu realizovat,
- risk management (analýza a řešení rizika),
- harmonogram,
- závěrečné hodnocení projektu. Výše uvedené informace jsou získány: (Sieber Uchytil s.r.o.) a (PDQM, s.r.o., 2014).

Obecně platí, že jednotlivé studie proveditelnosti se liší podle zadavatelů (soukromé, veřejnoprávní subjekty) a podle programů (výzev), jejichž pomocí se mohou některé projekty financovat, z čehož plyne, že studie proveditelnosti mají různou obsahovou stránku, metodickou náročnost a podrobnost zpracování jednotlivých kapitol.

Informační a komunikační technologie (ICT) zahrnují informační technologie používané pro komunikaci a práci s informacemi. ICT patří mezi klíčové kompetence, které se rychle vyvíjí. S rozvojem ICT, s novými technologiemi a verzemi souvisí i neustálá kontrola bezpečnosti a eliminací možných rizik. Protože finančních prostředků investovaných do ICT není nikdy dostatek, snaží se jednotlivé subjekty využívat dotací z operačních programů například:

- Ministerstvo průmyslu a obchodu České republiky: Operační program podnikání a inovace: Program podpory ICT a strategické služby (Ministerstvo průmyslu a obchodu České republiky, 2010).
- Ministerstvo vnitra České republiky: IOP - Integrovaný operační program: Výzva č. 6 – Technologická centra obcí s rozšířenou působností (Ministerstvo vnitra České republiky, 2014).
- Ministerstvo vnitra České republiky: IOP - Integrovaný operační program: Výzva č. 8 – Rozvoj služeb eGovernmentu v krajích (Ministerstvo vnitra České republiky, 2014).
- Ministerstvo vnitra České republiky: IOP - Integrovaný operační program: Výzva č. 17 - Modernizace veřejné správy: Rozvoj informační společnosti ve veřejné správě (Ministerstvo vnitra České republiky, 2014).

Všechny výše uvedené operační programy obsahují požadavky v předepsané formě, kterou žadatel musí splnit. Součástí žádosti o dotaci je studie proveditelnosti, která je tvořena především: popisem a analýzou současného stavu, návrhy technických řešení, organizací (personální a administrativní), náklady (investiční a provozní), ekonomickou a finanční analýzou, slabými a silnými místy řešení a analýzou rizik projektu.

5 PODMÍNKY DEFINOVANÉ ZÁKONEM Č. 412/2005 SB., V PLATNÉM ZNĚNÍ

Zákon č. 412/2005 Sb. upravující oblast ochrany utajovaných informací a bezpečnostní způsobilost je následně konkretizován prováděcími vyhláškami mezinárodními a českými standardy. Podmínky definované výše uvedeným zákonem, které musí každý řešitel při vybudování informačního systému pro zpracování utajovaných informací splnit, je možné rozdělit na požadavky na personální bezpečnost, průmyslovou bezpečnost, administrativní bezpečnost, fyzickou bezpečnost, bezpečnost informačních a komunikačních systému a kryptografickou ochranu.

5.1 Personální bezpečnost

V rámci personální bezpečnosti jsou stanoveny podmínky pro přístup fyzické osoby[1] k utajované informaci, kterou potřebuje k výkonu své práce jak listinné tak nelistinné povahy (Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, 2005). Personální bezpečnost definuje:

- Kdo bude mít přístup k utajovaným informacím: uživatelé splňující podmínku, že danou informaci potřebují k výkonu své práce, správce informačního systému, bezpečnostního správce, správce kryptografického prostředku aj. a dále jaké podmínky musí splňovat: např. musí být držiteli platného osvědčení fyzické osoby příslušného stupně a zároveň musí být poučeni (Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, 2005).
- Speciální požadavky na správce kryptografické ochrany, správce kryptografického materiálu a pracovníky kryptografické ochrany, kteří tvoří samostatnou kapitolu, kdy držitel platného osvědčení musí zároveň absolvovat úspěšné provedení zkoušky z odborné způsobilosti pracovníka kryptografické ochrany a jejich činnost musí být v souladu s postupy v bezpečnostní dokumentaci (Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, 2011).
- Pracovní podmínky pro uživatele, bezpečnostního správce informačního systému, správce informačního systému atd., kteří mimo podmínek definovaných v prvém

[1] Obecně platí, že fyzická osoba musí být občanem České republiky, nebo občanem členské země EU nebo daná země musí být členem NATO, je způsobilá, starší 18 let, bezúhonná a osobnostně a bezpečnostně spolehlivá

odstavci, se musí autorizovat jedinečným identifikátorem a postupovat způsobem stanoveným v bezpečnostní dokumentaci.

- Stanovení provozního řádu, jeho ověřování a vyhodnocování rizik v oblastech: seznamu oprávněných osob, které mají do objektu povolený přístup (včetně úklidu, elektrikářů atd.), manipulace s klíči, identifikačními prostředky a technickými prostředky (včetně označení, evidence, přidělení, odevzdání, úschovy, uložení duplikátů a likvidace), vedení provozního deníku návštěv, kontrolní činnosti (kontrola oprávnění pro vstup, kontrola pohybu osob a kontrola vynášených věcí a utajovaných informací), ochrany technického zařízení dle typu 4 (Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 a 454/2011 Sb., 2011) nebo vyšší dle přílohy č. 1 k § 5 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, což znamená zajištění bezpečnosti příslušníky ozbrojených sil nebo ozbrojených sborů, která je vykonávána způsobem nepravidelných obchůzek, bezpečnostní, požární a návštěvní řád.

5.2 Průmyslová bezpečnost

Podnikatel, právnická osoba, která ke své práci nezbytně potřebuje přístup k utajované informaci, musí být držitelem platného osvědčení podnikatele pro daný stupeň utajení. Podmínky pro žadatele jsou definovány § 96 odst. 2 písmena c) zákona č. 412/2005 Sb. Tento bod není předmětem práce, jelikož organizace SÚRAO je státní organizací a její činnost je upravena zákonem.

5.3 Administrativní bezpečnost

Administrativní bezpečnost vymezuje vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o bezpečnostní způsobilosti, ve znění zákonů č. 119/2007, 177/2007, 296/2007, 32/2008 a 255/2011 Sb. Obecně můžeme konstatovat, že se zabývá všemi pracovními činnostmi včetně přístupů do registrů. Rozsah podmínek je závislý na stupni utajení. Vyhláška č. 529/2005 Sb. v § 1 ustanovuje:

- Způsob vyznačování náležitostí na utajované informace v listinné a nelistinné formě.
- Druhy administrativních pomůcek, jejich náležitosti a vedení.

- Náležitosti souhlasu k pořizování opisu, kopie, výpisu a překladu utajovaného dokumentu.
- Podrobnosti k přepravě, přenášení, převzetí a zapůjčení utajovaného dokumentu a další manipulace s tím související, včetně organizačního zajištění těchto činností.
- Požadavky na přenosné schránky a obaly a vyznačování náležitostí na nich.
- Organizaci a činnost ústředního registru.
- Způsob označování a postupy při manipulaci s kryptografickým materiálem upraveno zvláštní právním předpisem.

5.4 Fyzická bezpečnost

Fyzická bezpečnost je vymezena vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášek č. 55/2008 a 433/2011 Sb., která stanovuje bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik a další požadavky na opatření fyzické bezpečnosti, přičemž objekt, budova nebo daný ohraničený prostor jsou fyzickým prostředím, ve kterém se nachází zabezpečená oblast anebo jednací oblast. Zabezpečené oblastí řadíme do dvou tříd:

- Třída I: zde se vstupem do oblasti dochází k seznámení s utajovanými informacemi.
- Třída II. zde se vstupem nedochází k seznámení.

Obdobným způsobem jsou charakterizovány a rozděleny na typy další entity:

- stavební konstrukce (dle šířky a použitých materiálů cihly, vápencové bloky, pórobetonové tvárnice, vyztužený beton atd.) do 5 typů (typ 4, 3, 2, 1,a 0),
- úschovné objekty (typ 4, 3, 2 a 1),
- hranice objektu (typ 4, 3, 2, 1 a 0),
- systém kontroly vstupu do zabezpečené oblasti (typ 4, 3, 2 a 1),
- ostraha (typ 5, 4, 3, 2 a 1),
- systém elektrické zabezpečovací signalizace (typ 4, 3, 2 a 1),
- zámky, uzamykací systémy, fyzické bariéry atd.

Aktiva certifikovaného informačního systému musí být umístěna do prostoru, kde je zajištěna fyzická ochrana. Požadavky informačního systému ve stručných bodech ve stupni 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 zábranných prostředků.
- Mechanické zábranné prostředky je nutné použít pouze certifikované mechanické zábranné prostředky a certifikovaná zařízení elektrické zabezpečovací signalizace.
- Zajištění, aby v zabezpečené oblasti nedošlo k nepovolenému získání utajovaných informací (kamerový systém).
- Zajištění ukládání utajovaných informací.
- Vypracování projektu fyzické bezpečnosti a její dokumentace včetně zabezpečení objektu s popisem kategorií, tříd a použitých technických prostředků a způsobu použití, včetně provozního řádu objektu a seznamu odpovědných osob a krizového plánu pro mimořádné události, hrozby a rizika (Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., 2008).

5.5 Bezpečnost informačních a komunikačních systémů

Oblast bezpečnosti informačních a komunikačních systémů je upravena vyhláškou 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, ve znění vyhlášky 453/2011 Sb. Bezpečnostní dokumentace informačního systému musí zohledňovat vše o jeho částech, bezpečnostní politice, konfiguraci, nastavení a provozu. 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 požadavky a na bezpečnostní požadavky bezpečnostní politiky nadřízeného orgánu, pokud byla zpracována. Z dalších požadavků je nutné dodržet následující:

- Informační systém musí být vždy certifikován Národním bezpečnostním úřadem.
- Informační systém je provozován v odpovídajícím bezpečnostním provozním módu.

- V informačním systému mohou být použity pouze HW a SW komponenty odpovídající schválené bezpečnostní dokumentaci informačního systému, které jsou chráněny proti škodlivému kódu (měření a otestování proti kompromitujícího vyzařování).
- Informační systém musí mít vypracovanou analýzu rizik se seznamem hrozeb a protiopatření.
- Informační systém pro stupeň Důvěrné musí zajistit:
  - jednoznačnou identifikaci, autentizaci uživatelů a řízení přístupu, bezpečnostního správce, správce informačního systému a správce kryptografické ochrany,
  - bezpečnost funkcí informačního systému, jež zajišťují identifikaci,
  - povinné anebo volitelné řízení přístupu k objektům pro různé role (uživatel, správce IS atd.),
  - důvěrnost a dostupnost informací,
  - nepřetržité zaznamenávaní událostí (video záznamy) včetně jejich zkoumání a vyhodnocování,
  - ošetření paměťových objektů a nosičů informací a jejich obsahu (šifrování),
  - zavedení, nastavení a provozu bezpečnostních mechanismů,
  - fyzickou bezpečnost a bezpečnost v prostředí počítačových sítí informačního systému (umístění jednotlivých komponent a jak mají vypadat) včetně jeho testování a kontroly,
  - bezpečný přenos informací mezi koncovými uživateli včetně zajištění důvěrnosti, integrity a neodmítnutelnosti odpovědnosti (listinné i nelistinné podoby),
  - ochranu rozhraní počítačové sítě proti průniku do informačního systému,
  - personální a administrativní bezpečnost informačního systému (školení všech rolí) včetně definování činností a odpovědnosti jednotlivých rolí, nastavení prověřování a soustavné kontroly (vyhodnocování logů),
  - instalaci informačního systému oprávněnými osobami,
  - plnou kontrolu správy počítačové sítě. (Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. 2005)

5.6 Kryptografická ochrana

Oblast kryptografické ochrany je upravena vyhláškou č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013 Sb. Vyhláška definuje instalaci kryptografického prostředku včetně značení, jeho nastavení, zajištění provozní obsluhy, používání kryptografických klíčů, zajištění výroby klíčových materiálů, odesílání kryptografické písemnosti v listinné a nelistinné podobě a zajištění servisu (Vyhláška č. 532/2011 Sb., o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013 Sb., 2011, 2013).

6 SPRÁVA ÚLOŽIŠŤ RADIOAKTIVNÍCH ODPADŮ

Pro studii proveditelnosti jsem využila skutečnou společnost Správa úložišť radioaktivních odpadů (dále SÚRAO) se sídlem Dlážděná 6, Praha 1. Jedná se modelovou situaci, kdy všechna použitá data byla získána z veřejně dostupných zdrojů a jsou v textu příslušně odkazována. Údaje, které není možné s ohledem na zákon 412/2005 Sb. zveřejnit jsou fiktivní a jsou použity pouze pro ilustraci reálného stavu. Společnost SÚRAO byla zřízena Ministerstvem průmyslu a obchodu 1. června 1997 na základě atomového zákona č. 18/1997 Sb., od roku 2000 dle § 51 zákona č. 219/2000 Sb. je organizační složkou státu. Cílem SÚRAO je obecně zajišťovat bezpečnost v oblasti nakládání s radioaktivními odpady tzn., že zajišťuje přípravu a výstavbu nových úložišť, správu a zajištění provozu povrchových a v budoucnu i hlubinných úložišť, úpravu a evidenci vyhořelého paliva, kontrolování a monitorování radioaktivních odpadů a jejich vlivu na okolí. Dokumenty, které SÚRAO vytváří, zpracovává a distribuuje, jsou utajovanými informacemi stupně utajení Vyhrazené a Důvěrné, a proto musí být zabezpečeny podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (SÚRAO: Správa uložišť radioaktivních odpadů).

SÚRAO zajišťuje bezpečnost čtyř povrchových úložišť: Dukovany, Bratrství – Jáchymov, Richard – Litoměřice a Hostim Beroun (toto úložiště je uzavřené, probíhá zde pouze kontrola a monitorování). V současné době je ve fázi přípravy tzv. hlubinná forma úložiště, pro tuto formu uskladnění byly vytipovány následující lokality: lokalita Kraví Hora (u obce Bukov), lokalita Čihadlo (u města Deštná), lokalita Březový potok (u obce Pačejov), lokalita Hrádek (u obce Rohozná), lokalita Magdaléna (u obce Jistebnice), lokalita Čertovka (u obce Blatno) a lokalita Horka (u obce Hodov) (SÚRAO: Správa uložišť radioaktivních odpadů).

7 ANALÝZA STÁVAJÍCÍHO STAVU

Analýza stávajícího stavu informačního systému SÚRAO byla provedena v oblasti: bezpečnosti stávajícího stavu informačního systému, využitelnosti stávajícího informačního systému, personální, fyzické a administrativní bezpečnosti a krizového řízení.

7.1 Bezpečnost informačního systému

Následující kapitola popisuje informační systém společnosti SÚRAO – jedná se o ilustrativní popis předpokládaného reálného nasazení. Ve společnosti SÚRAO je provozován certifikovaný informační systém pro zpracování utajovaných informací, schválený Národním bezpečnostním úřadem (NBÚ). Tento systém představuje zpracování dat na psacích strojích v jednotlivých lokalitách. Výsledná data z lokalit jsou přenášena v souladu s § 23 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací v označené obálce (Každý utajovaný dokument je: označen stupněm utajení podle § 5 vyhlášky č. 529/2005 Sb., prokazatelně zaevidován dle §7 stejné vyhlášky a jeho jednací číslo musí být uvedeno na obálce) skrze držitele poštovní licence (Zákon č. 29 /2000 Sb., o poštovních službách a o změně některých zákonů, 2000), který může přepravovat zásilky s utajovanými informacemi do stupně důvěrné, je-li místo zásilky v České republice. Držitel poštovní licence písemně potvrzuje převzetí zásilky a adresát potvrzuje příjem zásilky. Odesílatel (lokalita) dostává písemné potvrzení o doručení zásilky. V centru jsou data z lokalit zpracovávány a analyzovány na 8 pracovních stanicích, kde je nainstalován MS Office a antivirový program Symantec Endpoint Protection, který je aktualizován a upgradován 1x za týden. Uživatelská data stanic nejsou zálohována ani archivována. Výsledná data po schválení jsou 2x vytištěna (z 90%) a nebo 2x vypálena (10%) na DVD. Jedna verze je uložena v archivu SÚRAO a druhá verze je označena stupněm utajení, číslem jednacím a zabalena do bezpečnostní schránky. Kurýr nebo držitel poštovní licence zajišťuje přepravu do Státního úřadu pro jadernou bezpečnost (dále SÚJB) v bezpečnostní schránce, která je zajištěna proti neoprávněné manipulaci s jejím obsahem a to zámkem. Bezpečnostní schránka je označena větou: *"V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!"* (Vyhláška č. 55/2008, kterou se mění vyhláška č. 529/2005 Sb., o administrativní bezpečnosti

a o registrech utajovaných informací, 2008). Držitel poštovní licence i kurýr odpovídá státu za poškození a úbytek obsahu zásilky.

7.2 Využitelnost stávajícího informačního systému

Stávající informační systém byl pořízen před 6 lety a technicky je zastaralý. Využitelnost mají pouze licence Endpoint Protection v počtu 8 kusů, kde si SÚRAO kupovalo aktualizace antivirového software.

7.3 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. SÚRAO zpracovává utajované informace jak na ručních psacích strojích, tak na samostatných stanicích, proto můžeme konstatovat, že v organizaci je v současné době dostatečný počet uživatelů budoucího nového informačního systému s platným označením stupně utajení a to včetně bezpečnostního správce a správce informačního systému. SÚRAO má zpracován personální projekt dle § 72 zákona. Organizace v případě technického řešení II. bude potřebovat pracovníka kryptografické ochrany.

7.4 Fyzická bezpečnost

Fyzická bezpečnost představuje systém opatření, nástrojů a podmínek, kterými se zamezuje nebo ztěžuje fyzický přístup neoprávněných osob k utajovaným informacím, popřípadě umožňuje takový přístup nebo pokus o neoprávněný přístup zaznamenat pomocí ostrahy, režimových opatření a nasazených technických prostředků. Organizace SÚRAO 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 však neuvažoval o síťovém řešení 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 centrální úložiště utajovaných informací.

7.5 Administrativní bezpečnost

Administrativní bezpečnost tvoří systém při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi. Administrativní bezpečnost je v organizaci SÚRAO 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 pevné látkové obálky a bezpečnostní schránky. Organizace má podepsanou smlouvu s držitelem poštovní licence o přepravě utajovaných informací (z lokalit do centra SÚRAO), kdy předem oznámené osoby držitele licence 3x týdně převáží připravené utajované zásilky. Osobou kurýra je zaměstnanec SÚRAO, který je poučen a je držitelem platného osvědčení fyzické osoby pro příslušný stupeň utajení (Důvěrné), a který dle potřeby zaměstnavatele odváží příslušné zásilky do SÚJB a zpět. Odpovědnou osobou organizace je jmenována osoba odpovědná za vedení jednacího protokolu. Je zpracován vnitřní předpis o zajištění administrativní bezpečnosti v organizaci.

7.6 Kryptografická ochrana

V technickém řešení I. je partnerem SÚJB, který provozuje svůj vlastní certifikovaný systém a v rámci něho řeší i kryptografickou ochranu. Mezi SÚJB a SÚRAO existuje písemná dohoda o vytvoření vzdáleného samostatného pracoviště

v prostorech SÚRAO, o který bude informační systém SÚJB rozšířen. SÚJB bude odpovědný za tuto vzdálenou pracovní stanici. V technickém řešení II. si SÚRAO musí vybudovat kryptografické pracoviště a proškolit správce kryptografického prostředku. Kryptografické prostředky budou zajišťovat komunikaci mezi lokalitami a centrálou SÚRAO.

7.7 Krizové 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, tato příloha musí být doplněna o řešení krizových situací vyplývajících z vybrané varianty technického řešení. Součástí přílohy jsou požární poplachové směrnice a evakuační plán.

8 ANALÝZA POTŘEB

Analýza potřeb přesně vymezuje, tj. definuje předem odsouhlasené potřeby - požadavky zadavatele na zhotovení nového informačního systému, jež by měla studie proveditelnosti obsahovat a zároveň zohledňovat stávající stav. Vlastní analýza potřeb je podkladem k návrhu realizace informačního systému IS SURAO-UI. Výsledky analýzy potřeb.

8.1 Ochrana utajovaných informací

Ochrana utajovaných informací vyplývá z charakteru dokumentů (listinná a nelistinná podoba), jedná se o utajované dokumenty podle č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, v platném znění.

8.2 Stupeň utajení zpracovaných informací

Stupeň utajení zpracovávaných informací je stanoven na úroveň Vyhrazené nebo Důvěrné dle nařízení vlády č. 522/2005 Sb., ve znění nařízení vlády č. 240/2008 Sb. dle přílohy č.16, která definuje seznam utajovaných informací v oblasti jaderné bezpečnosti. SÚRAO zpracovává utajované informace Evropské unie v stupni utajení Restreint (Vyhrazené) a Confidential (Důvěrné). Z výše uvedeného vyplývá, že nový informační systém musí pracovat v bezpečnostním módu s nejvyšší úrovní stupně Důvěrné, který umožňuje zpracování utajovaných informací různého stupně utajení, všichni uživatelé v systému musí splňovat podmínky nejvyššího stupně utajení, ale nemusí být oprávněni se seznamovat všemi utajovanými informacemi. Objem zpracovávaných informací je 98% v úrovni Vyhrazené a 2% ve stupni Důvěrné.

8.3 Počet osob zpracovávající utajované informace

Počet osob zpracovávající utajované informace pomocí nového informačního systému je stanoven na počet 40 (po zavedení systémů). Z toho 15 osob se bude s utajovanými informacemi pouze seznamovat, 2 osoby budou určeny pro správu informačního systému - jedná se o roli bezpečnostního správce informačního systému a správce informačního systému. 10 osob bude mít přístup do zabezpečených oblastí, ale nebudou se seznamovat s utajovanými informacemi - jedná se o údržbáře

a uklízečky, u nich je nutné eliminovat riziko přístupu k informačním technologiím a médiím.

8.4 Distribuce informací uvnitř organizace a mimo organizaci

Utajované informace budou vznikat uvnitř organizace v pěti objektech, které splňují podmínky definované zákonem č. 412/2005 Sb. (viz. kapitola 5.4 Fyzická bezpečnost).

1) Sídlo SÚARO Dlážděná 6, Praha 1. Utajované informace budou vznikat, zpracovávat se a archivovat v patře X sídla SÚRAO odtud jsou utajované informace pravidelně odesílány Státnímu úřadu pro jadernou bezpečnost.
2) Dukovany, úložiště je přímo v areálu jaderné elektrárny Dukovany, utajované informace se budou zpracovávat v jedné ze zděných budov přímo ve středu celé elektrárny.
3) Bratrství – Jáchymov, úložiště je vybudováno v části opuštěných prostor bývalého uranového dolu Bratrství, utajované informace se budou zpracovávat v kancelářské zděné budově.
4) Richard – Litoměřice, úložiště je pod povrchem kopce Bídnice, utajované informace se budou zpracovávat v samostatném zděném objektu uprostřed oplocené plochy.
5) Hostim – Beroun, pouze měřící stroje, které monitorují a zaznamenávají data, utajované informace se zpracovávají přímo v úložišti pod povrchem (SÚRAO: Správa uložišť radioaktivních odpadů).

8.5 Komunikace v rámci Evropské unie

Komunikace v rámci Evropské unie se přímo nepředpokládá, bude prováděna skrze Státní úřad pro jadernou bezpečnost, tyto dokumenty budou označeny EU Restreint (Vyhrazené) a Confidential (Důvěrné).

8.6 Množství a druh dokumentů

Množství zpracovaných dokumentů a jejich druh. V současné době je 90% listinné a 10% nelistinné povahy utajovaných dokumentů (kapacita 40kB). Nový, elektronický informační systém IS SURAO-UI by měl zajistit přechod na opačný poměr tj. 90% nelistinné a 10% listinné povahy dokumentů. Odesílané dokumenty SÚJB jsou

o kapacitě 1100 kB. Disková kapacita a kapacita zálohování by měla počítat s 20% rezervou při nákupu.

8.7 Počítačová síť a pracovní stanice

Z rozsahu zpracovaných dat a počtu uživatelů (získané analýzou stávajícího stavu) vyplývá, že nový informační systém IS SURAO-UI musí umožnit zpracování informací tak, aby více uživatelů mohlo současně přistupovat k informacím celého týmu, informacím pracoviště a k dalším zdrojům. Materiály může distribuovat jakýkoliv uživatel jakémukoliv oprávněnému uživateli. Uživatel resp. skupina uživatelů má přístup jen k těm informacím v IS SURAO-UI, které nutně potřebují ke své práci. Uživatelé buď samostatně, nebo jako skupina uživatelů společně vytváří dokument, který je následně předán vedoucímu pracovníkovi do centrály SÚRAO, který materiál buď odsouhlasí, nebo vrátí k dopracování. Po schválení materiálu vedoucím 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. Automatizace zpracování dat:

- Technické řešení I. - samostatné stanice je uvedeno v rozsahu elektronického zpracování dat v rámci lokalit a centrály SÚRAO a následné exportování dat na SÚJB.
- Technické řešení II. - síťové provedení je uvedeno v rozsahu plné automatizace a elektronického zpracování dat v rámci lokalit a centrály SÚRAO a zároveň zajištění bezpečného a elektronickému přenosu mezi lokalitami, centrálou SÚRAO a SÚJB.

8.8 Komunikační bezpečnost při přenosu utajovaných informací

Komunikační bezpečnost při přenosu utajovaných informací je mezi lokalitami, centrálou SÚRAO a SÚJB zajištěna následovně.

- Technické řešení I. - samostatné stanice. Utajované informace elektronicky zpracované budou mezi lokalitami a centrálou přenášeny na vyjímatelných nosičích utajovaných informací. Komunikace mezi SÚRAO a SÚJB probíhá na základě dohody se SÚJB, kdy SÚRAO zřídí ve svém objektu v centru vzdálenou pracovní

stanici SÚJB. Za zajištění komunikační bezpečnosti mezi systémem IS SURAO-UI a vzdálenou pracovní stanicí bude odpovědný SÚJB. Správa vzdálené pracovní stanice bude v působnosti správy informačního systému SÚJB. Provozní obsluhou budou pověřeni zaměstnanci SÚRAO, kteří budou postupovat podle bezpečnostní směrnice pro obsluhu / užití informačního systému SÚJB.

- Technické řešení II. - síťové provedení. Utajované informace elektronicky zpracovávané budou posílány skrze zabezpečenou sítovou komunikaci do centrály SÚRAO. Komunikace mezi SÚRAO a SÚJB bude probíhat stejně jako u Technického řešení I.

8.9 Programové vybavení

Činnosti uživatelů IS SÚRAO-UI spočívají: v analýze provozních dat technického zařízení s jaderným obsahem a v analýze stavu životního prostředí. Jsou zaznamenány toky dat, porovnávány s normativy a vyhodnocovány odchylky. Data z technického zařízení budou u technického řešení I. předávány na DVD ve formě souborů v programu MS Excel. U technického řešení II. jsou data ve formě MS Excel zašifrována a skrze bezpečnou síťovou komunikaci odeslána příjemci. 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.). Všechna výše uvedená data budou v centru zaznamenávány do databáze Microsoft Access. Stanice budou zakoupeny s aktuální verzí operačního systému s možností downgrade na Windows 7 Enterprise.

8.10 Opatření počítačové bezpečnosti

U informačního systému IS SÚRAO-UI je potřebné mimo fyzické bezpečnosti definované vyhláškou 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, také splnit hardwarové, softwarové požadavky a zajistit organizační opatření. 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.

8.11 Zálohování a archivace dat

V informačním systému IS SÚRAO-UI bude provozovaná databáze všech získaných dat, na základě požadavku dostupnosti zpracovaných dat a celého informačního systému musí systém umožnit provádění záloh, archivaci dat a zálohování systémových prostředků.

8.12 Internet

Organizace by preferovala v rámci systému připojení k Internetu, po konzultaci s Národním bezpečnostním úřadem organizace překvalifikovala svůj požadavek a IS SÚRAO-UI nebude připojen k Internetu. Uživatelská potřeba využívat Internet bude řešena v rámci stávajícího firemního informačního systému.

9 TECHNICKÁ ŘEŠENÍ OBECNĚ

Po provedení analýzy stávajícího stavu, analýzy potřeb a definování podmínek stanovených zákonem č. 412/2005 Sb., o ochraně utajovaných skutečností a o bezpečnostní způsobilosti je možné navrhnout dvě technická řešení. Technické řešení I. je poloautomatizované ve smyslu přenosu dat. Technické řešení II. je plně automatizované provedení zajišťující komfort a rychlost. Utajované informace jsou z 98% zpracovávány ve stupni Vyhrazené a zbylé 2% ve stupni Důvěrné, což nabízí dvě možnosti řešení:

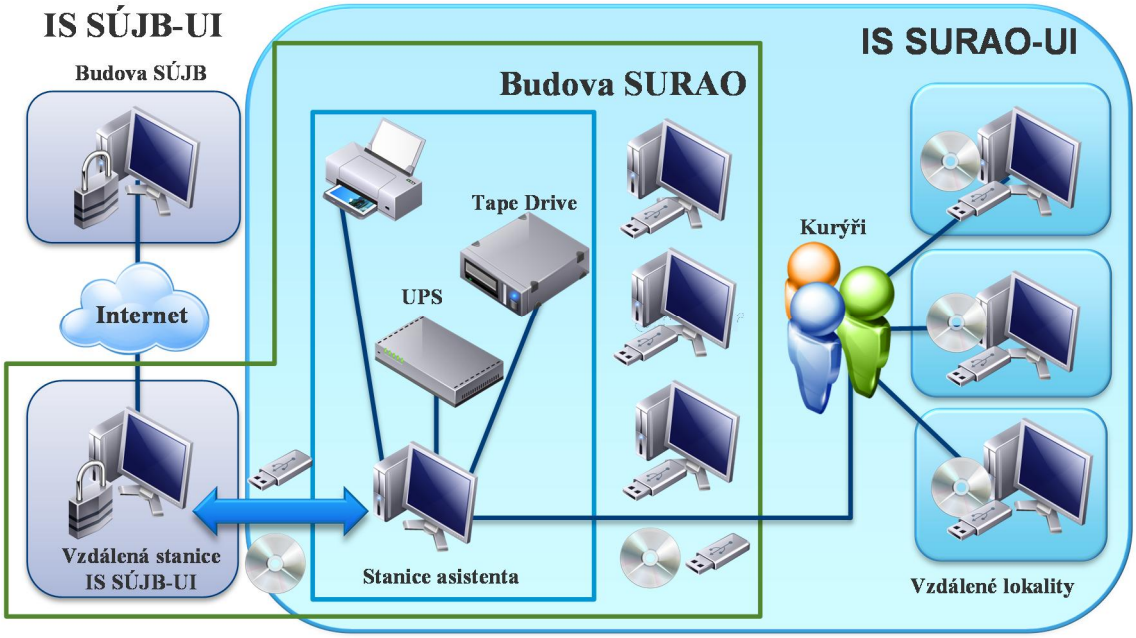
- Dané informační systémy od sebe oddělit do dvou samostatných informačních systémů, respektive do dvou podsystémů, kdy v jednom informačním systému by byly zpracovány utajované informace v režimu Vyhrazené a v druhém v režimu Důvěrné. Toto řešení snižuje požadavky personální bezpečnosti a možné náklady na zajištění fyzické bezpečnosti, na druhé straně by u tohoto provedení byly větší náklady na HW vybavení.
- Daná problematika různých stupňů utajovaných informací Vyhrazené a Důvěrné by byla řešena v jediném informačním systému v bezpečnostním 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 používaného stupně, který se v systému nachází a celý informační systém by musel splňovat požadavky na ochranu před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování, a zároveň by musely být v systému použity mechanismy volitelného řízení přístupu k informaci.

Pro účel této práce bude informační systém navržen ve stupni utajení Důvěrné a to z následujících důvodů: SÚRAO preferuje řešení v jediném informačním systému s pověřením všech uživatelů na nejvyšší používaný stupeň utajení, organizace preferuje zajištění fyzické bezpečnosti na stupeň utajení Důvěrné pro celý IS SURAO-UI. Objekty s budoucím IS SURAO-UI mají kolem sebe dostatečný perimetr kontrolovaný SÚRAO, aby mohlo být vyhověno požadavkům na ochranu proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování.

10 TECHNICKÉ ŘEŠENÍ I. – SAMOSTATNÉ STANICE

10.1 Počítačová síť I.

Informační systém IS SURAO-IU v technickém řešení I. je sestaven ze samostatných stanic, které nebudou propojeny žádnou sítí LAN (viz obrázek 1).



Obrázek 1: Technické řešení I.

Pro potřeby této práce uvažujme následující projekt fyzické bezpečnosti, organizace SÚRAO má 16 zabezpečených oblastí kategorie Důvěrné, patnáct zabezpečených oblastí se využívá pro zpracování utajovaných informací a jedna zabezpečená oblast je využívaná jako centrální úložiště utajovaných informací. Každá vzdálená lokalita (Dukovany, Bratrství – Jáchymov, Richard – Litoměřice a Hostim Beroun) má dvě zabezpečené oblasti: v jedné oblasti bude umístěna samostatná počítačová sestava systému IS SURAO-UI pro zpracování utajovaných informací a trezor pro lokální fyzickou archivaci rozpracovaných dat na Flash disk a druhá zabezpečená oblast bude určena pro seznamování s utajovanými informacemi, tzn., že tato oblast bude vybavena počítačovou sestavou informačního systému IS SURAO-UI umožňující pouze čtení. V centru organizace SÚRAO v Dlážděné 6 se nachází zbývajících 8 zabezpečených oblastí, jedna místnost X/Y1UI (X znamená označení patra / Y a číslo je označení místností systému UI utajovaných informací) bude vybavena dvěma počítačovými sestavami informačního systému IS SURAO-UI

umožňující pouze seznamování s utajovanými informacemi, v místnosti X/Y2UI bude umístěn vzdálený počítač SÚJB, v místnosti X/Y3UI bude umístěn stávající a nový elektronický archív s jednou počítačovou sestavou informačního systému IS SURAO-UI, místnost X/Y4UI bude definována jako místnost správce informačního systému s jednou počítačovou sestavou, v místnosti X/Y5UI bude umístěno tiskové centrum skládající se z počítačově sestavy IS SURAO-UI a tiskárny, v místnostech X/Y6UI a X/Y7UI budou umístěny počítačové sestavy informačního systému IS SURAO-UI v počtu 8 a místnost X/Y8UI zůstává jako prázdná rezerva.

10.2 Datové toky I.

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

1. Analyzovaná data od obsluhy technického zařízení s jaderným odpadem se vzdálených lokalit jsou ukládána: rozpracovaná data na Flash disk a následně uložena v trezoru a finální data na médiu DVD ve formátu souborů XLSX, ty jsou zabalena do pevné látkové obálky a bezpečnostní schránky a připravena pro přepravu utajovaných informací. Organizace má podepsanou smlouvu s držitelem poštovní licence o přepravě utajovaných informací, kdy předem oznámené osoby držitele licence 3x týdně převáží připravené utajované zásilky.
2. Bezpečnostní schránku přebírá osoba pověřená vedením jednacího protokolu.
3. Kontrola převzatých dat zahrnuje: kontrolu antivirovým programem a kontrolu čitelnosti média, provádí je osoba pověřená vedením jednacího protokolu.
4. Předání dat vedoucímu střediska znamená: zavedení dat do IS SURAO-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.
5. Zpracování dílčí analýzy dat. Jednotliví referenti zpracovávají analyzovaná data v certifikovaném systému IS SURAO-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 a materiál se distribuuje vedoucímu střediska.

6. Vedoucí střediska materiál buď odsouhlasí, nebo vrátí k dopracování; odsouhlasený materiál je postoupen odpovědné osobě ke schválení.
7. Odpovědná osoba organizace dokument schválí; dokument distribuuje svému asistentovi s pokynem k vytištění a expedici na SÚJB, nebo archivaci.
8. Asistent vytiskne příslušný dokument; dokument označí příslušným stupněm utajení; dokument označí číslem jednacím z jednacího protokolu; dokument nechá podepsat odpovědnou osobou.
9. Elektronickou verzi dokumentu schváleného odpovědnou osobou asistent uloží na příslušné médium tj. na 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.

10.3 Bezpečnostní provozní mód I.

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 SURAO-UI nemusí být oprávnění pracovat se všemi utajovanými informacemi v systému obsaženými.

10.4 Technické požadavky I.

Tato kapitola popisuje technické řešení I. z pohledu pracovních stanic, zálohování a archivace, kryptografického prostředku, řízení přístupu a tiskových služeb, autentizace uživatelů, zabezpečení disku stanic, antivirového programu a umístění systému v objektech.

10.4.1 Pracovní stanice I.

Pracovní stanice v celkovém množství 24 kusů (22 identických a 2 stanice ve speciální konfiguraci, jedná se o stanice EVOLVEO (Alza.cz) určené pro zálohování a archivování a pro komunikaci s SÚJB, 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 instalačního média vyrobeného správcem informačního systému (instalace pomocí klonů). Navržené uživatelské prostředí umožní, aby uživatelé nebyli vázáni na konkrétní stanici a mohli se s ohledem na režim práce dělit o pracovní stanice. Úložiště uživatelských dat bude směrováno výhradně na externí USB Flash disk. 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 vyjma stanice pro zálohování a archivaci a stanice SÚJB a jejich USB vstupy budou softwarově zakázány pomocí produktu OptimAccess (Sodatsw, 1997-2014). Součástí všech pracovních stanic je: klávesnice, myš, 19“ monitor, USB čtečka čipových karet a CyberPower BU600E - záložní zdroj (Alza.cz). Operačním systémem uživatelských stanic bude MS Windows 7 Enterprise, který má bezpečnostní certifikát NIST, stanice pro zálohování a archivace bude vybavena MS Windows Server Standard.

Množství	**Popis**
22x	Lenovo ThinkCentre E73 10DR
22x	Lenovo ThinkPlus Myš
22x	Lenovo ThinkPlus Klávesnice
2x	EVOLVEO Zeppelim 7900
24x	Lenovo LT1952p - LED display - 19" černý
24x	CyberPower BU600E-FR
24x	HID Omnikey 3121 USB - čtečka čipových karet
100x	HID Crescendo C700 - čipová karta
100x	Corsair Voyager 32 GB – Flash disk USB 3.0
24x	MS Windows SA Enterprise - pro stanice
1x	Windows Server Standard - pro zálohovací stanici EVOLVEO
14x	Symantec Protection Suite Enterprise Edition 4.0 a podpora
8x	Symantec Endpoind Protection 12 podpora (na stávající PC)
22x	Sodatsw OptimAccess

Množství	Popis
22x	ICZ Protect for Windows
22x	Microsoft Office Standard 2013
22x	Acrobat Adobe 11 Czech Standard

Tabulka 1: Pracovní stanice I.

10.4.2 Zálohování a archivace dat I.

Uživatelská data budou ukládána na USB Flash disky a ty budou správcem informačního systému vždy 2x týdně zálohovány. Výsledné tj. finální práce budou správcem informačního systému vypáleny na DVD nebo CD (dle kapacity), které následně asistent označí, zaeviduje a založí do archivu. V místnosti X/Y3UI bude umístěn stávající a nový elektronický archív s jednou počítačovou sestavou (ve speciální HW konfiguraci) informačního systému IS SURAO-UI. Na počítačové sestavě budou všechna uživatelská data s Flash disků uložena do předem připraveného jmenného adresáře a následně celý adresář bude zálohován. Zálohování a archivace bude prováděna automaticky programovým vybavením na externí storage páskové mechaniky TS2250, která má SAS rozhraní. Systém Storage TS2250 Tape Drive funguje na technologii LTO Ultrium5 se základní kapacitou 1500GB nativních dat a 3000 GB v komprimovaných datech s přenosovou rychlostí 140 Mbps native (Senetic.cz). Pro zálohování a archivaci je navržen software Symantec Backup Exec pro Windows Server. Zálohovací kopie budou ukládány v trezoru, a aby se předešlo haváriím a škodám, navrhuje se udržovat minimálně 3 generace záloh.

Množství	Popis
1x	IBM Storage TS2250 Tape Drive Model H5S
1x	IBM 6Gb SAS HBA
1x	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

Tabulka 2: Zálohování I.

10.4.3 Kryptografický prostředek I

Vlastní informační systém IS SURAO-UI nebude obsahovat žádný kryptografický prostředek. Komunikace mezi vzdáleným počítačem SÚJB, umístěného v prostorech SÚRAO (počítač dodá SÚRAO dle instrukcí SÚJB), a SÚJB, bude zajištěno kryptografickým prostředkem (vlastněným SÚJB), jehož instalaci, konfiguraci a klíčové hospodářství bude zajišťovat SÚJB. Správce informačního systému IS SURAO-UI, bude zároveň určeným pracovníkem pro zajištění komunikace mezi vzdálenou stanicí SÚJB a centrálou SÚJB, tento pověřený pracovník musí složit odbornou zkoušku způsobilosti pracovníka kryptografické ochrany (Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013 Sb., 2011, 2013). 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 2013 a Adobe Acrobat 11 Czech Standard (Alza.cz).

10.4.4 Řízení přístupu a tiskové služby I.

Pro řízení přístupu uživatelů budou použity mechanizmy ICZ Protect for Windows - bezpečnostní kryptografický SW (ICZ a.s., 2015), kdy vedoucí střediska zavede data do IS SURAO-UI a definuje rozsah osob, které s daty budou pracovat, nastaví k danému adresáři přístupová práva a oprávnění pro jednotlivé osoby.

Veškeré tisky budou prováděny na tiskárně HP LaserJet Pro 400 M 425w (Alza.cz), umístěné v zabezpečené oblasti X/Y5UI v kategorii Důvěrné. Tiskem dokumentů je pověřen asistent, který výslednou a schválenou práci přinese na Flash disku a z pracovní stanice u tiskárny provede tisk, následně zajistí v nejkratším čase evidenci utajovaných výtisků a manipulaci s nimi včetně skartace (Skartovačka Fellowers 75Cs nabízí křížový řez 3,9 x 38 mm o vstupní šíři 230 mm, najednou zvládne skartovat až 12 listů 70 gramového papíru, kancelářské sponky, čipové karty, CD a DVD (Alza.cz) vadných nebo nadbytečných výtisků.

Množství	Popis
1x	HP LaserJet Pro 400 M

Množství	Popis
2x	Fellowers 75Cs

Tabulka 3: Tiskárna a skartovačka I.

10.4.5 Autentizace uživatelů I.

K autentizaci uživatelů bude využita metoda autentizace pomocí SmartCard Logon, což je dvoufaktorová metoda typu: něco mám – SmartCard a něco 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. Čipová karta bude zakoupena v duálním provedení, kdy bezkontaktní část může být použita jako identifikační klíč pro kontrolovaný vstup do zabezpečených oblastí. Navrhovanou čipovou kartou je Crescendo C700 od společnosti HID (duální karta), která podporuje operační systémy Windows XP 2000/Vista/7 a Windows Server 2003a 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 (ASKON International s.r.o., 2014). Správce informačního systému na pokyn bezpečnostního správce zřídí na jednotlivých stanicích uživatelské účty (dle přístupů osob oprávněných), které jsou spárovány s příslušnou čipovou kartou. Pouze osoby oprávněné s příslušnou čipovou kartou po zadání PINu mohou pracovat v systému IS SURAO-UI a zároveň po přiložení čipové karty ke snímači vstupovat do zabezpečených oblastí. Správce informačního systému je odpovědný za zřizování, odstraňování uživatelských účtů a přidělení či odebrání čipových karet.

10.4.6 Zabezpečení disku stanice a antivirový program I.

Jednotlivé stanice umístěné v informačním systému IS SURAO-UI budou zabezpečeny proti krádeži, či odnesení pevného disku tak, že všechny pevné disky stanic budou pro pokrytí zbytkových rizik šifrovány komerčním kryptografickým prostředkem Protect for Windows (ICZ a.s., 2015), který spolupracuje s přihlašovacím

autentizačním zařízením od firmy HID čipová karta Crescendo C700 a čtečky Omnikey 3121 (ASKON International s.r.o., 2014).

Antivirová ochrana bude zajištěna antivirovými programy Symantec Endpoint Protection na pracovních stanicích, tato ochrana musí zajistit ochranu souborového systému pracovních 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.

10.4.7 Umístění informačního systému v objektech organizace I.

Informační systém bude instalován u organizace SURAO, Dlážděná 6, Praha 1 v patře X samostatné třípodlažní budovy, která je dle informací z katastru nemovitostí od ostatních prostor budovy oddělena železobetonovou zdí o síle 45 cm. Vstup do prostor je v souladu s platnou legislativou vymezen bezpečnostními dveřmi vybavenými elektrickým zámkovým zařízením a systémem kontroly vstupu certifikovaným pro stupeň utajení Důvěrné (stejný systém pro vstup je zaveden u všech vzdálených lokalit) a dané prostory nemají okna. Takto zabezpečená oblast plně splňuje požadavky uvedené ve vyhlášce Národního bezpečnostního úřadu č. 528/2005 Sb. Pro potřeby práce uvažujme, že vymezený objekt obsahuje 8 zabezpečených oblastí kategorie Důvěrné, z toho:

- jedna zabezpečená oblast (místnost X/Y1UI) bude vybavena dvěma počítačovými sestavami informačního systému IS SURAO-UI umožňující pouze seznamování s utajovanými informacemi,
- jedna zabezpečená oblast (místnost X/Y2UI) bude obsahovat vzdálený počítač SÚJB,
- jedna zabezpečená oblast (místnost X/Y3UI) bude obsahovat stávající a nový elektronický archív s jednou počítačovou sestavou informačního systému IS SURAO-UI,
- jedna zabezpečená oblast (místnost X/Y4UI) bude definována jako místnost správce informačního systému s jednou počítačovou sestavou,
- jedna zabezpečená oblast (místnost X/Y5UI) bude obsahovat tiskové centrum skládající se z počítačově sestavy IS SURAO-UI a tiskárny,

- dvě zabezpečení oblasti (místnosti X/Y6UI a X/Y7UI) budou použity pro počítačové sestavy informačního systému IS SURAO-UI v počtu 8 a místnost
- a jedna zabezpečená oblast (místnost X/Y8UI) zůstává jako prázdná rezerva.

Vždy dvě zabezpečené oblasti se nacházejí ve vzdálených lokalitách, kdy jedna je určena pro zpracování utajovaných informací a druhá pro seznamování s utajovanými informacemi. Všechny lokality jak jsou vybaveny bezpečnostními dveřmi s elektronickým zámkovým systémem a má-li objekt okna, pak jsou opatřena bezpečnostní mřížemi.

Všechny objekty s instalovanými komponentami IS SURAO-UI splňují požadavky na ochranu před únikem utajovaných informací prostřednictvím kompromitujícího vyzařování. Konečné splnění těchto požadavků bude před certifikací IS posouzeno Národním bezpečnostním úřadem.

10.5 Dostupnost služby I.

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:

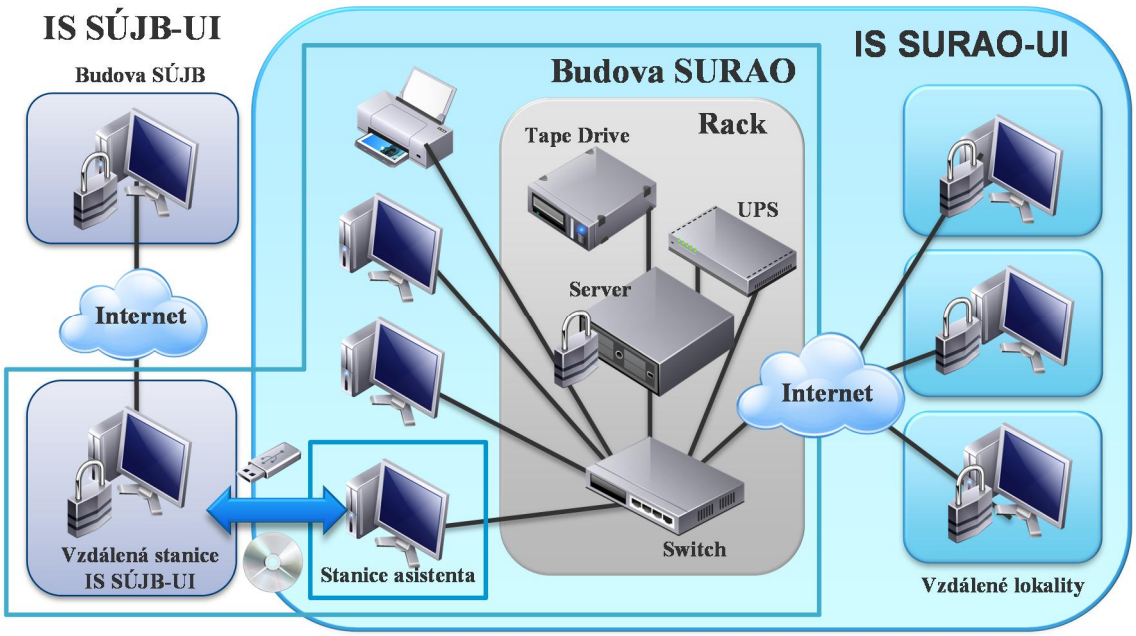
- V centru je k dispozici více 8 stanic, kdy v případě výpadku jedené stanice bude možné práci zajistit na zbývajících stanicích. V případě poruchy v lokalitě bude mít správce informačního systému k dispozici dvě stanice (určené pro servis), které budou předinstalovány a v případě poruchy správcem informačního systému dopraveny do vzdálené lokality, kde jsou zprovozněny.
- Pro zajištění nepřetržitého provozu budou všechny lokality a centrum vybaveny zdrojem UPS CyberPower BU600E-FR (Alza.cz)., který zajistí provoz i v době výpadku proudu po dobu nejméně 45 minut.
- Všechna uživatelská data budou 2x týdně zálohována v místnosti X/Y3UI, kde bude umístěn stávající a nový elektronický archív s jednou počítačovou sestavou informačního systému IS SURAO-UI.
- 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.

11 TECHNICKÉ ŘEŠENÍ II. – SERVEROVÉ ŘEŠENÍ

11.1 Počítačová síť II.

Informační systém IS SURAO-IU ve variantě technického řešení II. je navržen jako lokální vyčleněná (Dedicated) LAN. Vyčleněná LAN bude propojovat požadovaný počet pracovních stanic tak, aby uživatelé v centru mohli sdílet informace a zdroje v oblasti pamětí výpočetní techniky, nebo si zasílat v rámci dedikované sítě jednotlivé dokumenty atd., účastníci sítě v centru budou moci být trvale propojení s datovými úložišti (architektura Klient/Server). Vzdálená lokality (Dukovany, Bratrství – Jáchymov, Richard – Litoměřice a Hostim Beroun) budou propojeny chráněnou síťovou komunikací, kterou zajistí LANPCS (ICZ a.s., 2014, 2015) LANPCS je národní kryptografický prostředek, tj. interní šifrovací síťová karta do pracovní stanice, která umožňuje využití nezabezpečené komunikační infrastruktury (stávající kabeláže a nového aktivního prvku) v běžné kanceláři pro propojení certifikovaného informačního systému určeného pro zpracování utajovaných informací (ICZ a.s., 2014). Vzdálené lokality budou moci přijímat a odesílat utajovaná šifrovaná data, ale nebudou trvale propojeny s datovými úložišti (obrázek technického řešení II. č. 2.)



Obrázek 2: Technické řešení II.

11.2 Datové toky II.

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

1. Analyzovaná data od obsluhy technického zařízení s jaderným odpadem ze vzdálených lokalit jsou ve formátu souborů XLSX, následně jsou zašifrována a odeslána zabezpečenou komunikací osobě pověřené do její schránky (MS Exchange).
2. Za data v elektronické schránce, jejich kontrolu aktuálním antivirovým programem a vedení jednacího protokolu je odpovídá pověřená osoba.
3. Předání dat vedoucímu střediska znamená: zavedení dat do IS SURAO-UI; distribuce vybraných dat referentovi nebo referentům dle obsahu, 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 systému IS SURAO-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 a materiál se distribuuje vedoucímu střediska.
5. Vedoucí střediska materiál buď odsouhlasí, nebo vrátí k dopracování; odsouhlasený materiál je postoupen odpovědné osobě organizace ke schválení.
6. Odpovědná osoba 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.

11.3 Bezpečnostní provozní mód II.

Bezpečnostní provozní mód bude v technickém řešení II. stejný jako v kapitole 10.3. Technické požadavky I.

11.4 Technické požadavky II.

Informační systém bude založen na klasickém řešení Klient/Server, které spolu budou komunikovat pomocí počítačové sítě, tzn., že pracovní stanice a server budou propojeny pomocí strukturované kabeláže a switche IBM Ethernet Switch J48E (IBM, 2014). Na switch pak bude připojena ještě síťová tiskárna. Záložní zdroj elektřiny (UPS) bude napájet switch a server. Server, aktivní prvek, UPS a zálohovací zařízení budou v provedení pro rack a budou umístěny do 19“ uzamykatelného 25U velkého racku s ventilátorem, celý rackový komplet pak ještě bude doplněn o výsuvnou polici na klávesnici a o 1U 18,5 palců Standard Console Kit (obsahuje také sklápěcí monitor a klávesnici), UTP kabely, patch panel (na seřazení kabelů), dostatečně dimenzovanými zdroji elektřiny a čtečkou čipových karet pro přihlášení správce informačního systému.

11.4.1 Kabeláž, rozbočovač, aktivní prvek a UPS II.

Všechny budovy SÚRAO jsou zasíťované kabeláží značky Belden a Panduit (Kassex, 1995-2009), stávající zásuvky budou označeny a svedeny do nového aktivního prvku, který oddělí stávající síť. Aktivní prvek bude umístěn v 19palcovém racku IBM NetBay S2 25U Standard (IBM, 2008), který byl vybrán z důvodů kompatibility celého řešení, které je navrženo od značky IBM a také proto, že má perforované přední a zadní uzamykatelné, ocelové dveře, obsahuje chlazení, jeho hloubka je 100cm a výrobcem IBM je doporučován pro servery IBM Systems x. U aktivního prvku IBM System Networking RackSwitch G7052 (IBM, 2014) bude riziko proti výpadku 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. Pro zajištění bezpečné komunikace se vzdálenými lokalitami je použit LANPCS.

Množství	Popis
1x	IBM 25U Standard Rack Cabinet- RACK
1x	IBM Keyboard with integrated Poiting Device 3m cable/black/USB/ CZ

Množství	Popis
1x	IBM 1U 18.5in Standard Console Kit
6x	IBM 1.5m, 10A/100-250V, C13 to IEC 320-C14
1x	IBM 1500 LCD 2U Rack–UPS
2x	IBM System Networking RackSwitch G7052
2x	IBM 3 Year Onsite Repaier 22x7 4 Hour Response for RackSwitch

Tabulka 4: Rozbočovač, UPS a Switch II.

11.4.2 Server II.

Pro síťové technické řešení II. byl vybrán server IBM Server x3550 M4 v provedení 1U Rack, který může obsahovat: až dva CPU, 30MB Cache per procesor, 768GB ve 24 slotech, 8 HDD v provedení 2,5 palce, nebo tři disky v provedení 3,5 palce, s integrovaným řadičem 6Gbps RAID, dále jsou osazeny 2 zdroje napájení atd. (IBM, 2014). Na fyzickém serveru IBM budou ve virtuálním prostředí provozovány 4 virtuální Microsoft servery - první virtuální server bude obsahovat souborový tzv. File Server, tiskový tzv. Print Server, SQL server a MonitorWare Console (MonitorWare, 1988-2005), druhý virtuální server bude obsahovat doménový řadič pro Active Directory, DNS, DHCP, WINS a NTP, na třetím virtuálním serveru bude umístěna certifikační autorita a antivirová ochrana a na čtvrtém bude umístěn poštovní server MS Exchange. K virtualizaci bude využit free produkt VMware ESXi ve verzi 5.5. 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. Především z cenových, provozních (informační systém organizace SÚRAO nepracuje v režimu 7x24 a zaměstnanci nepracují v systému 5x8) a servisních (zajištění kvalitního servisu) důvodů není nabízené technické řešení předloženo v provedení dvou serverů v clusteru s jedním diskovým polem. V serveru bude instalováno 5 HDD o velikosti 300 GB v provedení SAS v režimu RAID 5, to znamená, že jeden disk bude použit jako hotspare disk, zbývající 4 disky budou tvořit lokální datové úložiště o efektivní kapacitě n-1 tj. 900 GB, z toho 100 GB bude použito na CA, 100GB na druhý virtuální server, 400 GB na první virtuální server a 300GB na MS Exchange (IBM, 2014).

Množství	Popis
1x	IBM Server x3550 M4, Xeon 4C E5-2609 2,4 GHz/1066 MHz/10MB, 1x4 GB
1x	Intel Xeon 4C Model E5-2609 Processor 2,4 GHz/1066 MHz - druhý CPU
1x	IBM 4 GB PC3L-10600 CL9 ECC DDR3 1333 MHz LP RDIMM
4x	IBM 8 GB PC3L-10600 CL9 ECC DDR3 1333 MHz LP RDIMM
5x	IBM 300 GB HDD 2,5in SFF G2HS 10K 6Gbps SAS HDD
1x	IBM ServeRAID M5110SAS/SATA Controller for IBM Systém x
1x	IBM ServeRAID M5100 Series 512 MB Cache/RAID 5 Upgrade for IBM Systém x
	IBM ServeRAID M5100 Series Battery Kit for IBM Systém x
1x	IBM 550W Hight Efficiency Platinum AC 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 5.5- tato verze je zdarma
4x	MS Windows Serveru 2012 Standard Edition
20x	MS Windows Server 2012 CAL Device
1x	MS SQL Server Standard 2014
16x	MS SQL Server Standard 2014 CAL Device
1x	MS Exchange Standard 2013
20x	MS Exchange Standard 2013 CAL Device
1x	MonitorWare Console Base Systém

Tabulka 5: Kabeláž, rozbočovač, UPS a Switch II.

11.4.3 Zálohování a archivace dat II.

Zálohování a archivace bude prováděna automaticky programovým vybavením na externí IBM Storage TS2250 Tape Drive Express Model H5S, která má připojení přes SAS rozhraní, je rozšiřitelná, funguje na technologii LTO Ultrium s fyzickou kapacitou 1,5 TB nativních dat a maximálně 3,0 TB v komprimovaných datech

s přenosovou rychlostí 140 Mbps native (IBM, 2014). 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.

Množství	Popis
1x	IBM Storage TS2250 Tape Drive Express Model H5S
1x	IBM 6 Gb SAS HBA
1x	IBM 19-inch Rack Mount Kit
1x	IBM Ultrium 5 Data Cartridge- 5-pack
1x	IBM 2M Mini-SAS/Mini-SAS 1x Cable
1x	IBM 3 roky Onsite Repair 9x5 Same Business Day
1x	Symantec Backup Exec 2014 for Windows Server
3x	Symantec Backup Exec 2014 for Agent for Windows Server
1x	Symantec Backup Exec 2014 Agent for Microsoft SQL Server
2x	Symantec Backup Exec 2014 Option Exchange Mailbox to 10 Users

Tabulka 6. Zálohování II.

11.4.4 Pracovní stanice II.

Pracovní stanice v celkovém množství 22 kusů (16 identických z toho 2 stanice budou určeny jako servisní rezerva a 6 stanic je ve speciální HW konfiguraci, jedná se o EVOLVEO stanici 1x pro SÚJB (Alza.cz), 4x pro vzdálené lokality, 1x pro správce informačního systému) 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 správcem informačního systému. 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 (Sodatsw, 1997, 2014), vyjma počítačů vzdálených lokalit (4x), počítače určeného pro SÚJB (1x) a počítače správce informačního systému. Součástí všech pracovních stanic je: klávesnice, 19“ monitor a USB čtečka čipových karet. Operačním systémem stanice bude MS Windows 7 Enterprise, který má bezpečnostní certifikát NIST. Všechny stanice ve vzdálených lokalitách (jak pro seznamování, tak pro zpracování tj. 8 počítačových sestav) a stanice určená pro SÚJB budou vybaveny záložním zdrojem napájení Cyber Power BU600E-FR (Alza.cz).

Množství	Popis
16x	Lenovo ThinkCentre E73 10DR
16x	Lenovo ThinkPlus Myš
16x	Lenovo ThinkPlus Klávesnice
6x	EVOLVEO Zeppelim 7900
22x	Lenovo LT1952p - LED display - 19" černý
9x	CyberPower BU600E-FR
22x	HID Omnikey 3121 USB - čtečka čipových karet
100x	HID Crescendo C700 - čipová karta
10x	Corsair Voyager 32 GB – Flash disk USB 3.0
22x	MS Windows SA Enterprise - pro stanice
12x	Symantec Protection Suite Enterprise Edition 4.0 a podpora
8x	Symantec Endpoind Protection 12 podpora (na stávající PC)
20x	Sodatsw OptimAccess
20x	ICZ Protect for Windows
20x	Microsoft Office Standard 2013
20x	Adobe Acrobat 11 Czech Standard

Tabulka 7: Pracovní stanice II.

11.4.5 Kryptografický prostředek II.

Kryptografické prostředky budou součástí řešení a) komunikační bezpečnosti IS-SUJB a b) komunikační bezpečnosti vlastního informačního systému IS SURAO-UI mezi vzdálenými lokalitami a centrálou.

a) Instalaci kryptografického prostředku, nainstalovaného v počítači pro komunikaci se SÚJB, jeho konfiguraci a klíčové hospodářství bude zajišťovat SÚJB. Určený zaměstnanec SÚRAO zajistí provozní obsluhu kryptografického prostředku (správce kryptografického prostředku). SÚJB dodá kryptografický prostředek a SURAO vlastní pracovní stanici certifikovaného systému IS SÚJB (dle pokynů SÚJB).

b) Instalaci kryptografických prostředků nainstalovaných ve vzdálených počítačích pro zpracování utajovaných informací pro zajištění komunikace mezi lokalitami a centrálou tj. počítačem správce informačního systému bude odpovídat za konfiguraci a klíčové hospodářství správce informačního systému organizace SÚRAO, který bude zároveň proškolen do pozice správce kryptografického prostředku, jeho úkolem bude zajišťovat provozní obsluhu kryptografických prostředků organizace SÚRAO (Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, 2011).

Pracovní stanice dle bodu a) i b) bude obsahovat: počítač včetně kryptografického prostředku, monitor, 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 2013 a Adobe Acrobat Czech 11 Standard (Alza.cz). Do místností s kryptografickým prostředkem, bude mít přístup obsluha (uživatelé – kteří zpracovávají utajované informace ve vzdálených lokalitách, asistent v centru a správce kryptografického prostředku (správce informačního systému), který složil odbornou zkoušku odborné způsobilosti pracovníka kryptografické ochrany (Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, 2011).

Množství	Popis
5x	ICZ LANPCS

Tabulka 8: Kryptografický prostředek II.

11.4.6 Řízení přístupu, souborové a tiskové služby II.

Pro uživatelská data a cestovní profily bude využíván souborový server. Cestovní profily budou upraveny pomocí skupinových politik tak, aby při přihlášení se kopírovaly pouze registry, ostatní části profilu budou přístupné přes namapované sdílené adresáře, výjimku budou tvořit pouze dočasná data aplikací, které se budou

ukládat na lokální HDD stanic umístěných v zabezpečených oblastech ve stupni Důvěrné a při odhlášení uživatele tato data budou automaticky smazána, tzn., že na HDD stanic nezůstanou po ukončení práce žádná data. 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 budou použity autorizační mechanizmy integrované v MS Windows a Active Directory.

Veškeré tisky budou prováděny na sdílené tiskárně HP LaserJet Pro 400 M425dw (Alza.cz) umístěné v zabezpečené oblasti (místnost X/Y5UI) v kategorii Důvěrné. V odpovědnosti uživatelů bude zajistit v nejkratším čase evidenci utajovaných výtisků (sešit připevněný u tiskárny) a manipulaci s nimi včetně skartace vadných nebo nadbytečných výtisků.

Množství	Popis
1x	HP LaserJet Pro 400 M
2x	Fellowers 75Cs

Tabulka 9: Tiskárna a skartovačka II.

11.4.7 Autentizace uživatelů II.

Autentizace bude zajištěna stejnou technologií SmartCard Logon (ASKON International s.r.o., 2014) jako u technického řešení I. tj. v kapitole10.4.5 Autentizace uživatelů I. s tím rozdílem, že pro autentizaci bude použit síťový autentizační protokol Kerberos, který integrován v 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, tato služba bude tímto způsobem provozována pro všechny osoby pouze v centru, v lokalitách uživatelům bude správcem informačního systému

zřízen na jednotlivých stanicích informačního systému IS SURAO-UI uživatelský účet, který je spárovaný s příslušnými čipovými kartami (tato druhá část je stejná jako v technickém řešení I.).

11.4.8 Zabezpečení disku stanice a antivirový program II.

Celá kapitola zabezpečení disku stanice a antivirový program je shodná s řešením uvedeným v kapitole 10.4.6 Zabezpečení disku stanice a antivirový program I.

11.4.9 Umístění informačního systému v objektech organizace II.

Podle projektu fyzické bezpečnosti má organizace SÚRAO 16 zabezpečených oblastí kategorie Důvěrné, patnáct zabezpečených oblastí se využívá pro zpracování utajovaných informací a jedna zabezpečená oblast je využívaná jako centrální úložiště utajovaných informací. Každá vzdálená lokalita má dvě zabezpečené oblasti v jedné oblasti bude umístěna počítačová sestava systému IS SURAO-UI pro zpracování utajovaných informací s LANPCS (ICZ, 2015), která bude zajišťovat ochranu síťové komunikace s centrálou a malým trezorem pro ukládání USB a lokálních podkladů, druhá zabezpečená oblast bude určena pro seznamování s utajovanými informacemi, tzn., že tato oblast bude vybavena počítačovou sestavou informačního systému IS SURAO-UI umožňující pouze čtení. V centru organizace SÚRAO v Dlážděné 6 se nachází zbývajících 8 zabezpečených oblastí,

- jedna zabezpečená oblast (místnost X/Y1UI) bude vybavena dvěma počítačovými sestavami informačního systému IS SURAO-UI umožňující pouze seznamování s utajovanými informacemi (stanice pro seznamování nejsou zapojeny do vyčleněné sítě),
- jedna zabezpečená oblast (místnost X/Y2UI) bude vybavena vzdáleným počítač SÚJB,
- jedna zabezpečená oblast (místnost X/Y3UI) bude serverovnou, kde umístěn RACK se serverem, UPS, switchem a systémem pro zálohování IS SURAO-UI,
- jedna zabezpečená oblast (místnost XY/4UI) bude definována jako pracoviště kryptografické ochrany správce informačního systému s jednou počítačovou sestavou,

- jedna zabezpečená oblast (místnost X/Y5UI) bude vybavena tiskovým centrem skládající se z počítačově sestavy IS SURAO-UI a tiskárny,
- dvě zabezpečené oblasti (místnosti X/Y6UI a X/Y7UI) budou vybaveny počítačovými sestavami informačního systému IS SURAO-UI v počtu 8 a místnost, které budou síťově propojeny se serverem a síťovou tiskárnou,
- jedna počítačová oblast (místnost X/Y8UI) zůstává prázdná (SÚRAO: Správa uložišť radioaktivních odpadů).

11.5 Dostupnost služby II.

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 splňovat 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.

12 HARMONOGRAM

Realizaci systému je možné rozdělit: na přípravnou fázi, na fázi realizace projektu a fázi provozu.

Harmonogram	rok 2015												rok 2016											
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
Přípravná fáze																								
Zpracování žádosti o dotaci																								
Schválení dotace																								
Příprava výběrového řízení																								
Schválení výběrového řízení																								
Výběr dodavatele zakázky																								
Schválení výsledků soutěže a podpis smlouvy																								
Podpis smlouvy o dílo s vítězem																								
Fáze realizace																								
Vytvoření bezpečnostní dokumentace, předkládá se NBÚ k certifikaci																								
Přepracování projektu fyzické bezpečnosti, předkládá se NBÚ ke schválení																								
Příprava rozvodů																								
Dodávka a instalace pracovních stanic																								
Instalace zálohovacího zařízení a archivace																								
Přeorganizování zabezpečených oblastí																								
Školení uživatelů																								
Školení správce informačního systému																								
Zkušební provoz a provedení bezpečnostních testů a doložení jejich výsledků NBÚ																								
Certifikace NBÚ, zajištění součinnosti																								
Schválení ostrého provozu NBÚ																								

Tabulka 10: Harmonogram - Technické řešení I.

Fáze provozu jsou roky: 2017, 2018,2019,2020,2021

Harmonogram	rok 2015												rok 2016											
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
Přípravná fáze																								
Zpracování žádosti o dotaci																								
Schválení dotace																								
Příprava výběrového řízení																								
Schválení výběrového řízení																								
Výběr dodavatele zakázky																								
Schválení výsledků soutěže a podpis smlouvy																								
Podpis smlouvy o dílo s vítězem																								
Fáze realizace																								
Vytvoření bezpečnostní dokumentace, předkládá se k NBÚ k certifikaci																								
Přepracování projektu fyzické bezpečnosti, předkládá se NBÚ ke schválení																								
Realizace kabeláže																								
Dodávka a instalace serveru a UPS																								
Dodávka a instalace pracovních stanic																								
Konfigurace virtuálních serverů a vytvoření uživatelských účtů																								
Dodávka a instalace zálohovacího zařízení																								
Oživení informačního systému																								
Přeorganizování zabezpečených oblastí																								
Školení uživatelů																								
Školení správce informačního systému																								
Školení správce kryptografického prostředku																								
Zkušební provoz a provedení bezpečnostních testů a doložení jejich výsledků NBÚ																								
Certifikace NBÚ, zajištění součinnosti																								
Schválení ostrého provozu NBÚ																								

Tabulka11: Harmonogram - Technické řešení II.

Fáze provozu jsou roky: 2017, 2018,2019,2020,2021

13 NÁKLADY

Náklad představuje zdroje, hodnotu, které byly nebo budou nenávratně vynaloženy, jsou tedy spojeny s výdajem peněz. V účetním období náklady snižují ekonomický přínos, což se odrazí v úbytku aktiv nebo snížení jejich hodnoty nebo vznikem či zvýšením závazků, jehož následkem je snížení vlastního kapitálu jinou formou než jeho rozdělením (vyplacením) vlastníkům. Náklad je přiřazován do období, ve kterém vznikly výnosy vynaložením tohoto nákladu, není-li takovýchto výnosů je náklad přiřazen do období, se kterým věcně a časově souvisí. Náklady je možné členit například na:

- **Finanční náklady** jsou náklady spojené s úrokovou mírou, daněmi, cenou investic a amortizací. V účetnictví jsou uvedeny pod účtovou třídou 5 respektive pod částí 56 (patří sem: finanční náklady, prodané cenné papíry a podíly, úroky, kurzové ztráty, náklady s přeceněním majetkových cenných papírů, náklady z finančního majetku, náklady z derivátových operací, ostatní finanční náklady, manka a škody na finančním majetku).
- **Náklady v účetnictví** jsou náklady uvedené pod účtovou třídou 5, které členíme na spotřebované nákupy (50), služby (51), osobní náklady (52), daně a poplatky (53), jiné provozní náklady (54), odpisy, rezervy a opravné položky provozních nákladů (55), finanční náklady (56), rezervy a opravné položky finančních nákladů (57), mimořádné náklady (58) a daně z příjmů a převodové účty (59).
- **Jednicové náklady** jsou náklady přímo související s jednotkou dílčího výkonu či konkrétní operaci. Jednicové náklady tvoří: výrobní materiál, mzdové výrobní náklady a jiné další náklady na licence, patenty, speciální balení, mimořádné náklady na expedici, na uvedené výrobku do provozu, školení aj. Opakem jsou režijní náklady.
- **Fixní,** někdy taky označované jako **kapacitní náklady** jsou náklady nezávislé na vyrobeném množství (např. nájemné), rostou skokem, jsou vyvolané potřebou zajištění určitých podmínek procesu.
- **Variabilní náklady** jsou náklady závislé na vyrobeném množství (např. cena surovin). Mohou být rozděleny na proporcionální (rostou přímoúměrně s objemem výkonu), podproporcionální (rostou pomaleji než objem výkonu) a nadproporcionální (rostou rychleji než objem výkonu).

- **Investiční náklady** jsou náklady, které vstupují do pořizovací ceny dlouhodobého majetku, tzn. cena pořízení majetku a další vedlejší náklady na pořízení jako náklad na koupi zařízení, náklad na instalaci zařízení, náklady na rozvody vody, vzduchu, kabelů aj, náklady na uvedení do provozu, náklady na zkoušky.
- **Provozní náklady** (**neinvestiční náklady**) jsou náklady na zajištění běžné činnosti (osobní náklady - mzdy, materiální náklady, náklady na služby, náklady na údržbu, daně a poplatky (bez DPH) a odpisy), tj. neinvestiční náklady (tj. s výjimkou finanční nákladů – úroků). Spadají do variabilních nákladů externích.
- **Mezní náklady**, marginální náklady jsou náklady při výrobě dodatečné jednotky výstupu resp. zvýšení celkových nákladů spojené s výrobou jednoho výrobku navíc.
- **Utopené náklady** jsou vynaložené náklady minulé, které již nelze získat zpět. Tyto náklady by neměly ovlivňovat další rozhodování o budoucnosti projektu.
- **Náklady obětovaní příležitosti**, doslova se jedná o náklady na příležitost, jedná se o příjmy z nějaké činnosti, které nezískáme, neboť jsme naše prostředky investovali do nějaké jiné činnosti.
- **Přímé náklady** jsou náklady, které jsou přímo přiřaditelné k jednotlivým výkonům (výrobkům, službám) bez jejich soustřeďování a dalšího rozpočítávání; jedná se obvykle o náklady na suroviny, materiál, polotovary, obaly, někdy i mzdy
- **Nepřímé náklady** jsou náklady, které nelze přímo přiřadit k určitému výkonu (výrobku, službě), nýbrž je nutné je určitým způsobem rozpočítávat, obvykle jsou nepřímými náklady např. na mzdy režijních pracovníků, nájemné, energie atd.
- **Prvotní náklady** jsou náklady vynaložené na vstupu do výroby.
- **Druhotné náklady** jsou kalkulované náklady na vlastní výkony.
- **Výrobní náklady** jsou náklady potřebné k zajištění výroby, zpravidla jednoho kusu. Informace použity: (HEURECA), (AZ data), (MANAGEMENT MANIA, 2014), (Šustová, 2007).

Pro účely této práce byly zohledněny **náklady investiční**, které by zároveň byly v komerční firmě fixními a přímými náklady a **provozní tj. neinvestiční náklady**, které by byly variabilními náklady.

13.1 Náklady v investiční fázi

Dílčí kalkulace jednotlivých technických řešení jsou uvedeny v Příloze č. I. Jednotlivé náklady v investiční fázi je možné zobrazit jako celkový přehled nákladů daného řešení v investiční fázi a náklady v investiční fázi dle jednotlivých let a následně tyto náklady mezi sebou porovnat podle stejného přístupu zobrazení.

13.1.1 Technické řešení I.

Celkové náklady v investiční fázi I.	Cena bez DPH	Cena s DPH 21%
Zálohování	**59.800 Kč**	**72.358 Kč**
HW	44.900 Kč	54.329 Kč
SW Licence	14.900 Kč	18.029 Kč
Pracovní stanice	**843.630 Kč**	**1.020.792,30Kč**
HW	444.210 Kč	537.494,10 Kč
SW licence	399.420 Kč	483.298,20 Kč
Řízení přístupu	**20.700 Kč**	**25.047 Kč**
HW	20.700 Kč	25.047 Kč
Implementace	**1.051.000 Kč**	**1.271.710 Kč**
Školení	**575.000 Kč**	**695.750 Kč**
Fyzická bezpečnost	**668.800 Kč**	**809.248 Kč**
HW	468.800 Kč	567.248 Kč
Implementace	200.000 Kč	242.000 Kč
Cena	**3.218.930 Kč**	**3.894.905,30 Kč**
Celkem HW	978.610 Kč	1.184.118,10 Kč
Celkem SW	414.320 Kč	501.327,20 Kč
Celkem Implementace	1.251.000 Kč	1.513.710 Kč
Celkem školení	575.000 Kč	695.750 Kč
Celkem	**3.218.930 Kč**	**3.894.905,30 Kč**
Zaokrouhleno		**3.894.905 Kč**

Tabulka12: Celkové náklady v investiční fázi - Technické řešení I.

Realizační náklady	2015	2016	2017	Celkem s DPH 21%
HW		1.184.118		1.184.118
SW		501.327		501.327
Implementace	484.000	1.029.710		1.513.710
Školeni		695.750		695.750
Celkem	**484.000**	**3.410.905**		**3.894.905**

Tabulka13: Náklady v investiční fázi dle jednotlivých let realizace - Technické řešení I.

13.1.2 Technické řešení II.

Celkové náklady v investiční fázi II.	Cena bez DPH	Cena s DPH 21%
Kabeláž HW	**137.200 Kč**	**166.012 Kč**
Servery	**306.300 Kč**	**370.623 Kč**
HW	93.200 Kč	112.772 Kč
SW licence	213.100 Kč	257.851 Kč
Zálohování	**108.100 Kč**	**130.801 Kč**
HW	45.600 Kč	55.176 Kč
SW Licence	62.500 Kč	75.625 Kč
Pracovní stanice	**664.820 Kč**	**804.432,20 Kč**
HW	320.060 Kč	387.272,60 Kč
SW Licence	344.760 Kč	417.159,60 Kč
Řízení přístupu HW	**20.700 Kč**	**25.047 Kč**
Kryptografický prostředek HW	**400.000 Kč**	**484.000 Kč**
Implementace	**1.322.000 Kč**	**1.599.620 Kč**
Školení	**647.000 Kč**	**782.870 Kč**
Fyzická bezpečnost	**668.800 Kč**	**809.248 Kč**
HW	468.800 Kč	567.248 Kč
Implementace	200.000 Kč	242.000 Kč

Celkové náklady v investiční fázi II.	Cena bez DPH	Cena s DPH 21%
Cena	**4.274.920 Kč**	**5.172.653,20 Kč**
Celkem HW	1.485.560 Kč	1.797.527,6 Kč
Celkem SW	620.360 Kč	750.635,6 Kč
Celkem Implementace	1.522.000 Kč	1.841.620 Kč
Celkem školení	647.000 Kč	782.870 Kč
Celkem	**4.274.920 Kč**	**5.172.653,20 Kč**
Zaokrouhleno		**5.172.623 Kč**

Tabulka14: Celkové náklady v investiční fázi - Technické řešení II.

Realizační náklady	2015	2016	2017	Celkem s DPH 21%
HW		1.797.527		1.797.527
SW		750.636		750.636
Implementace	484.000	1.357.620		1.841.620
Školeni		782.870		782.870
Celkem	**484.000**	**4.688.653**		**5.172.653**

Tabulka15: Náklady v investiční fázi dle jednotlivých let realizace - Technické řešení II.

13.1.3 Porovnání nákladů v investiční fázi

Popis	Technické řešení I.	Technické řešení II.
HW	978.610 Kč	1.485.560 Kč
SW licence	414.320 Kč	620.360 Kč
Implementace	1.251.000 Kč	1.522.000 Kč
Školení	575.000 Kč	647.000 Kč
Celkem bez DPH	**3.218.930 Kč**	**4.274.920 Kč**
Celkem s DPH 21%	**3.894.905,30 Kč**	**5.172.653,20 Kč**
Zaokrouhleno	**3.894.905 Kč**	**5.172.623 Kč**

Tabulka16: Porovnání nákladů v investiční fázi

Realizační náklady	2015	2016	2017	Celkem s DPH 21%
Technické řešení I.	484.000	3.410.905		3.894.905
Technické řešení II.	484.000	4.688.653		5.172.623

Tabulka17: Porovnání nákladů v investiční fázi dle jednotlivých let realizace

13.2 Náklady v provozní fázi

Náklady v provozní fázi, jak bylo uvedeno výše, jsou náklady na zajištění běžné činnosti, ale protože SÚRAO provozuje informační systém pro nakládání s utajovanými informacemi, nejsou náklady např. na mzdy zaměstnanců novými náklady. Kapitola náklady v provozní fázi tedy identifikuje pouze provozní náklady spojené s vybudování nového informačního systému pro nakládání s utajovanými informacemi, jako jsou náklady na nákup prodloužených SW a HW záruk, náklady na cizí sužby (kurýrní služba) a požadované podpoře a údržbě ze strany SÚKL. Samotné odpisy jsou pak řešeny v kapitole ekonomická a finanční analýza.

Dílčí kalkulace jsou uvedeny v Příloze č. I. Jednotlivé náklady v provozní fázi je možné zobrazit jako celkový přehled nákladů daného řešení v provozní fázi a náklady v provozní fázi dle jednotlivých let a následně tyto náklady mezi sebou porovnat.

13.2.1 Technické řešení I.

Množství	Popis - řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
1x	IBM 5 roky Onsite Repair 9x5 Same Business Day (zálohování)	30.000 Kč	30.000 Kč
22x	SW: MS Windows SA Enterprise - pro stanice na 5 let	5.625 Kč	123.750 Kč
8x	Symantec Endpoind Protection 60 podpora (na	2.350 Kč	18.800 Kč

Množství	Popis - řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
	stávající PC)		
14x	Symantec Endpoind Protection 60 podpora (na stávající PC) 48 měsíců	1.880 Kč	26.320 Kč
1x	Podpora od SÚJB k počítačové stanici s kryptografickým prostředkem na 60 měsíců	270.000 Kč	270.000 Kč
4x	(52 týdnů x 3 odvozy v týdnu)* 5 let	468.000 Kč	1.872.000 Kč
	Cena celkem bez DPH		**2.340.870 Kč**
	Cena celkem s DPH		**2.832.452,70 Kč**
	Následně počítáno s částkou		**2.832.450 Kč**

Tabulka18: Celkové náklady v provozní fázi – Technické řešení I.

Provozní náklad	2016	2017	2018	2019	2020	2021
Technické řešení I.	0	566.490	566.490	566.490	566.490	566.490
Celkem kumulace	0	566.490	1.132.980	1.699.470	2.265.960	2.832.450

Tabulka 19: Náklady dle jednotlivých let - Technické řešení I.

13.2.2 Technické řešení II.

Množství	Popis - řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
2x	IBM 5 Year Onsite Repaier 22x7 4 Hour Response for RackSwitch	10.400 Kč	20.800 Kč
1x	IBM 5Year Onsite Repair 24x7,	14.900 Kč	14.900 Kč

Množství	Popis - řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
	24 Hour Committed Service (server)		
1x	IBM 5 roky Onsite Repair 9x5 Same Business Day (zálohování)	30.000 Kč	30.000 Kč
20x	SW: MS Windows SA Enterprise - pro stanice na 5 let	5.625 Kč	112.500 Kč
8x	Symantec Endpoind Protection 60 podpora (na stávající PC)	2.350 Kč	18.800 Kč
12x	Symantec Endpoind Protection 60 podpora (na stávající PC) 48 měsíců	1.880 Kč	22.560 Kč
1x	Podpora od SÚJB k počítačové stanici s kryptografickým prostředkem na 60 měsíců	270.000 Kč	270.000 Kč
	Cena celkem bez DPH		**453.860 Kč**
	Cena celkem s DPH		**549.170,60 Kč**
	Následně počítáno s částkou		**549.170 Kč**

Tabulka 20: Celkové náklady v provozní fázi – Technické řešení II.

Provozní náklad	2016	2017	2018	2019	2020	2021
Technické řešení II.	0	109.834	109.834	109.834	109.834	109.834
Celkem kumulace	0	109.834	219.668	329.502	439.336	549.170

Tabulka 21: Náklady v provozní fázi dle jednotlivých let - Technické řešení II.

13.2.3 Porovnání provozních nákladů

Provozní náklad	2017	2018	2019	2020	2021	Celkem s DPH 21%
Technické řešení I.	566.490	566.490	566.490	566.490	566.490	2.832.450
Technické řešení II.	109.834	109.834	109.834	109.834	109.834	549.170

Tabulka 22: Porovnání provozních nákladů

14 EKONOMICKÁ A FINANČNÍ ANALÝZA

Metody, které jsou uvedené v kapitole ekonomická a finanční analýza, mají své opodstatnění v podnikové sféře, kde podnikové finance jsou tvořeny buď vlastními prostředky uloženými v bankovním ústavu, nebo úvěry a v některých případech dotacemi nebo subvencemi. V rozpočtové sféře neexistuje zisk, neexistují zde úvěry, pokud je vláda (jako výjimku) neschválí, neexistují zde v podstatě vlastní finanční zdroje, jsou zde jen příjmy (a ty se až na výjimky odvádí do státního rozpočtu) a výdaje, které představují prostředky přidělené ze státního rozpočtu organizační složce na její provoz, tj. zajištění služeb a rozvoj. Pokud organizační složka státu nebude žádat o dotace, pak nezvažuje nějakou úrokovou sazbu, vystačí si s porovnáním předpokládaných investičních a provozních výdajů (kapitola 13 – Náklady) a s životností investice. Operační programy vyžadují diskontování cash flow dle metodiky Evropské komise, kde diskontní faktor je uveden ve výši 5%. V oblasti výpočetní techniky u operačních programů je vyžadována: čistá současná hodnota (NPV), index ekonomické rentability, výnosnost investice a doba návratnosti. Práce pak byla doplněna o metodu diskontovaných hodnot nákladů a metodu převedených nákladů.

V ekonomické a finanční analýze jsou uvažovány pouze přímé finanční toky vyplývající z realizace projektu, jejichž příjemcem je nositel projektu. Všechny uvažované hodnoty jsou očištěny od redundantních částek.

Skutečné hotovostní toky jsou uvažovány jako příjmy a výdaje, nikoli jako náklady a výnosy v účetním smyslu. Pro výpočet ukazatelů nejsou započítány utopené náklady, tj. náklady spojené s předinvestiční fází projektu. Vzhledem k normativním požadavkům kladeným na informační systémy zpracovávající utajované informace, které zajišťují funkčnost celku, jsou v této studii porovnávány jednotlivé varianty mezi sebou z technického a funkčního pohledu.

Veškeré uvedené hodnoty jsou uvedeny v reálných cenách roku 2014 včetně DPH ve výší 21%. Hodnoty jsou následně uvedeny v roční vzdálenosti (nikoli však kalendářní) od zahájení projektu.

14.1 Ekonomické přínosy a újmy

Hlavní ekonomické přínosy (benefity) budou realizací projektu:

1) v oblasti personálního zajištění, kde hovoříme o benefitech:

- úspora pracovních míst,
- úspora času uživatelů,
- úspora času pracovních kapacit pro správu stávajícího informačního systému.

2)v oblasti samotného systému:

- odstranění duplicitních záznamů a chybovosti záznamů,
- zajištění doposud nedostupných informací,
- zrychlení pracovních postupů a zrychlení komunikace a práce týmů a tím
- zrychlení tvorby výstupů, a tím
- zrychlení vnitřních služeb úřadu,
- zpřesnění popisů,
- zkvalitnění evidence,
- snížení bezpečnostních rizik.

Neocenitelné přínosy:

- zvýšení kvality a rychlosti služeb poskytovaných SÚRAO,
- zrychlení přístupu k jednotlivým aplikacím a programům,
- efektivnější vzájemná komunikace mezi uživateli,
- vyšší úroveň bezpečnosti přenosu dat a informací,
- sjednocení informací.

Újma, neočekává se vyšší zátěž stávajících zaměstnanců, kteří musí znát příslušnou legislativu a postupy při práci se stávajícím systém pro zpracování utajovaných informací (byť většinou v papírové rovině). I přesto, že bezpečnostní správce bude využívat na kontrolu celého systému automatizované systémy, je nutné vzít v potaz navýšenou zátěž na správu systému. Větší zátěž bude mít jen správce informačního systému, který bude muset zajišťovat údržbu a procesy správy například kontroly nastavení a instalace nových virových bází atd.

14.1.1 Úspory v důsledku pracovních míst

Kvalifikace benefitu - průměrné náklady na jednoho analytika pracujících za plat definovaný zákoníkem práce č. 262/2006 Sb., činí v průměru 31.920 Kč (Měšec.cz, 2015), (Acjobs.cz, 2014). Celkové náklady na jednoho zaměstnance činí tedy 383.000Kč. Efekt tohoto benefitu je spočítán jako roční částka na analytika násobená počtem uspořených míst. Technické řešení I. a i II. vykazují v tomto ohledu stejnou míru úspory. Automatizace systému umožňuje vyloučit činnosti přepisu, opisu, kopírování a neustálé držení celkové kontinuity, nižší nároky jsou i na osoby vedoucích projektů.

	Počet míst	Roční sazba	Úspora za 1 rok
Technické řešení I.	3	383.000 Kč	1.149.000 Kč
Technické řešení II.	3	383.000 Kč	1.149.000 Kč

Tabulka 23: Úspora pracovních míst

14.1.2 Úspory v důsledku úspory času zaměstnanců

Díky realizaci projektu dojde ke zrychlení práce zaměstnanců SÚRAO a úspoře času u významné části jejich aktivit. Celkové hodnocení úspory času zaměstnanců je ½ hodiny denně, tj. to je 6,4% hodiny času pro nejvíce exponované zaměstnance (8 hodin = 100%, 30 minut = 6,4%). Celkový počet zaměstnanců po zavedení informačního systému je 40 osob, úspora se netýká 15 osob, které se budou pouze seznamovat s utajovanými informacemi. U technického řešení II. je větší úspora času odpovědné osoby, proto bude u této varianty přičtena 1 hodina (Zohledněno jako úspora přes 2 zaměstnance po ½ hodině.).

Benefit	Technické řešení I.	Technické řešení II.
Počet zaměstnanců	25	27
Průměrná doba odpracovaná všemi zaměstnanci za jeden kalendářní rok (210×dní8×počet zaměstnanců) v hodinách	42.000	45.360
Průměrná úspora	6,4%	6,4%

Úspora času zaměstnanců v hodinách	2.688	2.903
Průměrné náklady na analytika z kapitoly 14.1.1 (při 21 dnech a 8 hodinách práce) – uvedeno v Kč/ hodina	190	190
Celková úspora času/ rok	510.720 Kč	551.570 Kč

Tabulka 24: Úspora času zaměstnanců

14.1.3 Újma na straně větší zátěže správce informačního systému

Větší zátěž správce informačního systému. Průměrné náklady na správce informačního systému činí 39.408 Kč, hodinová sazba při 21 dnech je: 235 Kč (Mešec.cz, 2015). Uživatelé nepřistupují a ani nepracují s internetem, proto pravidelné činnosti správce informačního systému vyžadují následující údržbu:

- Technické řešení I. – není možné aktualizaci antiviru spouštět automaticky, je nutné obejít všechny PC.
- Technické řešení II. – instalace antiviru na základě instalačního balíčku, instalace na jednom serveru a jedné stanici pro kontrolu.

Újma	**Technické řešení I.**	**Technické řešení II.**
Počet PC	22	2
Odhad pracnosti na jednu stanici je 15 minut – uvedeno v minutách/ měsíc	330	30
Odhad pracnosti jednoho instalačního balíčku – uvedeno v minutách / měsíc	120	120
Celkem minuty/ měsíc	450	150
Celkem hodiny/ měsíc	7,5	2,5
Celkem hodiny/rok	90	30
Průměrné náklady na správce IT	235Kč	235 Kč
Celková újma/ rok	21.150 Kč	7.050 Kč

Tabulka 25: Újma správce informačního systému

14.2 Metody srovnání

Pokud existuje jedna varianta investičního kapitálu, pak rozhodnutím může být její přijetí, nebo její odmítnutí. Existuje-li více možností pro investování firemního kapitálu, mohou nastat dvě situace: kapitál stačí na jednu akci, nebo kapitál stačí na více akcí. V našem případě budeme brát v potaz pouze variantu s výběrem jedné nejvýhodnější varianty. Obě technická řešení porovnáme podle: absolutních čísel, NVP čisté současné hodnoty, indexu ekonomické rentability, výnosnost investice, doby návratnosti, porovnání variant metodou diskontovaných budoucích hodnot nákladů, porovnání metodou převedených nákladů aj. (Synek, 2011).

14.2.1 Ekonomické a finanční vyhodnocení projektu

Tabulky níže uvedené ukazují celkové náklady a ekonomické přínosy. Dle metodiky Evropské komise činí diskontní faktor 5%. Pokud by nebyl stanoven diskontní faktor, vzali bychom diskontní sazbu ČNB a k ní bychom zohlednili 2% meziročního růstu inflace a 2% na výměnu HW v čase. Diskontní faktor ve výši 1,0000 začíná v roce 2014. Jednotlivé výpočty jsou uvedeny pro variantu a) bez získání dotace na celé technické řešení a b) s dotací ve výši 70% na investici v technickém řešení. Dotace jsou přidělovány v režimu zpětného vyplácení, to znamená, po schválení a výběru projektu komisí je přislíbena dotace. SÚRAO celý projekt bude zpočátku financovat ze svého rozpočtu a teprve po předání projektu do provozu a kontrole komisí, bude přidělena dotace (tento efekt v práci nebude zohledněn). SÚRAO je rozpočtová organizace a oddělní informatiky získává prostředky z rozpočtu, tyto prostředky nejsou započteny jako příjem, vůči, kterému bychom mohli postavit investici. Investice byla postavena oproti socioekonomickým přínosům včetně újmy.

Poznámky k níže uvedeným tabulkám – všechny vzorce jsou uvedené v Metodice diplomové práce – kapitola 3:

- **Diskontované DCF** je metoda diskontovaných peněžních toků, to znamená, že je to metoda výnosového očekávání. Výnosová metoda vychází z předpokladu, že hodnota investice je určena očekávaným užitkem pro SÚRAO, v našem případě je očekávaným užitkem peněžní tok (cash flow) a její diskontování odráží míru rizika oceňované investice. Výsledek kumulovaného DCF je roven čisté současné hodnotě

- **Kumulované DCF** je rovno čisté současné hodnotě (zkráceně NPV, nebo ČSH), které vyjadřuje celkovou současnou (tj. diskontovanou) hodnotu všech peněžních toků souvisejících s investičním projektem. **Čistá současná hodnota** představuje rozdíl mezi současnou hodnotou očekávaných příjmů (cash flow) a nákladů na investici. V práci byly použity dva výpočty NPV, výsledek NPV dle vzorce uvedeného panem Synkem vyšel v první tabulce ve výši: 655.297, druhý výsledek NPV (Trhfirem.cz: Partner pro prodej a akvizice malých a středních firem, 2014-2015), který v našem případě můžeme nazvat kontrolním výsledkem, vypočteme dosažením hodnot (CF = cash flow, v = diskontní faktor, i = úroková míra rovna 0,05, r = rok) do vzorce:

$$NPV = \frac{CF}{(1+0{,}05)} + \frac{CF}{(1+0{,}05)^2} + \frac{CF}{(1+0{,}05)^3} + \frac{CF}{(1+0{,}05)^4} + \frac{CF}{(1+0{,}05)^5} + \frac{CF}{(1+0{,}05)^6} + \frac{CF}{(1+0{,}05)^7}$$

$$= \frac{-484.000}{1{,}05} + \frac{-3.010.905}{1{,}1025} + \frac{1.072.080}{1{,}1576} + \frac{1.072.080}{1{,}2155} + \frac{1.072.080}{1{,}2762} + \frac{1.072.080}{1{,}3401} + \frac{1.072.080}{1{,}4071} = 655.351$$

Menší rozdíly v jednotlivých výsledcích NPV jsou způsoby zaokrouhlováním.

- ROI značíme metodu výnosnosti (ziskovosti, rentability) investic, kde za efekt investice se považuje zisk a vychází z předpokladu, že změna v nákladech vyvolá změnu objemu výroky, jež se promítnou v zisku. (Synek, 2011)
- Doba návratnosti = době splácení investice.

14.2.1.1 Technické řešení I. - bez dotace

bez dotace	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Přínos/ Příjmy			**1.638.570**	**1.638.570**	**1.638.570**	**1.638.570**	**1.638.570**
Úspory z pracovních míst			1.149.000	1.149.000	1.149.000	1.149.000	1.149.000
Úspory času zaměstnanců			510.720	510.720	510.720	510.720	510.720
Újma správce IT			-21.150	-21.150	-21.150	-21.150	-21.150
Provozní náklady			**-566.490**	**-566.490**	**-566.490**	**-566.490**	**-566.490**
Realizační náklady	**-484.000**	**-3.410.905**					
CASH FLOW	**-484.000**	**-3.410.905**	**1.072.080**	**1.072.080**	**1.072.080**	**1.072.080**	**1.072.080**
Kumulované CF	-484.000	-3.894.905	-2.822.825	-1.750.745	-678.665	393.415	1.465.495
Diskontní faktor	**0.9524**	**0,9070**	**0,8638**	**0.8227**	**0,7835**	**0,7462**	**0,7107**
Diskontované DCF	**-460.962**	**-3.093.691**	**926.062**	**882.000**	**839.975**	**799.986**	**761.927**
Kumulované DCF	**-460.962**	**-3.554.653**	**-2.628.591**	**-1.746.591**	**-906.616**	**-106.630**	**655.297**

Tabulka 26: Plán průběhu cash flow bez dotace - Technické řešení I.

Ukazatel	Hodnota	Komentář
NPV čistá současná hodnota	655.297 Kč	Ekonomická čistá současná hodnota (ENPV) dosahuje kladné hodnoty, což po zohlednění soci-ekonomických přínosů projektu za období 7 let, diskontované společenskou diskontní sazbou ve výši 5%, převyšující investiční náklady přinese zisk.
Index ekonomické rentability	0,168	Projekt dosahuje výše, který rovněž prokazuje rentabilitu projektu z hlediska socioekonomických přínosů.
ROI výnosnost investice	27,52%	Výnos kapitálu je kladný, vyjadřuje míru zhodnocení investice, tj. vyjadřuje efektivitu provozní výkonnosti investice.
Doba návratnosti	3,63	Doba návratnosti je kratší jak 8 let, po kterou se v oblasti UI očekává životnost projektu.

Tabulka 27: Výsledky kriteriálních ukazatelů bez dotace – Technické řešení I.

Výpočty:

- **NPV čistá současná hodnota** je výsledná hodnota kumulovaného DCF, tj.: 655.297.
- **Index ekonomické rentability** byl získán výpočtem kumulovaného DCF/investice tj.: 655.297/3.894.905 = 0,168.
- **ROI výnosnost investice** = (průměrný zisk v pěti následujících letech/investice)×100, tj.: (1.072.080/3.894.905)×100=27,52%.
- **Doba návratnosti** od zaplacení investice od roku 2016 je: investice/ roční CF, tj.: 3.894.905/1.072.080=3,63.

14.2.1.2 Technické řešení I. - s dotací

s dotací	2015	2016	2017	2018	2019	2020	2021
Přínos/ Příjmy			**1.638.570**	**1.638.570**	**1.638.570**	**1.638.570**	**1.638.570**
Úspory z pracovních míst			1.149:000	1.149.000	1.149.000	1.149.000	1.149.000
Úspory času zaměstnanců			510.720	510.720	510.720	510.720	510.720
Újma správce IT			-21.150	-21.150	-21.150	-21.150	-21.150
Provozní náklady			**-566.490**	**-566.490**	**-566.490**	**-566.490**	**-566.490**

s dotací	2015	2016	2017	2018	2019	2020	2021
Realizační náklady	**-145.200**	**-1.023.272**					
CASH FLOW	**-145.200**	**-1.023.272**	**1.072.080**	**1.072.080**	**1.072.080**	**1.072.080**	**1.072.080**
Kumulované CF	-145.200	-1.168.472	-96.392	975.688	2.047.768	3.119.848	4.191.928
Diskontní faktor	**0.9524**	**0,9070**	**0,8638**	**0.8227**	**0,7835**	**0,7462**	**0,7107**
Diskontované DCF	**-138.289**	**-928.108**	**926.063**	**882.000**	**839.975**	**799.986**	**761.927**
Kumulované DCF	**-138.289**	**-1.066.397**	**-140.334**	**741.666**	**1.581.641**	**2.381.627**	**3.143.554**

Tabulka 28: Plán průběhu cash flow s dotací - Technické řešení I.

Ukazatel	Hodnota	Komentář
NPV čistá současná hodnota	3.143.554 Kč	Ekonomická čistá současná hodnota (ENPV) dosahuje kladné hodnoty, což po zohlednění soci-ekonomických přínosů projektu za období 7 let, diskontované společenskou diskontní sazbou ve výši 5%, převyšující investiční náklady přinese zisk.
Index ekonomické rentability	2,690	Projekt dosahuje výše, který rovněž prokazuje rentabilitu projektu z hlediska socioekonomických přínosů.
ROI výnosnost investice	91,75%	Výnos kapitálu je kladný, vyjadřuje míru zhodnocení investice, tj. vyjadřuje efektivitu provozní výkonnosti investice.
Doba návratnosti	1,09	Doba návratnosti je ani ne jeden rok a to je kratší jak 8 let, po kterou se v oblasti UI očekává životnost

Tabulka 29: Výsledky kriteriálních ukazatelů s dotací – Technické řešení I.

Výpočty:

- **NPV čistá současná hodnota** je výsledná hodnota kumulovaného DCF, tj.: 3.143.554.
- **Index ekonomické rentability** byl získán výpočtem kumulovaného DCF/investice tj.: 3.143.554/1.168.472=2,690.
- **ROI výnosnost investice** = (průměrný zisk v pěti následujících letech/investice) ×100, tj.: (1.072.080/1.168.472) × 100=91,75%.
- **Doba návratnosti** od zaplacení investice od roku 2016 je: investice/ roční CF, tj.: 1.168.472/1.072.080=1,09.

14.2.1.3 Technické řešení II. – bez dotace

bez dotace	2015	2016	2017	2018	2019	2020	2021
Přínos/ Příjmy			**1.693.520**	**1.693.520**	**1.693.520**	**1.693.520**	**1.693.520**
Úspory z pracovních míst			1.149.000	1.149.000	1.149.000	1.149.000	1.149.000
Úspory času zaměstnanců			551.570	551.570	551.570	551.570	551.570
Újma správce IT			-7.050	-7.050	-7.050	-7.050	-7.050
Provozní náklady			**-109.834**	**-109.834**	**-109.834**	**-109.834**	**-109.834**
Realizační náklady	**-484.000**	**-4.688.653**					
CASH FLOW	**-484.000**	**-4.688.653**	**1.583.686**	**1.583.686**	**1.583.686**	**1.583.686**	**1.583.686**
Kumulované CF	-484.000	-5.172.653	-3.588.967	-2.005.281	-421.595	1.162.091	2.745.777
Diskontní faktor	**0.9524**	**0,9070**	**0,8638**	**0.8227**	**0,7835**	**0,7462**	**0,7107**
Diskontované DCF	**-460.962**	**-4.252.608**	**1.367.988**	**1.302.898**	**1.240.818**	**1.181.746**	**1.125.526**
Kumulované DCF (PVCP)	**-460.962**	**-4.713.570**	**-3.345.582**	**-2.042.684**	**-801.866**	**379.880**	**1.505.406**

Tabulka 30: Plán průběhu cash flow bez dotace - Technické řešení II.

Ukazatel	Hodnota	Komentář
NPV čistá současná hodnota	1.505.406 Kč	Ekonomická čistá současná hodnota (ENPV) dosahuje kladné hodnoty, což po zohlednění soci-ekonomických přínosů projektu za období 7 let, diskontované společenskou diskontní sazbou ve výši 5%, převyšující investiční náklady přinese zisk.
Index ekonomické rentability	0,291	Projekt dosahuje výše, který rovněž prokazuje rentabilitu projektu z hlediska socioekonomických přínosů.
ROI výnosnost investice	30,62%	Výnos kapitálu je kladný, vyjadřuje míru zhodnocení investice, tj. vyjadřuje efektivitu provozní výkonnosti investice.
Doba návratnosti	3,27	Doba návratnosti je kratší jak 8 let, po kterou se v oblasti UI očekává životnost.

Tabulka 31: Výsledky kriteriálních ukazatelů bez dotace – Technické řešení II.

Výpočty:

- **NPV čistá současná hodnota** je výsledná hodnota kumulovaného DCF tj.: 1.505.406.

- **Index ekonomické rentability** byl získán výpočtem kumulovaného DCF/investice tj.: 1.505.406/5.172.653=0,291.
- **ROI výnosnost investice** = (průměrný zisk v pěti následujících letech/investice) ×100, tj.: (1.583.686/5.172.653) × 100=30,62%.
- **Doba návratnosti** od zaplacení investice od roku 2016 je: investice/ roční CF, tj.: 5.172.653/1.583.686=3,27.

14.2.1.4 Technické řešení II. – s dotací

s dotací	2015	2016	2017	2018	2019	2020	2021
Přínos/ Příjmy			**1.693.520**	**1.693.520**	**1.693.520**	**1.693.520**	**1.693.520**
Úspory z pracovních míst			1.149.000	1.149.000	1.149.000	1.149.000	1.149.000
Úspory času zaměstnanců			551.570	551.570	551.570	551.570	551.570
Újma správce IT			-7.050	-7.050	-7.050	-7.050	-7.050
Provozní náklady			**-109.834**	**-109.834**	**-109.834**	**-109.834**	**-109.834**
Realizační náklady	**-145.200**	**-1.406.596**					
CASH FLOW	**-145.200**	**-1.406.596**	**1.583.686**	**1.583.686**	**1.583.686**	**1.583.686**	**1.583.686**
Kumulované CF	-145.200	-1.551.796	31.890	1.615.576	3.199.262	4.782.948	6.366.634
Diskontní faktor	**0.9524**	**0,9070**	**0,8638**	**0.8227**	**0,7835**	**0,7462**	**0,7107**
Diskontované DCF	**-138.289**	**-1.275.783**	**1.367.988**	**1.302.898**	**1.240.818**	**1.181.746**	**1.125.526**
Kumulované DCF (PVCP)	**-138.289**	**-1.414.072**	**-46.084**	**1.256.814**	**2.497.632**	**3.679.378**	**4.804.904**

Tabulka 32: Plán průběhu cash flow s dotací - Technické řešení II.

Ukazatel	Hodnota	Komentář
NPV čistá současná hodnota	4.804.904 Kč	Ekonomická čistá současná hodnota (ENPV) dosahuje kladné hodnoty, což po zohlednění soci-ekonomických přínosů projektu za období 7 let, diskontované společenskou diskontní sazbou ve výši 5%, převyšující investiční náklady přinese zisk.
Index ekonomické rentability	3,096	Projekt dosahuje výše, který rovněž prokazuje rentabilitu projektu z hlediska socioekonomických přínosů.
ROI výnosnost investice	102,05%	Výnos kapitálu je kladný, vyjadřuje míru zhodnocení investice, tj. vyjadřuje efektivitu provozní výkonnosti investice.

Ukazatel	Hodnota	Komentář
Doba návratnosti	0,98	Doba návratnosti je kratší jak 8 let, po kterou se v oblasti UI očekává životnost.

Tabulka 33: Výsledky kriteriálních ukazatelů s dotací – Technické řešení II.

Výpočty:

- **NPV čistá současná hodnota** je výsledná hodnota kumulovaného DCF, tj.: 4.804.904.
- **Index ekonomické rentability** byl získán výpočtem kumulovaného DCF/investice, tj.: 4.804.904/1.551.796=3,096.
- **ROI výnosnost investice** = (průměrný zisk v pěti následujících letech/investice)×100, tj.: (1.583.686/1.551.796) × 100=102,05%.
- **Doba návratnosti** od zaplacení investice od roku 2016 je: investice/ roční CF, tj.: 1.551.796/1.583.686=0,98.

14.2.2 Metoda diskontovaných hodnot nákladů

Metoda diskontovaných hodnot budoucích provozních nákladů zohledňuje a pracuje s provozními náklady, je jí možné uplatnit v případě, kdy jsou provozní náklady neměnné. K výpočtu potřebujeme: úrokovou míru i=5%, počet let n=5, které dosadíme do níže uvedeného vzorce (Synek, 2011):

$$diskontovaná\ hodnota\ nákladů = \frac{1-\left(\frac{1}{1+i}\right)^n}{i}$$

Diskontovanou hodnotu nákladů po dosazení a výpočtu získáme ve výši 4,36. Roční provozní náklad technického řešení I. je 566.490 a právě toto číslo násobíme diskontovanou hodnotou nákladů 4,36 a získáme celkové diskontované náklady technického řešení I. ve výši 2.469.896 Kč. Obdobně získáme celkové diskontované náklady i u provozních nákladů technického řešení II.: 109.834×4,36= 478.876 Kč a stejně postupujme při výpočtu diskontovaných budoucích hodnot nákladů u řešení s dotacemi. Rozdíly v jednotlivých letech oproti výše uvedenému číslu je dáno zaokrouhlováním samotného výpočtu diskontované hodnoty nákladů tj. 4,36, ale i násobením nákladů s odúročitelem. Pro získání představy, která varianta dle této metody je výhodnější jsou desetinné hodnoty zanedbatelné, takže bylo použito

zaokrouhlení. Následující tabulky ukazují diskontované náklady pro obě řešení bez dotací a s dotacemi.

Roky	Náklady technické řešení I.	Odúročitel	Diskontované náklady	Náklady technické řešení II.	Odúročitel	Diskontované náklady
0	3.894.905	1,0000	3.894.905	5.172.653	1,0000	5.172.653
1	566.490	0,9524	539.598	109.834	0,9524	104.606
2	566.490	0,9070	513.806	109.834	0,9070	99.619
3	566.490	0,8638	489.390	109.834	0,8638	94.875
4	566.490	0,8227	466.051	109.834	0,8227	90.360
5	566.490	0,7835	443.845	109.834	0,7835	86.055
Celkem	6.727.355		6.347.595	5.721.823		5.648.168

Tabulka 34: Metoda diskontovaných budoucích hodnot nákladů bez dotace.

Roky	Náklady technické řešení I.	Odúročitel	Diskontované náklady	Náklady technické řešení II.	Odúročitel	Diskontované náklady
0	1.168.472	1,0000	1.168.472	1.551.796	1,0000	1.551.796
1	566.490	0,9524	539.598	109.834	0,9524	104.606
2	566.490	0,9070	513.806	109.834	0,9070	99.619
3	566.490	0,8638	489.390	109.834	0,8638	94.875
4	566.490	0,8227	466.051	109.834	0,8227	90.360
5	566.490	0,7835	443.845	109.834	0,7835	86.055
Celkem	4.000.922		3.621.162	2.100.966		2.027.311

Tabulka 35: Metoda diskontovaných budoucích hodnot nákladů s dotací.

Závěr: Na základě metody diskontovaných budoucích hodnot nákladů je nejvýhodnější varianta technického řešení II. s dotacemi.

14.2.3 Metoda převedených nákladů

Z investičních nákladů bude pořízen dlouhodobý hmotný majetek ve formě HW, který je tvořen servery, počítači atd. a dlouhodobý nehmotný majetek je tvořen SW

licencemi. Cena jednotlivých položek HW a SW je uveden v Příloze I. Pro účely této práce jednotlivé částky byly zaokrouhleny.

Popis	Technické řešení I.	Technické řešení II.
HW	978.610 Kč	1.485.560 Kč
SW licence	414.320 Kč	620.360 Kč
Implementace	1.251.000 Kč	1.522.000 Kč
Školení	575.000 Kč	647.000 Kč
Celkem bez DPH	**3.218.930 Kč**	**4.274.920 Kč**
Celkem s DPH 21%	**3.894.905,30 Kč**	**5.172.653,20 Kč**
Zaokrouhleno	**3.894.905 Kč**	**5.172.623 Kč**
Provozní náklad / 1 rok	566.490 Kč	109.834 Kč
HM: SW a HW	1.392.930 Kč	2.105.920 Kč
Odpisy HW/ 1rok	195.722 Kč	297.112 Kč
Odpisy SW / 1 rok	82.864 Kč	124.072 Kč
Celkem odpis za 1 rok	**278.586 Kč**	**421.184 Kč**
Převedené jednorázové náklady	69.647 Kč	105.296 Kč
Roční průměrné náklady:	914.723 Kč	636.314 Kč

Tabulka 36: Porovnání celkových nákladů v investiční fázi bez dotace

Odpisy: SW je odepisován většinou po dobu tří let a HW (servery a PC) je možné odepisovat po dobu tří až pěti let. Pro účely této práce budou odpisy sjednoceny na dobu pěti let.

- Převedené jednorázové náklady vypočteme násobením úrokové míry i×náklad (Synek, 2011), v našem případě u technické varianty I.: 0,05×1.392.930= 69.647, u technické varianty II.: 0,05×2.105.920=105.296
- Roční průměrný náklad získáme následujícím výpočtem: roční odpisy + převedené jednorázové náklady + provozní náklady (Synek, 2011), tj. u technického řešení I.: 278.586+69.647+566.490=914.723 Kč, technického řešení II.: 421.184+105.296+109.834=636.314 Kč. Obdobně byl výpočet proveden i pro variantu s dotacemi.

Popis	Technické řešení I.	Technické řešení II.
Provozní náklad / 1 rok	566.490 Kč	109.834 Kč
HM: SW a HW	417.879 Kč	631.776 Kč
Celkem odpis za 1 rok	**83.576 Kč**	**126.355 Kč**
Převedené jednorázové náklady	27.212 Kč	31.589 Kč
Roční průměrné náklady:	677.278 Kč	267.787 Kč

Tabulka 37: Porovnání celkových nákladů v investiční fázi s dotací

- Výpočet: i×náklad (Synek, 2011), technické varianty I.: 0,05×417.879= 27.212, u technické varianty II.: 0,05×631.776=31.589
- Roční průměrný náklad vypočteme: roční odpisy + převedené jednorázové náklady + provozní náklad (Synek, 2011) tj. u technického řešení I.: 83.576+27.212+566.490=677.278 Kč, technického řešení II.:126.355+31.598+109.834=267.787 Kč.

Závěr: Efektivnější je ta metoda, která dosahuje nižších celkových ročních průměrných nákladů. V našem případě je to varianta technického řešení II. s dotacemi. Tato metoda nezohledňuje čas, ten bychom mohli zohlednit tak, že náklady násobíme umořovatelem.

14.3 Závěry ekonomické a finanční analýzy

Uvedené skutečnosti v komparaci s výsledky finanční analýzy potvrzují nekomerční charakter projektu, ve kterém jeho hlavní přínosy vycházejí z jeho socioekonomických přínosů pro jednotlivé benefity. Z níže uvedeného celkového přehledu je jednoznačně nejvýhodnější variantou Technické řešení II. s dotací a druhé místo patří Technickému řešení I. s dotací. Stejného výsledku bychom dosáhli, pokud na výsledná data použijeme metodu součtu pořadí. V případě kladení důrazu na provozní náklady se nám jako nejvýhodnější bude jevit Technické řešení II. s dotací a na druhém místě se dostane stejné Technické řešení II. bez dotace, tento závěr potvrdila i metoda převedených nákladů. V případě nepřidělení dotace by první místo připadlo Technickému řešení II. bez dotace a méně výhodnou variantou by bylo Technické řešení I. bez dotace.

Výsledky: Nejvýhodnější (4body), druhé pořadí (3 body), třetí pořadí (2 body), nejméně výhodná (1 bod) varianta.

Ukazatele	TŘ I. bez dotací	TŘ II. bez dotací	TŘ I. s dotacemi	TŘ II. s dotacemi
Hodnota celkových nákladů (investice a provozní náklady)	6.243.355	5.721.823	4.000.922	2.100.966
Hodnota investice	3.894.906	5.172.653	1.168.472	1.551.796
Hodnota provozních nákladů	566.490	109.834	566.490	109.834
NPV čistá současná hodnota	655.297	1.505.406	3.143.554	4.804.904
Index ekonomické rentability	0,168	0,291	2,690	3,096
ROI výnosnost investice	27,52%	30,62%	91,75%	102,05%
Doba návratnosti investice	3,63	3,27	1,09	0,98
Metoda budoucích hodnot diskontovaných nákladů	6.347.595	5.648.168	3.621.162	2.027.311
Metoda převedených nákladů	914.723	636.314	677.278	267.787
Celkem suma bodů	11	20	26	35
Metoda součtu pořadí: suma ukazatelů = 9	1,22	2,22	2,89	3,89

Tabulka 38: Závěry ekonomické a finanční analýzy

Závěr: Na základě výsledků kriteriálních ukazatelů finanční a ekonomické analýzy je možno konstatovat, že všechny projekty technického řešení systému pro zpracování utajovaných informací v organizaci Správa úložišť radioaktivních odpadů

jsou efektivní a dosahují významných socioekonomických přínosů a lze je proto doporučit k financování z Integrovaného operačního programu.

15 ANALÝZA RIZIK PROJEKTU

Kapitola analýza rizik se zabývá odhadnutými riziky celého projektu, jejich dopadem a návrhem opatření, kterými se eliminují hrozby. Rizika projektu je možné rozdělit na projektová, technické - realizační a provozní, legislativní., ekonomická a investiční.

Označení / Popis rizika – projevy rizika
Dopad na projekt
Pravděpodobnost míry naplnění rizika
Akční plán (ošetření rizika) – návrh opatření vedoucí k omezení vlivu rizika.
Kritérium úspěchu – měřitelný cíl nebo výstup.

Tabulka 39: Popis zpracování projektových rizik

15.1 Projektová rizika

Označení / popis rizika	1/ Termíny uvedené v projektu nebudou dodrženy.
Dopad	Vysoký
Pravděpodobnost	Vysoký
Akční plán	Alokovat dostatečné množství kvalitních kapacit, jak na straně dodavatele, tak na straně SÚRAO. Součástí zadávací dokumentace budou požadovány: a) osvědčení podnikatele pro práci s utajovanými informacemi b) předložení seznamu významných zakázek obdobného charakteru c) jmenný seznam osob, které se budou zakázce pracovat. Tím bude zajištěna odbornost, znalost problematiky.
Kritérium úspěchu	Původní termíny harmonogramu budou dodrženy.
Označení / popis rizika	2/ Nebude zajištěna odpovídající součinnost interních pracovníků.
Dopad	Střední
Pravděpodobnost	Střední
Akční plán	V dostatečném předstihu budou alokovány zdroje na straně SÚRAO za účelem poskytnutí požadované součinnosti při vybudování informačního systému.

Kritérium úspěchu	Nedojde k prodlení harmonogramu projektu z důvodů neposkytnutí součinností interními pracovníky SÚRAO.
Označení / popis rizika	3/ Nedojde k alokaci dostatečného množství kvalitních pracovníků na straně dodavatele.
Dopad	Střední
Pravděpodobnost	Střední
Akční plán	Smluvně ošetřit kvalitní pracovníky dodavatele na základě jejich zkušeností a na základě poskytnutých CV.
Kritérium úspěchu	Nedojde k opoždění termínu realizace na straně dodavatele a projekt bude realizován v odpovídající kvalitě.

Tabulka 40: Projektová rizika

15.2 Technická, realizační a provozní rizika

Označení / popis rizika	4/ Prověření systému a udělení certifikátu ze strany NBÚ nebude dodržen v termínu.
Dopad	Vysoký
Pravděpodobnost	Vysoký
Akční plán	Aktivní spolupráce s NBÚ. Eskalování problematiky na nadřízenou organizaci Ministerstvo průmyslu a obchodu s prosbou o intervenci směrem k NBÚ.
Kritérium úspěchu	Certifikát systému bude ze strany NBÚ získán v termínu.
Označení / popis rizika	5/ Schválení bezpečnostní dokumentace pro samotnou realizaci ze strany NBÚ nebude dodržen v termínu.
Dopad	Vysoký
Pravděpodobnost	Střední
Akční plán	Bezpečnostní dokumentace zpracována před zahájením vlastního projektu. Aktivní spolupráce s NBÚ. Eskalování problematiky na nadřízenou organizace Ministerstvo průmyslu a obchodu s prosbou o intervenci směrem k NBÚ.
Kritérium úspěchu	Bezpečnostní dokumentace bude ze strany NBÚ schválena v termínu.

Označení / popis rizika	6/ Termín dodání jednotlivých komponent nebude dodržen.
Dopad	Střední
Pravděpodobnost	Nízká
Akční plán	Aktivní prověřování termínu dodávek. Včasná eskalace možného zpoždění. V projektu vyjma (kryptografického prostředku) jsou vyžadovány standardizované a na trhu běžně dostupné HW a SW komponenty.
Kritérium úspěchu	Nedojde k časovému posunu dodání jednotlivých komponent.
Označení / popis rizika	7/ HW komponenta (jako celek) neprojde měřením kompromitujícího vyřazování.
Dopad	Střední
Pravděpodobnost	Nízká
Akční plán	Informační systém bude umístěn v zónách, které budou proměřeny na požadovaný stupeň, a v kombinaci s HW by mělo být dosaženo výsledného zákonem požadovaného stavu.
Kritérium úspěchu	HW komponenty budou proměřeny na kompromitující vyřazování a budou vyhovovat.
Označení / popis rizika	8/ HW a SW komponenty z pohledu bezpečnosti nebudou vůči sobě kompatibilní.
Dopad	Střední
Pravděpodobnost	Nízká
Akční plán	V projektu jsou vyžadovány: a) standardizované HW a SW komponenty a b) doporučované komponenty ze strany NBÚ a c) s ohledem na Common Criteria. Včasná eskalace problému.
Kritérium úspěchu	HW a SW komponenty budou kompatibilní.
Označení / popis rizika	9/ Správce kryptografického prostředku neprovede zkoušky správy kryptografického prostředku.
Dopad	Střední
Pravděpodobnost	Nízká

Akční plán	Pro zajištění dostupnosti budou vyčleněny dvě osoby s IT vzděláním. Zkoušku je možné opakovat a získat jí po celou dobu instalace projektu. Opakováním nevznikají náklady na školení, ale jen na samotné provedení zkoušky, dané nákladové riziko na sebe přebírá SÚRAO.
Kritérium úspěchu	Správce kryptografického prostředku úspěšné provede zkoušku.

Tabulka 41: Technická, realizační a provozní rizika

15.3 Legislativní rizika

Označení / popis rizika	10/ Dojde k porušení podmínek dotace.
Dopad	Vysoký
Pravděpodobnost	Střední
Akční plán	Organizačně, projektově zařídit, aby byly splněny veškeré podmínky pro poskytnutí dotace, zveřejněné na portále MV a zajištění udržení podmínek po celou dobu udržitelnosti projektu.
Kritérium úspěchu	Dotace je přidělena a vyplacena. Případná kontrola neshledala porušení podmínek, za kterých byla dotace přidělena – nedochází k vrácení peněz.
Označení / popis rizika	11/ Nedostatečná politická podpora projektu.
Dopad	Střední
Pravděpodobnost	Nízká
Akční plán	Realizovat kampaň zacílenou na vedení SÚRAO, za účelem vysvětlení důležitosti a prospěšnosti.
Kritérium úspěchu	Realizace projektu.
Označení / popis rizika	12/ Výrazné legislativní změny.
Dopad	Střední
Pravděpodobnost	Střední
Akční plán	Podepsání smlouvy s dodavatelem řešení zahrnující závazek dodržování shody s legislativou.
Kritérium úspěchu	Systém splňuje shodu s legislativou.

Tabulka 42: Legislativní rizika

15.4 Ekonomická a investiční rizika

Označení / popis rizika	13/ Náklady na realizaci nepřiměřeně přesáhnou náklady spočítané v rámci studie proveditelnosti.
Dopad	Střední
Pravděpodobnost	Střední
Akční plán	Zajistit garanci cen nabídky v souladu s poskytnutím dotace. V případě odůvodněného nárůstu výdajů je nezbytné zajistit jejich pokrytí vlastními zdroji.
Kritérium úspěchu	Náklady na vybudování IS-SURAO-UI nepřerušují očekávané výdaje.
Označení / popis rizika	14/ Dotace na realizaci projektu nebude poskytnuta.
Dopad	Vysoká
Pravděpodobnost	Nízká
Akční plán	Organizačně, projektově a technicky zajistit, aby byly splněny veškeré podmínky pro přijetí dotace zveřejněné na portále MV. Alokace finančních prostředků z vlastního rozpočtu.
Kritérium úspěchu	Dotace je přidělena a vyplacena.

Tabulka 43: Ekonomická a investiční rizika

16 SILNÁ A SLABÁ MÍSTA TECHNICKÝCH ŘEŠENÍ

Při hodnocení slabých a silných stránek stavu podniku, se používá jedna z nejznámějších metod, tzv. SWOT analýza[2], tato analýza je součástí situační analýzy podniku a slouží k základní identifikaci posuzovaného stavu subjektu v prostředí. Našim úkolem však není posoudit postavení organizace Správy úložišť radioaktivního odpadu na trhu, ale pouze posoudit silná a slabá místa obou technických řešení tzn., že využijeme modifikaci SWOT analýzy k identifikaci silných a slabých míst technických řešení. Silná a slabá místa můžeme získat a) dotazníkovým šetřením, kde by byli dotázáni všichni stávající uživatelé a management společnosti SÚRAO a b) nezávislým externím hodnocením – zda byly navrženými informačními systémy dodrženy všechny sledované faktory. Pro účely této práce byla použita varianta b). Na informační systém je možné se podívat z několika hledisek, které jsou rozebrány ve stejném pořadí v jednotlivých hodnoceních.

16.1 Cíle informačního systému a sledované faktory

Cíl je stav, který by nový informační systém pro zpracování utajovaných informací měl dosáhnout, je složen z jednotlivých požadavků a nároků, které na jedné straně byly popsány v analýze potřeb (Analýza potřeb – kapitola 8), ale které můžeme definovat i jako požadované tj. sledované faktory.

Postup:

- Stanovení sledovaných faktorů
- Vymezení sledovaných faktorů
- Každý sledovaný faktor je hodnocen samostatně, zdali byl splněn.
- Každý sledovaný faktor je posouzen z hlediska obou technických variant. To znamená, že slabé a silné místo jednotlivých systémů pak představuje pouze jejich rozdíl.

Sledovaný faktor	Vymezení
Komplexnost řešení	Práce s UI musí zohlednit všechny aspekty mající vliv na informační systém tj. personální, průmyslovou,

[2] Z anglického překladu **S**trengths silné a **W**eaknesses slabé stránky, příležitosti **O**pportunities a hrozby **T**hreats.

Sledovaný faktor	Vymezení
	administrativní, fyzickou bezpečnost, bezpečnost informací a kryptografickou ochranu.
Popis technické nastavení	Technické nastavení informačního systému musí být detailně popsáno a nastaveno v souladu s popisem nastavení v bezpečnostní dokumentaci.
Disková kapacita IS	Informační systém by měl disponovat s dostatečnou kapacitou pro ukládání dat.
Automatizace	Infomační systém by měl usnadnit práci a odstranit přepisování a neustálé kopírování.
Efektivnost systému	Vysoká provozní efektivnost.
Chybovost informaci	Odstranění chybovosti.
Duplicita informací	Odstranění duplicit.
Čitelnost informací	Přehlednost a čitelnost informací.
Kvalita výstupních informací	Přesné, přehledné zpracování doplněné o tabulkové a grafické znázornění.
Vyhledávání informací podle různých parametrů	Větší počet vyhledávacích atributů.
Rychlost zpracování informací	Rychlé zpracování informací.
Reakční doba	Rychlá reakční doba, rychlá odezva. Možnost okamžité zpětné reakce.
Uživatelské prostředí	Uživatelsky přívětivé prostředí tzn. snadná uživatelská práce.
Náročnost na kvalifikaci lidských zdrojů	Nepožadovat vyšší nároky na znalosti uživatelů při práci v systému.
Personální zajištění	Nenavýšení stávajícího počtu zaměstnanců, výhodou snížení počtu zaměstnanců
Výpadek elektřiny	Informační systém by měl být funkční i v případě výpadku dodávky elektrické energie z elektrických sítí.
Nezávislost systému na cizích službách	Informační systém by měl být nezávislý na cizích službách.
Doba splácení	Krátká doba splácení.
Životnost	Dlouhá provozní životnost.

Tabulka 44: Sledované faktory technického řešení I.

16.2 Technické řešení I.

Silné stránky technického řešení I. jsou označeny modře a slabé stránky světlou antracitovou oproti technickému řešení II.

Sledovaný faktor	Splnění	Rozdíly mezi technickými variantami I. a II.
Komplexnost řešení	Splněno	
Popis technické nastavení	Splněno	
Disková kapacita IS	Splněno	
Automatizace	Splněno	Automatizace činnosti, kterou zaměstnanci vykonávali. Ostatní činnosti nebyly automatizovány.
Efektivnost systému	Splněno	
Chybovost informaci	Splněno	
Duplicita informací	Splněno	
Čitelnost informací	Splněno	
Kvalita výstupních informací	Splněno	
Vyhledávání informací podle různých parametrů	Splněno	Technické řešení II. umožňuje díky použitým aplikacím vyhledat podle více atributů.
Rychlost zpracování informací	Splněno	Závislost zpracování na získání informací z poboček.
Reakční doba	Splněno	Závislost na typu dotazů, vyhledání dat minulých splněno rychle, dotazy směřované k novým měřením jsou závislé na získání informací z poboček.
Uživatelské prostředí	Splněno	
Náročnost na kvalifikaci lidských zdrojů	Splněno	
Personální zajištění	Splněno	
Výpadek elektřiny	Splněno	
Nezávislost systému na cizích službách	Splněno	Systém je závislý na stejných službách jako při současném stávajícím stavu. Technické řešení II. nevyžaduje ani tyto služby.
Doba splácení	Splněno	Technické řešení I. s dotací i bez dotace má delší dobu splácení, pokud bereme v potaz i náklady na provoz.
Životnost	Splněno	Technické řešení I. má životnost delší jak technické řešení II., kde systém je závislý na prvcích v centru (tj. server).

Tabulka 45: Slabé a silné stránky technického řešení I.

16.3 Technické řešení II.

Silné stránky technického řešení II. jsou označeny modře a slabé stránky světlou antracitovou oproti technickému řešení I.

Sledovaný faktor	Splnění	Rozdíly mezi technickými variantami I. a II.
Komplexnost řešení	Splněno	
Popis technické nastavení	Splněno	
Disková kapacita IS	Splněno	
Automatizace	Splněno	Automatizace činností, které zaměstnanci nevykonávali.
Efektivnost systému	Splněno	
Chybovost informaci	Splněno	
Duplicita informací	Splněno	
Čitelnost informací	Splněno	
Kvalita výstupních informací	Splněno	
Vyhledávání informací podle různých parametrů	Splněno	Technické řešení II. umožňuje díky použitým aplikacím vyhledat podle více atributů.
Rychlost zpracování informací	Splněno	Nezávislost zpracování na získání informací z poboček.
Reakční doba	Splněno	Nezávislost na typu dotazů.
Uživatelské prostředí	Splněno	
Náročnost na kvalifikaci lidských zdrojů	Splněno	
Personální zajištění	Splněno	
Výpadek elektřiny	Splněno	
Nezávislost systému na cizích službách	Splněno	Systém není závislý na žádných stávajících cizích službách.
Doba splácení	Splněno	Technické řešení s dotací i bez dotace má kratší dobu splácení, pokud bereme v potaz i náklady na provoz.
Životnost	Splněno	Technické řešení I. má životnost delší jak technické řešení II., kde systém je závislý na prvcích v centru (tj. server).

Tabulka 46: Slabé a silné stránky technického řešení II.

Z výše provedené analýzy silných a slabých míst obou technických řešení je zřejmé, že technické řešení II. oproti technickému řešení I. má více benefitů, tj. disponuje více kladnými parametry, které by pro organizaci SÚRAO byly přínosem.

17 ZÁVĚR

Ochrana utajovaných informací se zajišťuje celým komplexem opatření, který je stanoven platnými právními předpisy a normami. Systém těchto pravidel přesně definuje podmínky pro činnosti spojené s tvorbou, zpracováním, distribucí a uchováváním utajovaných informací. To vše při respektování ostatních obecně platných právních předpisů, mezinárodních standardů, zejména EU a NATO a technických norem. Zajistit, aby uvažovaný informační systém byl bezpečný a přitom funkční, je finančně poměrně náročné. Cílem diplomové práce proto bylo vypracovat srovnávací studii proveditelnosti, jejímž výstupem je návrh nejefektivnějšího technického řešení, to vše při respektování výše uvedených normativních podmínek.

V prvé řadě bylo potřebné shromáždit všechny právní předpisy, normy a standardy upravující oblast ochrany utajovaných informací. Dalším krokem bylo definovat a strukturovat takto získané požadavky do jednotlivých oblastí, jako je oblast personální, průmyslová, administrativní, oblast fyzické bezpečnosti a bezpečnosti informačních a komunikačních systémů a oblast kryptografické ochrany.

Dalším logickým krokem bylo modelové provedení analýzy stávajícího stavu informačního systému a bezpečnosti v organizaci Správu úložišť radioaktivního odpadu. Po analýze stávajícího stavu následovala analýza potřeb. Porovnáním zjištěných nároků na informační systém s živým prostředím reálné organizace se požadavky na vlastní technické řešení velice jednoduše a snadno generovaly. Zde bylo nutné ověřit, zdali jsou daná technická řešení bezpečnosti a funkcionality informačních systémů reálná, vhodná pro danou organizaci s ohledem na její zdroje, činnosti, technologie a požadované záruky a zároveň vyhovují požadavkům Národního bezpečnostního úřadu.

Následně byly navrženy dvě varianty technického řešení na pořízení požadovaného informačního systému. Obě technická řešení zohledňují podmínky a determinace definované legislativou, analýzu stávajícího stavu, analýzu potřeb (Například: dostupnost, ochrana před výpadkem, rychlost, chybovost, duplicita dat, kvalita aj.) a kladou důraz na vytvoření řešení počítačové bezpečnosti a řešení datového toku do informačního systému Státního úřadu pro jadernou bezpečnost. V této technologické části bylo potřebné zjistit na jakých hardwarových a softwarových technologiích (Microsoft Windows, Symantec, Adobe, VMware) je možné vybudovat

odpovídající řešení s ohledem na bezpečnostní hodnocení nezávislé organizace Common Criteria. a s podmínkou aby navržená a popsaná technická řešení mohla být zdárně certifikována Národním bezpečnostním úřadem. Pro dlouhodobou udržitelnost informačních systémů byla připočtena k navrženým řešením 20% rezerva diskové kapacity a pamětí pro případný rozvoj informačních systémů. U technického řešení II. byl použit při sestavování serveru konfigurátor výrobce IBM, který vygeneroval podrobnou technickou konfiguraci serveru (IBM), který byl následně v IBM naceněn. Oblast kryptografické ochrany v technickém řešení II. je řešena v obecné rovině, podrobnější popis dle platné legislativy u certifikovaného kryptografického prostředku není možné uvést, s danou konfigurací se mohou seznámit pouze fyzické osoby s příslušným osvědčením tj. prověrkou a certifikátem tj. zkoušky o způsobilosti seznamovat se s kryptografickým prostředkem. Informace o certifikovaných kryptografických prostředcích jsou Národním bezpečnostním úřadem poskytovány na základě písemné a oprávněné žádosti, po splnění podmínek. (Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, 2011).

Mimo návrhu technického řešení bylo dalším cílem diplomové práce provést finanční a ekonomickou analýzu navržených technických řešení. Výsledkem je výběr nejvhodnějšího technického řešení z pohledu socioekonomického a finančního. Toho bylo dosaženo tak, že všechny položky řešení byly oceněny jak ve fázi investiční, tak ve fázi provozní. Výsledné hodnoty technických řešení byly porovnány z hlediska: celkových nákladů, čisté současné hodnoty, indexu ekonomické rentability, výnosnosti investice, doby návratnosti aj. Výsledky daných kriteriálních ukazatelů finanční a ekonomické analýzy prokázaly, že technická řešení systémů pro zpracování utajovaných informací v organizaci Správa úložišť radioaktivních odpadů jsou více či méně efektivní a dosahují významných socioekonomických přínosů a lze je proto doporučit k financování z Integrovaných operačních programů.

Závěr srovnávací studie proveditelnosti patří provedené analýze rizik projektu s definováním způsobu eliminace hrozeb a slovní formulaci silných a slabých míst technických řešení.

Prvním cílem diplomové práce bylo vytvořit srovnávací studii proveditelnosti informačního systému pro nakládání s utajovanými informacemi do stupně utajení Důvěrné v oblasti technologické a ekonomické, která měla pro danou problematiku

navrhnout vhodná a reálná řešení tak, aby byly splněny podmínky dané legislativou a zohledněny potřeby organizace Správy úložišť radioaktivního odpadů. Druhým cílem bylo ocenění investičních a provozních nákladů navržených řešení a provedení ekonomické a finanční analýzy, definování analýzy rizik projektu, slovní formulace silných a slabých míst navrhovaných řešení. Konstatuji, že předloženou prací byly zadané cíle splněny.

Celkově se práce snaží ukázat komplexní přístup při rozhodování o volbě druhu informačního systému pro zpracování utajovaných informací a možnostech jeho provozování se silným akcentem nejen na bezpečnost, ale i na socioekonomickou efektivitu.

SEZNAM POUŽITÝCH ZDROJŮ

1. Acrobat Adobe 11 Czech Standard. In. *Alza.cz.* Dostupné z: http://www.alza.cz/adobe-acrobat-xi-standard-cz-win-full-d370072.htm
2. Bezpečnost. (2015). In *ICZ a.s.* Dostupné z: http://www.i.cz/co-delame/bezpecnost/.
3. Bezpečnost v kostce. (2011). In *chrantesidata.cz.* Dostupné z: http://www.chrantesidata.cz/cs/art/1039-hlavni-strana/.
4. Configuration Tools: IBM Systems: Systém x. In *IBM*. Dostupné z: http://www-03.ibm.com/systems/x/hardware/configtools.html
5. Common Criteria (2015). In *The Common Criteria Portal.* Dostupné z: http://www.commoncriteriaportal.org/.
6. Crecsendo C700. (2014) In *ASKON International s.r.o.* Dostupné z: http://www.askon.cz/Produkty/Autentizace/Cipove-karty-SmartCards/Crecsendo-C700.html.
7. CyberPower BU6600E-FR. In *Alza.cz*. Dostupné z: http://www.alza.cz/cyberpower-bu600e-fr-d504876.htm.
8. Čermák, M. (2013). Analýza rizik: jemný úvod do analýzy rizik. In *CLEVER AND SMART*. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/.
9. Česko. Nařízení vlády č. 522 ze dne 25. prosince 2005, kterým se stanoví seznam utajovaných informací. (2005). In *Sbírka zákonů: Česká republika*. (pp. 9950-9977). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
10. 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. (2008). In *Sbírka zákonů: Česká republika.* (pp. 842-844). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
11. Česko. Vyhláška č. 432 ze dne 16. prosince 2011 o zajištění kryptografické ochrany utajovaných informací. (2011). In *Sbírka zákonů: Česká republika.* (pp. 5712-5730). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
12. 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. (2005). In *Sbírka*

zákonů: Česká republika. (pp. 9978-9993). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.

13. Česko. Vyhláška č. 524 ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. (2005). In *Sbírka zákonů: Česká republika*. (pp. 9994-10008). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
14. Česko. Vyhláška č. 525 ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. (2005). In *Sbírka zákonů: Česká republika*. (pp. 10009-10014). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
15. 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). (2005) In *Sbírka zákonů: Česká republika*. (pp. 10015.10044). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
16. 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). (2005). In *Sbírka zákonů: Česká republika*. (pp. 10045-10078). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
17. Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. (2005). In *Sbírka zákonů: Česká republika*. (pp. 10079-10115). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
18. Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008. (2008). In *Sbírka zákonů: Česká republika.* (pp. 454-460). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
19. Česko. Vyhláška č. 528 ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 a 454/2011. (2011). In *Sbírka zákonů: Česká republika.* (pp. 5888-5919). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.

20. Česko. Vyhláška č. 529 ze dne 15. prosince 2005 o administrativní bezpečnosti a o registrech utajovaných informací. (2005). In *Sbírka zákonů: Česká republika*.(10016-10155). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
21. Česko. Vyhláška č. 532 ze dne 16. prosince 2011 o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013. (2013). In *Sbírka zákonů: Česká republika.* (pp. 7038-7039). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
22. Česko. Zákon č. 29 ze dne 18. ledna 2000 o poštovních službách a o změně některých zákonů (zákon o poštovních službách). (2000). In *Sbírka zákonů: Česká republika*. (pp. 336-350). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
23. Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. (2005). In *Sbírka zákonů: Česká republika*. (7528-7531). Praha, Czechia: Tiskárna Ministerstva vnitra, p.o.
24. Discounted Cash Flows. (2004-2015). In *Trhfirem.cz: Partner pro prodej a akvizice malých a středních firem.* Dostupné z: http://www.trhfirem.cz/cz/discounted-cash-flows.
25. Dočkal, J. (2010). Bezpečnost WLAN v souladu se standardy. *DATA SECURITY MANAGEMENT*. XIV/2, 40.
26. Evolveo. In Alza.cz. Dostupné z: http://www.alza.cz/pc-sestavy/evolveo/18842956-v4057.htm
27. Fellowes 75Cs. In: *Alza.cz*. Dostupné z: http://www.alza.cz/fellowes-75cs-d434776.htm.
28. HP LaserJet Pro 400 M425dw. In *Alza.cz*. Dostupné z: https://www.alza.cz/hp-laserjet-pro-400-m425dw-d368636.htm.
29. IBM System x Top of Rack. (2014) In *IBM*. Dostupné z: http://www-03.ibm.com/systems/xbc/cog/network_switches/network_switches.html.
30. IBM System x3550 M4: Compact, high-performance two-socket server for a widerangeof business-criticalworkloads. (2014). In *IBM*. Dostupné z: http://public.dhe.ibm.com/common/ssi/ecm/en/xsd03131usen/XSD03131USEN.PDF.

31. Instalation Guide: IBM S2 25U Standard Rack and IBM S2 42U Standardr and Expansion Racks. (2008) In. IBM. Dostupné z: ftp://ftp.software.ibm.com/systems/support/system_x_pdf/43w7831.pdf
32. Integrovaný operační program: Modernizace veřejné správy - Rozvoj informační společnosti ve veřejné správě. (2014). In *Ministerstvo vnitra České republiky*. Dostupné z: http://www.mvcr.cz/clanek/strukturalni-fondy-integrovany-operacni-program.aspx.
33. Integrovaný operační program: Technologická centra obcí s rozšířenou působností. (2014). In *Ministerstvo vnitra České republiky*. Dostupné z: http://www.mvcr.cz/clanek/vyzvy-iop-vyzva-iop-c-06-technologicka-centra-obci-s-rozsirenou-pusobnosti.aspx.
34. Integrovaný operační program: Rozvoj služeb eGovernmentu. (2014). In *Ministerstvo vnitra České republiky*. Dostupné z: http://www.mvcr.cz/clanek/vyzva-c-08-k-predkladani-zadosti-o-financni-podporu-v-ramci-integrovaneho-operacniho-programu-na-rozvoj-sluzeb-egovernmentu-v-krajich.aspx.
35. Jednicové náklady. (2014). In: *MANAGEMENT MANIA*. Dostupné z: https://managementmania.com/cs/jednicove-naklady.
36. Junior - Analytik. (2014). In *Acjobs.cz*. Dostupné z: http://www.profesia.cz/prace/advantage-consulting/O1926921.
37. Kindl, J. (2004). *Projektování bezpečnostních systému I. Díl.* (1th ed.). Zlín, Czechia: Univerzita Tomáše Bati ve Zlíně.
38. Mzdová kalkulačka: Čistá mzda. (2015). In *Měšec.cz*. Dostupné z: http://www.mesec.cz/kalkulacky/vypocet-ciste-mzdy/.
39. Lacký, V. (2007). *Bezpečnostní futurologie* (1th ed.). Zlín, Czechia: Univerzita Tomáše Bati ve Zlíně.
40. Lacký, V. (2009). *Speciální bezpečnostní technologie.* (1th ed.). Zlín, Czechia: Univerzita Tomáše Bati ve Zlíně.
41. Lacký, V. (2004). *Technologie komerční bezpečnosti* I. (2th. ed.). Zlín, Czechia: Univerzita Tomáše Bati ve Zlíně.
42. MonitorWare Console - Data Viewer & Analyzer (1988-2005). In. *MonitorWare*. Dostupné z: http://www.mwconsole.com/en/.

43. Náklady. In: *AZ data*. Dostupné z: http://www.az-data.cz/slovnik/naklady.
44. Náklady. In: *HEURECA: Daně & účetnictví*. Dostupné z: http://www.daneaucetnictvi.com/ucetnictvi/naklad.htm.
45. Operační program podnikání a inovace: Program podpory ICT a strategické služby. (2010). In *Ministerstvo průmyslu a obchodu České republiky*. Dostupné z: http://www.mpo-oppi.cz/ict-a-strategicke-sluzby/.
46. OptimAccess: Technické řešení (1997-2014). In *Sodatsw.cz.* Dostupné z: http://www.sodatsw.cz/personalni-audit-jak-optimaccess.
47. Panduit. (1995-2009). In *Kassex.* Dostupné z: http://www.kassex.cz/produkty/panduit.
48. Pekárek, O., Čížek, V. (2007). *Práce s agenturními a elektronickými informacemi*.(1th ed.). České Budějovice, Czechia: Vysoká škola evropských a regionálních studií.
49. Piper, F., Murphy, S. (2006). *Kryptografie*. In. Pavel Mondschein (ed). Praha: Czechia: Dokořán.
50. Požar, J. (2005) *Informační bezpečnost.* (1th ed.) Plzeň, Czechia: Vydavatelství a nakladatelství Aleš Čeněk.
51. Přehled vztahů k problematice. In *Přehled vztahu k problematice spoření, důchody, anuitní splácení úvěrů: Pro SVŠE Znojmo.* Dostupné z: http://svse.sweb.cz/materialy/vzorce_3.pdf.
52. Pszczolka, M. (2005). Objektová bezpečnost: Úvod do problematiky. In *Specialista.info.* Dostupné z: http://magazin.specialista.info/view.php?cisloclanku=2005100201.
53. Steiner, O. (2010). Úskalí při nasazování elektronického podpisu. *DATA SECURITY MANAGEMENT*. XIV/2, 48.
54. Studie proveditelnosti: Feasibility Study, FS. In *Sieber Uchytil s.r.o.* Dostupné z: http://sieber-uchytil.cz/studie-proveditelnosti-feasibility.html.
55. Studie proveditelnosti. (2014) In: *PDQM, s.r.o.* Dostupné z: http://www.pdqm.cz/Analysis/Studie-proveditelnosti.html.
56. Synek, M. (2011). In *Manažerská ekonomika*. (5st. ed., pp. 471). Praha, Czechia: Expert (Grada).

57. System x rack and powerinfrastructureoptions. In *IBM*. Dostupné z: http://www-03.ibm.com/systems/x/options/rackandpower/rack.html.
58. Šustova, P. (2007). Optimální volby zdroje – porovnání nákladů na vytápění – II. díl. In: *tzbinco.cz*. Dostupné z: http://www.tzb-info.cz/4469-optimalni-volby-zdroje-porovnani-nakladu-na-vytapeni-ii-dil.
59. Tuček, P. (2010). TMP aneb důvěryhodný počítač. *DATA SECURITY MANAGEMENT*. XIV/2, 34.
60. Uložiště radioaktivních odpadů. In *SÚRAO: Správa uložišť radioaktivních odpadů*. Dostupné z: http://www.surao.cz/cze/Uloziste-radioaktivnich-odpadu.
61. Utajované informace. (2014). In *ICZ a.s.* Dostupné z: http://www.i.cz/co-delame/bezpecnost/utajovane-informace/.
62. Vacca, J. R. (2009). *Computer and Information Security Handbook*. (1th ed.). Burlington, England: Morgan Kaufmann.
63. Volner, Š. (2009). *Bezpečnosť v 21. storočí*. (1th ed.). Bratislava, Slovakia: Iris.
64. Williams, B., Sawyer, S. (2010). *Using Information Technology*. (9th ed.). New York, United States of America: Career Education.
65. Žilka, R. (2009). Utajování dat v souborových systémech. *DATA SECURITY MANAGEMENT*. XIII/2, 34.
66. 3580S5E. In *Senetic.cz*. Dostupné z: http://www.senetic.cz/product/3580S5E.

SEZNAM OBRÁZKŮ A TABULEK

SEZNAM PLATNÉ LEGISLATIVY, NOREM A STANDARDŮ

	Platná legislativa
Nařízení vlády č. 522/2005 Sb.	kterým se stanoví seznam utajovaných informací, v platném znění, ve znění 240/2008 Sb.
Vyhláška č. 363/2011 Sb.	o personální bezpečnosti a o bezpečnostní způsobilosti ve znění vyhlášky č. 415/2013 Sb.,
Vyhláška č. 405/2011 Sb.	o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb.
Vyhláška č. 432/2011 Sb.	o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.
Vyhláška č. 363/2011 Sb.	o personální bezpečnosti a o bezpečnostní způsobilosti ve znění vyhlášky č. 415/2013 Sb.,
Vyhláška č. 405/2011 Sb.	o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb.
Vyhláška č. 432/2011 Sb.	o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.
Vyhláška č. 525/2005 Sb.	o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.
Vyhláška č. 528/2005 Sb.	o fyzické bezpečnosti a certifikaci technických prostředků, v platném znění, ve znění č. 19/2008 Sb. a 454/2011 Sb.
Vyhláška č. 529/2005 Sb.	o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.
Zákon č. 412/2005 Sb.	o ochraně utajovaných informací a o bezpečnostní způsobilosti, v platném znění, v aktuálním znění – zákonů č. 119/2007, 177/2007, 296/2007, 32/2008, 255/2011 Sb.

	Platná legislativa
Zákon č. 413/2005 Sb.	o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti – změnový zákon.

Tabulka 47: Platná legislativa

	Ostatní obecně závazné právní předpisy
Bezpečnostní strategie České republiky	Bezpečnostní strategie České republiky ze dne 8. Září 2011, ISBN: 978-80-7441-005-5
Metodický pokyn NBÚ MP-USB	o používání Firmware a USB portů a bezpečnostní aspekty paměti typu „flash“.
Nařízení vlády č. 616/2006 Sb.	o technických požadavcích na výrobky z hlediska elektromagnetické kompatibility.
Sdělení MZV č. 221/1998 Sb.	o sjednání Evropské úmluvy o poskytování informací o cizím právu a Dodatkového protokolu k Evropské úmluvě o poskytování informací o cizím právu.
Ústavní zákon č. 110/1998 Sb.	o bezpečnosti státu.
Zákon České národní rady 133/1985 Sb.	o požární ochraně.
Zákon č. 101/2000 Sb.	o ochraně osobních údajů.
Zákon č. 106/1999 Sb.	o svobodném přístupu k informacím.
Zákon č. 18/1997 Sb.	o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů.
Zákon č. 181/2014 Sb.	o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
Zákon č. 185/2011 Sb.	zákoník práce, ve znění pozdějších předpisů.

	Ostatní obecně závazné právní předpisy
Zákon č. 222/1999 Sb.	o zajišťování obrany České republiky.
Zákon č. 227/2000 Sb.	o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
Zákon č. 239/2000 Sb.	o integrovaném záchranném systému a o změně některých zákonů.
Zákon č. 240/2000 Sb.	o krizovém řízení a o změně některých zákonů (krizový zákon).
Zákon č. 241/2000 Sb.	o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů.
Zákon č. 273/2008 Sb.	o Policii České republiky.
Zákon č. 365/2000 Sb.	o informačních systémech veřejné správy a o změně některých dalších zákonů.
Zákon č. 468/2011 Sb.	o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.
Zákon č. 499/2004 Sb.	o archivnictví a spisové službě a o změně některých zákonů.
Zákon č. 89/2012 Sb.	Občanský zákoník.
Zákon č. 93/2009 Sb.	o auditorech a o změně některých zákonů (zákon o auditorech).
Zákon č. 95/2005 Sb.	o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, a některé další zákony.

Tabulka 48: Ostatní obecně závazné předpisy

	Mezinárodní standardy EU a NATO
Nařízení Rady	kterým se provádí článek 24 Smlouvy o založení

	Mezinárodní standardy EU a NATO
31958R0003(01)	Evropského společenství pro atomovou energii (doplněné bezpečnostní předpisy).
Rozhodnutí Rady 2013/488/EU	o bezpečnostních pravidlech na ochranu utajovaných informací EU.
Rozhodnutí Rady 2001/264/ES	Bezpečnostní předpisy Rady.
Rozhodnutí Komise 32001D0844	Bezpečnostní předpisy Komise.
Rozhodnutí Komise 32005D0094	kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom (2005/94/ES, Euratom), o bezpečnosti informací.
C-M/2002/49	Security within the North Atlantic Treaty Organization (NATO).
CM/2002/49-COR3	Security within the North Atlantic Treaty Organization (NATO).
CM/2002/49-COR6	Security within the North Atlantic Treaty Organization (NATO).
CM/2002/49-COR8	Security within the North Atlantic Treaty Organization (NATO).
CM/2002/49-COR9	Copy for Compendiun Security policy - Security within the North Atlantic Treaty Organization (NATO).
AC/35-D/2000	Directive on Personal Security.
AC/35-D/2001	Directive on Physical Security.
AC/35-D/2002	Directive on Security of Information.
AC/35-D/2003	Directive on Industrial Security.
AC/35-D/2004	Primary Directive on INFOSEC.
AC/35-D/2005	INFOSEC Management Directive for CIS.

	Mezinárodní standardy EU a NATO
AC-35-D-2000-REV7	Directive on Personal Security.
AC-35-D-2001-REV2	Directive on Physical Security.
AC-35-D-2002-REV4	Directive on Security of Information.
AC-35-D-2003-REV4	Directive on Industrial Security.
AC-35-D-2004-REV3	Primary Directive on INFOSEC.
AC-35-D-2005-REV2	INFOSEC Management Directive for CIS.

Tabulka 49: Mezinárodní standardy EU a NATO

	Hlavní technické normy
(010336) ČSN ISO/TR 10017	Návod k aplikaci statistických metod v ISO 9001:2000
(010350) TNI 01 0350	Management rizik - Slovník (Pokyn 73)
(010351) ČSN ISO 31000	Management rizik - Principy a směrnice
(010352) ČSN EN 31010	Management rizik - Techniky posuzování rizik
(369040) ČSN ISO/IEC 15939	Systémové a softwarové inženýrství - Proces měření
(369043) ČSN ISO/IEC 90003	Softwarové inženýrství - Směrnice pro použití ISO 9001:2000 na počítačový software
(369789) ČSN ISO/IEC 15408-1	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a obecný model
(369789) ČSN ISO/IEC 15408-2	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty
(369789) ČSN ISO/IEC 15408-3	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk
(369797) ČSN ISO/IEC	Informační technologie - Bezpečnostní techniky -

	Hlavní technické normy
27001	Systémy řízení bezpečnosti informací - Požadavky
(369798) ČSN ISO/IEC 27002	Informační technologie - Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
(369790) ČSN ISO/IEC 27003	Informační technologie - Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací
(369790) ČSN ISO/IEC 27004	Informační technologie - Bezpečnostní techniky – Řízení bezpečnosti informací - Měření
(369790) ČSN ISO/IEC 27005	Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací
(369790) ČSN ISO/IEC 27006	Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
(369790) ČSN ISO/IEC 27007	Informační technologie - Bezpečnostní techniky - Směrnice pro audit systémů řízení bezpečnosti informací
(369790) ČSN ISO/IEC 27032	Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost

Tabulka 50: Hlavní technické normy

SEZNAM POUŽITÝCH ZKRATEK

Název zkratky	Celý název
AD	ActiveDirectory
AES	AdvancedEncryption Standard, šifrovací algoritmus
AM	Administrativní pomůcka
CA	Certifikační autorita
CBA	Cost-benefit analysis, analýza nákladů a přínosů
CD	CompactDisc
CEA	Cost-effeciencyanalysis, analýza efektivity nákladů
CF	Cash Flow
CPU	CentralProcessing Unit, Procesor
CRL	CertificateRevocation List
CV	Curricullum Vitae, životopis
ČSH	Čistá současná hodnota
DC	DomainController, doménový řadič
DCF	Diskontované Cash Flow
DER	DER zakódovaný certifikát
DES	Data Encryption Standard
DHCP	Dynamic Host ConfigurationProtocol
DNS	DomainNameSystém
DoS	DenialofService
DVD	Digital VersatileDisc nebo Digital Video Disc
EIA	EnvironmentalImpactAssessment, vyhodnocení vlivů na životní prostředí
EKV	Elektronická kontrola vstupu
EPS	Elektronický protipožární systém
EZS	Elektronický zabezpečovací systém
FO	Fyzická osoba
FS	File Server, souborový server
GB	Gigabite

Název zkratky	Celý název
HDD	Hard disk drive, pevný disk
HTML	HyperText MarkupLanguage
http	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technologies, informační a komunikační technologie
IP	Internet Protocol
ISA	Industry Standard Architecture
IT	Informační technologie
KS	Komunikační systém
LDAP	LightweightDirectory Access
Mbps	Megabit za sekundu
MS	Microsoft
MV	Ministerstvo vnitra
NATO	NorthAtlanticTreatyOrganization, Severoatlanská aliance
NBÚ	Národní bezpečnostní úřad
NIST	National Institute of Standards and Technology
NPV	Net Present Value, čistá současná hodnota
NTP	Network Time Protocol
OCR	Optical Character Recognition, optické rozpoznávání znaků
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	Print Server, tiskový server

Název zkratky	Celý název
ROI	Return on Investment, Výnosnost investice
SSL	Secure Sockets Layer
SÚJB	Státní úřad pro jadernou bezpečnost
SÚRAO	Správa úložišť radioaktivního odpadu
SW	Software
TB	Terabyt
TCP	Transmission Control Protocol - protokol transportní vrstvy v sadě protokolů TCP/IP používaných v síti Internet.
UPS	Uninterruptible Power Supply – nepřerušitelný zdroj energie
Úřad	Národní bezpečnostní úřad
WINS	Windows Internet Naming Service

Tabulka 51: Seznam zkratek

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 informacemi v daném informačním systému, tak jako správce informačního systému, nebo bezpečnostní správce.

Pojem	Výklad
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	HyperText 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 základě shodných charakteristik.

Pojem	Výklad
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 Microsoft.

Pojem	Výklad
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 identifikačníčíslo.
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 s bezpečnostním atributem, jež pro subjekt vyjadřuje úroveň oprávnění. 2) Ochrana integrity bezpečnostního atributu. 3)

Pojem	Výklad
	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 přístup	Je omezení přístupu subjektů do systémů, je založený na kontrole přístupových práv, přičemž každý, kdo má přístupová práva může zvolit, na které další subjekty tato přístupová práva budou

Pojem	Výklad
	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.

Tabulka 52: Seznam pojmů

PŘÍLOHA: KALKULACE PRO INVESTIČNÍ FÁZI

Náklady obou technických řešení v investiční fázi byly rozděleny na: 1) dlouhodobý majetek hmotný movitý, který bude tvořen HW, 2) dlouhodobý majetek nehmotný, který představují dodávané licence tedy SW a 3) implementaci a školení.

Všechny uvedené hodnoty jsou v reálných cenách roku 2014 včetně DPH ve výši 21%. Výrobci HW (IBM a Lenovo) byli požádáni o speciální cenu (special bid), to je cena, kterou při daném množství může výrobce zákazníkovi nabídnout a garantovat po dobu 4 měsíců, do stejné speciální ceny byl zařazen SW získaný od výrobce HW. Softwarové licence Microsoft jsou uvedeny z licenčního kanálu Microsoft Open licence pro státní správu a licence Symantec jsou převzaty v programu GOV. Ostatní ceny byly vyžádány a nalezeny na internetových obchodech společností: Alza.cz, Abacus, MonitorWare a ICZ.

Technické řešení I.

Zálohování I.

Množství	Popis - Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HW: IBM Storage TS2250 Tape Drive Model H5S	37.000 Kč	37.000 Kč
1x	HW: IBM 6Gb SAS HBA	3.000 Kč	3.000 Kč
1x	HW: IBM Ultrium 5 Data Cartridge- 5-pack	4.300 Kč	4.300 Kč
1x	HW: IBM Mini-SAS/mini-SAS 1x Cable	600 Kč	600 Kč
1x	SW: Symantec Backup Exec 2010 for Windows Server	14.900 Kč	14.900 Kč
	Cena celkem bez HW		**59.800 Kč**
	Cena celkem s DPH		**72.358 Kč**
	Z toho HW	44.900 Kč	54.329 Kč
	Z toho SW	14.900 Kč	18.029 Kč
	Celkem	**59.800 Kč**	**72.358 Kč**

Tabulka 53: Kalkulace - Zálohování – Technické řešení I.

Pracovní stanice I.

- Stanice ThinkCentre E73 10DR je v provedení věž, 1x Pentium G3240/ 3.1 GHz, RAM 4GB, HDD 500 GB, DVD SuperMulti, HD Grafits, GigE, Windows 7 Pro 64-bit/Windows 8.1 downgrade, předem instalované W7.
- EVOLVEO 7900 je v provedení, věž AMD FX-4300 4core 3.8GHz, 8MB, socket AM3+, 95W Box, základní deska MB AM3+ 760G 4x DDR3, 6xSATA, PCIE, GLAN, 4xUSB 3.8, 8x USB2.0, DVI, HDMI,D-Sub., microATX, 4GB RAM, HDD 250GB, DVD-RW LG, Windows 7 Pro 64-bit/Windows 8.1 downgrade, předem instalované W7 (Alza.cz).

Množství	Popis – Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
22x	HW: Lenovo ThinkCentre E73 10DR	8.500 Kč	187.000 Kč
22x	HW: Lenovo ThinkPlus Myš	205 Kč	4.510 Kč
22x	HW: Lenovo ThinkPlus Klávesnice	540 Kč	11.880 Kč
2x	HW: EVOLVEO Zeppelim 7900	8.400 Kč	16.800 Kč
24x	HW: Lenovo LT1952p - LED display - 19" černý	3.170 Kč	73.680 Kč
24x	HW: CyberPower BU600E-FR	850 Kč	20.400 Kč
24x	HW: HID Omnikey 3121 USB - čtečka čipových karet	350 Kč	8.400 Kč
100x	HW: HID Crescendo C700 - čipová karta	300 Kč	57.040 Kč
100x	HW: Corsair Voyager 32 GB – Flash disk USB 3.0	645 Kč	64.500 Kč
1x	SW: Windows Server Standard - pro zálohovací stanici EVOLVEO	19.400 Kč	19.400 Kč
14x	SW: Symantec Protection Suite Enterprise Edition 4.0 a podpora	980 Kč	13.720 Kč

Množství	Popis – Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
22x	SW: Sodatsw OptimAccess	550 Kč	12.100 Kč
22x	SW: ICZ Protect for Windows	3.500 Kč	77.000 Kč
22x	SW: Microsoft Office Standard 2013	7.400 Kč	162.800 Kč
22x	SW: Adobe Acrobat 11 Czech Standard	5.200 Kč	114.400 Kč
	Cena celkem bez DPH		**843.630 Kč**
	Cena celkem s DPH		**1.020.792,30 Kč**
	Z toho HW	444.210 Kč	537.494,10 Kč
	Z toho SW	399.420 Kč	483.298,20 Kč
	Celkem	**843.630 Kč**	**1.020.792,30 Kč**

Tabulka 54: Kalkulace - Pracovní stanice – Technické řešení I.

Řízení přístupu, souborové a tiskové služby I.

Množství	Popis – Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HP LaserJet Pro 400 M	11.300 Kč	11.300 Kč
2x	Fellowers 75Cs	4.700 Kč	9.400 Kč
	Cena celkem bez DPH		20.700 Kč
	Cena celkem s DPH		25.047 Kč
	Z toho HW	20.700 Kč	25.047 Kč
	Celkem	20.700 Kč	25.047 Kč

Tabulka 55: Kalkulace - Tiskárna a skartovačka – Technické řešení I.

Implementace I.

Množství	Práce - Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
1x	Tvorba Bezpečnostní	400.000 Kč	400.000 Kč

Množství	Práce - Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
	dokumentace		
20x	Instalace stanic ThinkCentre	4.000 Kč	80.000 Kč
2x	Instalace stanic EVOLVEO	10.000 Kč	20.000 Kč
1x	Instalace CA, PKI a nastavení klíčového hospodářství	300.000 Kč	300.000 Kč
1x	Instalace zálohování	80.000 Kč	80.000 Kč
1x	Instalace tiskárny	5.000 Kč	5.000 Kč
22x	Instalace bezpečnostních testů	3.000 Kč	66.000 Kč
1x	Podpora při certifikaci	100.000 Kč	100.000 Kč
	Cena celkem bez DPH		**1.051.000 Kč**
	Cena celkem s DPH		**1.271.710 Kč**

Tabulka 56: Kalkulace - Implementace – Technické řešení I.

Školení I.

Množství	Školení – Technické řešení I.	Cena za kus bez DPH	Cena celkem bez DPH
55x	Školení uživatelů	8.000 Kč	440.000 Kč
1x	Školení bezpečnostního správce	60.000 Kč	60.000 Kč
1x	Školení správce informačního systému	60.000 Kč	60.000 Kč
1x	Školení pověřené obsluhy pracovní stanice s SÚKL	15.000 Kč	15.000 Kč
	Cena celkem bez DPH		**575.000 Kč**
	Cena celkem s DPH		**695.750 Kč**

Tabulka 57: Kalkulace - Školení – Technické řešení I.

Technické řešení II.

Kabeláž, rozbočovače, UPS, Switch II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HW: IBM 25U Standard Rack Cabinet- RACK	24.000 Kč	24.000 Kč
1x	HW: IBM Keyboard with integrated Poiting Device 3m cable/black/USB/ CZ	1.500 Kč	1.500 Kč
1x	HW: IBM 1U 18.5in Standard Console Kit	18.900 Kč	18.900 Kč
6x	HW: IBM 1.5m, 10A/100-250V, C13 to IEC 320-C14	50 Kč	300 Kč
1x	HW: IBM 1500 LCD 2U Rack–UPS	10.500 Kč	10.500 Kč
2x	HW: IBM System Networking RackSwitch G7052	41.000 Kč	82.000 Kč
	Cena celkem bez DPH		**137.200 Kč**
	Ceny celkem s DPH		**166.012 Kč**
	Z toho HW	137.200 Kč	166.012 Kč
	Celkem	**137.200 Kč**	**166.012 Kč**

Tabulka 58: Kalkulace - Kabeláž, rozbočovač, UPS a Switch – Technické řešení II.

Servery II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HW: IBM Server x3550 M4, Xeon 4C E5-2609 2,4 GHz/1066 MHz/10MB, 1x4 GB	42.000 Kč	42.000 Kč
1x	HW: Intel Xeon 4C Model E5-2609 Processor 2,4 GHz/1066 MHz - druhý CPU	9.500 Kč	9.500 Kč
1x	HW: IBM 4 GB PC3L-10600 CL9 ECC DDR3 1333 MHz LP	1.950 Kč	1.950 Kč

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
	RDIMM		
4x	HW: IBM 8 GB PC3L-10600 CL9 ECC DDR3 1333 MHz LP RDIMM	3.200 Kč	12.800 Kč
5x	HW: IBM 300 GB HDD 2,5in SFF G2HS 10K 6Gbps SAS HDD	3.300 Kč	16.500 Kč
1x	HW: IBM ServeRAID M5110SAS/SATA Controller for IBM Systém x	4.000 Kč	4.000 Kč
1x	HW: IBM ServeRAID M5100 Series 512 MB Cache/RAID 5 Upgrade for IBM Systém x	1.000 Kč	1.000 Kč
	HW: IBM ServeRAID M5100 Series Battery Kit for IBM Systém x	1.700 Kč	1.700 Kč
1x	HW: IBM 550W Hight Efficiency Platinum AC Power Supply	2.400 Kč	2.400 Kč
1x	HW: IBM Ultraslim Enhanced SATA Multi-Bunner- DVD	700 Kč	700 Kč
1x	HW: HID Omnikey 3121 USB - čtečka čipových karet	350 Kč	350 Kč
1x	HW: Crescendo C700 - čipová karta	300 Kč	300 Kč
4x	SW: MS Windows Serveru 2012 Standard Edition	18.000 Kč	72.000 Kč
20x	SW: MS Windows Server CAL 2012 Device	600 Kč	12.000 Kč
1x	SW: MS SQL Server Standard 2014	18.200 Kč	18.200 Kč
16x	SW: MS SQL server Standard 2014 CAL Device	4.200 Kč	67.200 Kč
1x	SW: MS Exchange Standard	14.300 Kč	14.300 Kč

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
	2013		
20x	SW: MS Exchange Standard CAL Device	1.400 Kč	28.000 Kč
1x	SW: MonitorWare Console Base Systém	1.400 Kč	1.400 Kč
	Cena celkem bez DPH		**306.300 Kč**
	Cena celkem s DPH		**370.623 Kč**
	Z toho HW	93.200 Kč	112.772 Kč
	Z toho SW	213.100 Kč	257.851 Kč
	Celkem	**306.300 Kč**	**370.623 Kč**

Tabulka 59: Kalkulace - Servery – Technické řešení II.

Zálohování II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HW: IBM Storage TS2250 Tape Drive Express Model H5S	37.000 Kč	37.000 Kč
1x	HW: IBM 6Gb SAS HBA	3.000 Kč	3.000 Kč
1x	HW: IBM 19-inch Rack Mount Kit	700 Kč	700 Kč
5x	HW: IBM Ultrium 5 Data Cartridge- 5-pack	4.300 Kč	4.300 Kč
1x	HW: IBM 2M Mini-SAS/Mini-SAS 1x Cable	600 Kč	600 Kč
1x	SW: Symantec Backup Exec 2014 for Windows Server	14.900 Kč	14.900 Kč
3x	SW: Symantec Backup Exec 2014 for Agent for Windows Server	8.900 Kč	26.700 Kč
1x	SW: Symantec Backup Exec 2014 Agent for Microsoft	14.900 Kč	14.900 Kč

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
	SQL Server		
2x	SW: Symantec Backup Exec 2014 Option Exchange Mailbox to 10 Users	3.000 Kč	6.000 Kč
	Cena celkem bez DPH		**108.100 Kč**
	Cena celkem s DPH		**130.801 Kč**
	Z toho HW	45.600 Kč	55.176 Kč
	Z toho SW	62.500 Kč	75.625 Kč
	Celkem	**108.100 Kč**	**130.801 Kč**

Tabulka 60: Kalkulace - Zálohování – Technické řešení II.

Pracovní stanice II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
16x	HW: Lenovo ThinkCentre E73 10DR	8.500 Kč	136.000 Kč
16x	HW: Lenovo ThinkPlus Myš	205 Kč	3.280 Kč
16x	HW: Lenovo ThinkPlus Klávesnice	540 Kč	8.640 Kč
6x	HW: EVOLVEO Zeppelim 7900	8.400 Kč	50.400Kč
22x	HW: Lenovo LT1952p - LED display - 19" černý	3.170 Kč	69.740 Kč
9x	HW: CyberPower BU600E-FR	850 Kč	7.650 Kč
22x	HW: HID Omnikey 3121 USB - čtečka čipových karet	350 Kč	7.700 Kč
100x	HW: HID Crescendo C700 - čipová karta	300 Kč	30.000 Kč
10 Kč	HW: Corsair Voyager 32	665 Kč	6.650 Kč

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
	GB – Flash disk USB		
12x	SW: Symantec Protection Suite Enterprise Edition 4.0 a podpora	980 Kč	11.760 Kč
20x	SW: Sodatsw OptimAccess	550 Kč	11.000 Kč
20x	SW: ICZ Protect for Windows	3.500 Kč	70.000 Kč
20x	Microsoft Office Standard 2013	7.400 Kč	148.000 Kč
20x	SW: Adobe Acrobat 11 Czech Standard	5.200 Kč	104.000 Kč
	Cena celkem bez DPH		**664.820 Kč**
	Cena celkem s DPH		**804.432,20 Kč**
	Z toho HW	320.060 Kč	387.272,60 Kč
	Z toho SW	344.760 Kč	417.159,60 Kč
	Celkem	**664.820 Kč**	**804.432,20**

Tabulka 61: Kalkulace – Pracovní stanice – Technické řešení II.

Řízení přístupu, souborové a tiskové služby II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
1x	HP LaserJet Pro 400 M	11.300 Kč	11.300 Kč
2x	Fellowers 75Cs	4.700 Kč	9.400 Kč
	Cena celkem bez DPH		20.700 Kč
	Cena celkem s DPH		25.047 Kč
	Z toho HW	20.700 Kč	25.047 Kč
	Celkem	**20.700 Kč**	**25.047 Kč**

Tabulka 62: Kalkulace - Tiskárna a skartovačka – Technické řešení II.

Kryptografický prostředek II.

Množství	Popis – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
5x	ICZ LANPCS	80.000 Kč	400.000 Kč
	Cena celkem bez DPH		**400.000 Kč**
	Cena celkem s DPH		**484.000 Kč**
	Z toho HW	400.000 Kč	484.000 Kč
	Celkem	**400.000 Kč**	**484.000 Kč**

Tabulka 63: Kalkulace - Kryptografický prostředek – Technické řešení II.

Implementace II.

Množství	Práce – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
1x	Tvorba Bezpečnostní dokumentace	400.000 Kč	400.000 Kč
1x	Instalace aktivních prvků	60.000 Kč	60.000 Kč
1x	Instalace serveru, VMware, SQL	200.000 Kč	200.000 Kč
22x	Instalace stanic ThinkCentre	3.000 Kč	66.000 Kč
6x	Instalace kryptografického prostředku	10.000 Kč	60.000 Kč
1x	Instalace CA, PKI a nastavení klíčového hospodářství	250.000 Kč	250.000 Kč
1x	Instalace zálohování	100.000 Kč	100.000 Kč
1x	Instalace sítové tiskárny	20.000 Kč	20.000 Kč
22x	Instalace bezpečnostních testů	3.000 Kč	66.000 Kč
1x	Podpora při certifikaci	100.000 Kč	100.000 Kč
	Cena celkem bez DPH		**1.322.000 Kč**
	Cena celkem s DPH		**1.599.620 Kč**

Tabulka 64: Kalkulace - Implementace – Technické řešení II.

Školení II.

Množství	Školení – Technické řešení II.	Cena za kus bez DPH	Cena celkem bez DPH
55x	Školení uživatelů	8.000 Kč	440.000 Kč
1x	Školení bezpečnostního správce	60.000 Kč	60.000 Kč
1x	Školení správce informačního systému	60.000 Kč	60.000 Kč
1x	Školení správce kryptografické ochrany	72.000 Kč	72.000 Kč
1x	Školení pověřené obsluhy pracovní stanice s SÚKL	15.000 Kč	15.000 Kč
	Cena celkem bez DPH		**647.000 Kč**
	Cena celkem s DPH		**782.870 Kč**

Tabulka 65: Kalkulace - Školení – Technické školení II.

Fyzická bezpečnost - náklady společné pro obě řešení

Množství	Fyzická bezpečnost	Cena za kus bez DPH	Cena celkem bez DPH
4x	OMO 1K/3Ocelová mříž jednokřídlová pro běžné okno od výrobce AŽD Praha s.r.o. (jen dvě lokality mají okna)	12.000 Kč	48.000 Kč
12x	MRB Sazovice Bezpečnostní dveře BEDEX Vario V3 s jednokřídlové 900x2000	13.300 Kč	159.600 Kč
12x	Rozvorový zámek MUL-T-LOCK typ lock case 235 a cylindrická vložka	4.000 Kč	48.000 Kč
5x	Ústředna EZS – TP- 4-20 GSM od výrobce Tecnoalarm	11.900 Kč	59.500 Kč

Množství	Fyzická bezpečnost	Cena za kus bez DPH	Cena celkem bez DPH
16x	Detektor pohybu IR 2000 od výrobce Tecnoalarm	800 Kč	25.000 Kč
12x	TP-020-LCD Klávesnice s indikací LED a LCD Displejem od výrobce Tecnoalarm (4 centrum a 2 na lokality) včetně záložních baterii	3.900 Kč	46.800 Kč
1x	Mobilní skříňový trezor TLA 13 od výrobce P-KOVO Brno s.r.o.	49.900 Kč	49.900 Kč
4x	Malý mobilní skříňový trezor TLA 13 od výrobce P-KOVO Brno s.r.o.	8.000 Kč	32.000 Kč
1x	Instalace	200.000 Kč	200.000 Kč
	Cena celkem bez DPH		**668.800 Kč**
	Cena celkem s DPH		**809.248 Kč**
	Z toho HW	468.800 Kč	567.248 Kč
	Z toho implementace	200.000 Kč	242.000 Kč
	Celkem	**668.800 Kč**	**809.248 Kč**

Tabulka 66: Kalkulace - Náklady fyzické bezpečnosti pro Technické řešení I. a II.