Koncept specializovaného pracoviště pro odhalování kybernetické trestné činnosti

Concept of specialized workplace for cyber crime investigations

Bc. Jakub Velička

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Jakub VELIČKA**
Osobní číslo:	**A08546**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Koncept specializovaného pracoviště pro odhalování kybernetické trestné činnosti**

Zásady pro vypracování:

1. **Pro vlastní potřebu zpracujte rešerši literatury a pramenů, které se vztahují k tématu diplomové práce.**
2. **Definujte kybernetickou trestnou činnost současnosti, vývoj, trendy, očekávaný budoucí vývoj.**
3. **Vypracujte dokumentaci – koncept specializovaného pracoviště pro boj s kybernetickým zločinem.**
4. **Stanovte požadavky nutné k realizaci pracoviště – ekonomické hledisko, časová náročnost, nutné zdroje.**
5. **Podrobně popište problematiku realizace pracoviště včetně technického vybavení, personálního obsazení, technické specifikace a zabezpečení.**
6. **Uveďte v obecné i praktické rovině metodologické postupy činnosti pracoviště.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **STRAUS, Jiří. Kriminalistická metodika. Plzeň : Aleš Čeněk s.r.o., 2006. ISBN 80-86898-66-0. s. 271-286.**
2. **HNÍK, Václav. KRULÍK, Oldřich. Zahraniční inspirace související s tématem kybernetických hrozeb. 2007.**
3. **REYES, Anthony. WILES, Jack. The Best Damn Cybercrime and Forensics Book Period. Elsevier, Inc., 2007. ISBN 13: 978-1-59749-228-7.**
4. **SPIVEY, Mark. Practical Hacking Techniques and countermeasures. Auerbach Publications., 2007. ISBN 13: 978-0-8493-7057-1.**
5. **FOOT, M., HOOK, C.: Personalistika. Computer Press, Praha 2002. ISBN: 8072265156**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem práce je definovat problematiku vztahující se k tvorbě specializovaného pracoviště – forenzní laboratoře pro odhalování útoků kybernetické trestné činnosti, možnosti využití tohoto pracoviště v privátní sféře, hardwarové a softwarové vybavení, personální obsazení pracoviště, plánování a metodika činnosti, zabezpečení, předpokládané náklady spojené s návrhem a realizací specializovaného forenzního pracoviště.

Klíčová slova: Kybernetická kriminalita, informační kriminalita, kybernetická bezpečnost, informační bezpečnost, specializované vyšetřovací pracoviště.

ABSTRACT

Main goal is to define problems connected with the development of special workplace – forensic laboratory for cyber atacks investigations, methods of using this workplace in private sector, hardware and software equipment, selection of workpace personnel, planning and working metodology, security, cost presumption of development and realization of special forensic workplace.

Keywords: Cyber crime, info crime, cyber security, info security, specialized investigative workplace.

Děkuji své nejbližší rodině za finanční i duševní pomoc, bez které by mé studium nebylo reálně možné. Děkuji tímto také svému vedoucímu diplomové práce PhDr. Mgr. Stanislavu Zelinkovi za odbornou pomoc, které se mi dostávalo v průběhu realizace práce. Děkuji všem dalším lidem, kteří mi s tvorbou diplomové práce pomohli.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Není tomu tak dávno co byly všechny informace psány ručně nebo na stroji. Tyto informace pak byly ukládány do obrovských archivů, ve kterých bylo velmi obtížné informace hledat. Za několik posledních desítek let se ovšem situace rapidně změnila. Ještě naši dědové zažili dobu, ve které bylo za vrchol běžně dostupné technologie považováno rádio. Oproti tomu dnes je naprosto běžné mít na zdi domu satelit, v kapse mobilní telefon a v ruce notebook s rychlým internetovým připojením, které umožní během několika sekund komunikaci s kamarádem žijícím na druhé straně zeměkoule. A to je teprve začátek. Dramatický vývoj technologií změnil způsob přístupu k informacím. Z informace na papíře se stala informace digitální. Bohužel s vývojem technologií přichází na svět nový fenomén, kybernetická kriminalita. A my všichni žijeme v době zrodu této trestné činnosti. V současnosti je kybernetická kriminalita širokou veřejností stále opomíjena či ignorována. Ovšem díky rapidnímu a neustálému rozvoji technologií je možné, že za několik desítek let bude kybernetická hrozba stejně nebezpečná, jako například zbraně hromadného ničení. Termín kybernetický terorismus se v mnoha publikacích již objevuje. Potřeba ochrany proti tomuto druhu trestné činnosti se bude tedy stále více zvyšovat. A ochrana jako taková je i hlavním předmětem zájmu této diplomové práce. Protože s rostoucím vývojem technologií bude růst i potřeba ochrany proti novým druhům kybernetických hrozeb.

Specializované pracoviště pro odhalování kybernetické trestné činnosti je jedním z druhů ochrany proti hrozbám moderního světa. Takovéto pracoviště slouží nejenom jako způsob ochrany, ale také jako prostředek k dopadení a usvědčení samotného pachatele. Tento materiál se zabývá problematikou vývoje tohoto pracoviště. A to od jeho výstavby, až po metodiku jeho činnosti. Konkrétně rozděluje tuto problematiku do čtyř hlavních úseků. Jedná se o výstavbu pracoviště, zajištění jeho funkčnosti, vymezení metodiky činnosti a také konkrétní technické postupy při vyšetřování trestné činnosti v závislosti na druhu útoku. Využití tohoto pracoviště je směrováno k soukromé sféře, a to buď jako jednotka uvnitř organizace, nebo jako samostatná jednotka vybudovaná za účelem zisku. Dříve než se ovšem vrhneme do výstavby specializovaného pracoviště, zaměříme se na vymezení základních pojmů vztahujících se ke kybernetické trestné činnosti.

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Pokud mluvíme o tomto specifickém druhu trestné činnosti, je třeba si uvědomit, že nejde tak ani o to jestli bude subjekt napaden, ale spíše jde o to kdy se tak stane. Vždyť téměř každý se jistě někdy setkal se situací, která by se dala označit jako kybernetický zločin. neustálý boj s nevyžádanou poštou v emailových stránkách nebo s počítačem zahlceným viry a jinými skrytými programy jsou běžnou součástí našeho života. Většina z nás srovnává kybernetický zločin s výše zmíněnými problémy. Viry nebo spam jsou ale pouze špičkou ledovce. Většina kybernetické trestné činnosti je veřejnosti skryta. Ve sdělovacích prostředcích občas uslyšíme tento pojem ve spojení s nelegálními kopiemi, krádežemi hesel či kódů, útokem hackerů, a podobně. Ve skutečnosti se většina druhů kybernetické kriminality vztahuje ke krádeži duševního vlastnictví, útok na servisní sítě, finančním podvodům, softwarové pirátství, porušení autorského práva. Nejdůležitější je si uvědomit, že se kybernetický zločin neustále mění. Chcete-li vyvíjí. V současnosti je převážně tento zločin páchán jednotlivci. Jejich motivace je různá, ale většinou jejich činny nemají zásadní negativní vliv na poškozeného. Dosavadní průběh vývoje kybernetické zločinnosti ovšem jasně poukazuje na budoucí směr, kterým se tato trestná činnost bude ubírat. Dnes realizují tuto činnost především nadšenci do počítačové techniky a jiných technologií. jejich cílem není v prvé řadě finanční zisk nebo poškození subjektu jejich zájmu. Vývoj ale směřuje k situaci, kdy právě zisk nebo poškození objeti budou hlavní motivací pachatele kybernetické trestné činnost.

Hrozbu pro budoucnost neznamenají ani tak jednotlivci, jako spíše organizované skupiny. Již dnes podobné skupiny provádějí svou nelegální činnost bezstarostně. Ať už je jejich motivace jakákoli, způsobují jejich obětem nemalé finanční ztráty. Naprosto běžně se můžeme setkat s podobnými organizovanými skupinami v zábavním průmyslu. Díky rozvoji technologií zaznamenal v posledních letech obrovský rozvoj především video herní průmysl. V současnosti toto odvětví dokonce překonává filmový průmysl. Zisky vývojářských týmů a vydavatelských společností ve video herním průmyslu jsou počítány na stovky milionů dolarů a kybernetická zločinnost těmto společnostem způsobuje obrovské finanční ztráty. Dnes a denně můžeme vidět boj mezi vývojáři počítačových her a organizovanými skupinami hackerů. Cílem těchto skupin je prolomit bezpečnostní ochranu a umožnit tak bezproblémové kopírování a tvorbu nelegálních kopií. Ať už je motivace těchto skupin jakákoli, je jisté že způsobují velké finanční ztráty.

Hlavním problémem kybernetické zločinnosti jsou informace respektive jejich možné zneužití. Dříve byla informace pouze v mysli nebo na papíře. Dnes je trend jasný. Informace se transformují do digitální podoby. Proto se mění i snaha jak tyto informace zneužít. Kybernetická trestná činnost je zaměřena především na informace. Přesněji na elektronická data, která obsahují tyto informace. Informace se dají koupit, prodat. mají tedy určitou hodnotu. Takováto hodnota informace je i hlavním cílem zájmu pro pachatele kybernetického zločinu. S patřičnou znalostí vzniká totiž moc a ta se pak dá nějakým způsobem využít. Například v konkurenčním boji, kdy jedna strana může získat informace o konkurentovi a na základě této znalosti konkurenta zničit.

Specifickým aspektem kybernetické trestné činnosti je vzdělanost. Aby mohl být kybernetický zločinec ve svém snažení úspěšný, musí být velmi kvalitním odborníkem. Často se tedy stává, že osoba pracující v některém odvětví výpočetních technologií zároveň doma ve volném čase páchá trestnou činnost, která je úzce spjatá s jeho profesí. Jedním příkladem budiž člověk, kterému se jako prvnímu podařilo prolomit ochranu mobilního telefonu iPhone. Tento člověk je zaměstnán jako programátor u mezinárodní společnosti vyvíjející jak hardware, tak software. Útok tedy může přijít jak z vnějšku, tak zevnitř. Nedá se stanovit, která z hrozeb je pravděpodobnější. Jisté ale je, že je nutné se proti těmto hrozbám chránit, ať už pocházejí odkudkoli. Základním prvkem úspěšného boje s kybernetickým zločinem je totiž prevence.

Kapitola sama pro sebe je osobnost pachatele kybernetických zločinů. Oblast kybernetické trestné činnosti je velmi obsáhlá. Proto se pachatelé vždy specializují na konkrétní činnost. Pokud se podíváme na pravděpodobný věk pachatele, musíme konstatovat, že se jedná téměř vždy o člověka mladého. Velmi často se jedná o studenty. Důležitý je fakt, že páchání této trestné činnosti vyžaduje určitou vzdělanost, jak bylo řečeno již dříve. Proto je vývoj kybernetického zločince započat již v dospívajícím věku. Čím větší vědomosti postupem času tato osoba získá, tím nebezpečnější může potencionálně být. To znamená, že uskutečnění kybernetického zločinu je podmíněno vědomostmi a tyto získání těchto vědomostí je podmíněno dlouhodobým studiem. Již dnes lze rozlišovat mezi pachatele kybernetického zločinu na amatéry a profesionály. Je jednoznačné, že nastala doba kdy se dají toto trestnou činností získávat peníze. A to buď přímo nebo zprostředkovaně. Některé typy pachatelů svou činnost provádějí příležitostně, jiní takto činí naprosto záměrně a opakovaně. Je jisté že jsou tito pachatelé stále více vytrvalejší, než kdy dříve. je to znovu

dáno vývojem technologií. Neustálý technologický rozvoj dává pachatelům stále nové možnosti a tyto nepřeberné možnosti zase pachatelům poskytují patřičnou dávku sebevědomí. Vždyť možnost páchat kybernetickou zločinnost anonymně je největší výhodou kybernetických zločinců. Tito zločinci jsou naplněni pocitem neodhalitelnosti a tím pádem beztrestnosti. Tato situace je patrná napříč všemi odvětvími kybernetického zločinu. Ze všeho nejvíc je ovšem patrná v oblasti softwarového pirátství. Není tomu tak dávno co bylo nelegální kopírování datových nosičů na běžném pořádku i v České republice. Motiv pachatele může být různý. Od finančního zisku, získání tajných informací, až po pouhé upozornění na sebe sama. Ať už je motivem cokoli, poškozenému subjektu vždy vzniká újma v závislosti na druhu spáchané trestné činnosti.

1.1 Kybernetická trestná činnost

Jedná se o sjednocující pojem, zahrnující veškeré zločinné jednání souvisejícím s informačními a komunikačními technologiemi. Což mohou být počítače a jejich periferie, systémy a aplikace, dále počítačové sítě, databázové systémy, elektronické komunikační systémy, atd. Toto nezákonné jednání je nebezpečné jak pro bezpečnost státu, tak pro jeho společnost. [1]

Kybernetická trestná činnost zahrnuje jevy jako např. počítačová kriminalita, informační kriminalita, softwarové pirátství, kybernetický terorismus, politická a hospodářská špionáž, extrémní politická nebo teroristická propaganda, atd. Někdy se pojem kybernetická trestná činnost zkráceně nazývá kybernalita.

1.2 Počítačová kriminalita

Jde o trestnou činnost, ve které nějakým způsobem figuruje počítač, jako souhrn technického a programového vybavení, nebo některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti nebo jako nástroj trestné činnosti. [1]

Definovat přesně počítačovou kriminalitu je ovšem nemožné. Je to dáno jejím neustálým vývojem. S vývojem technologií se tedy může měnit i pohled na definování této trestné

činnosti. Dnešní počítačová kriminalita je totiž velmi odlišná od dob minulých a bude stejně odlišná v letech budoucích.

1.3 Informační kriminalita

Jedná se o veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat. [1]

Je to trestná činnost vztahující se k informacím v elektronické podobě. Pojmy informační a počítačová kriminalita mají k sobě velmi blízko, respektive definice těchto pojmů se v mnoha ohledech prolínají. Definice informační kriminality vznikla jako taková odnož počítačové kriminality, a to z důvodu potřeby dodání důrazu na činnost vztahující se k informacím. Většina počítačové kriminality má velmi blízko k nelegálnímu nakládání s informacemi, ale ne všechny druhy počítačové kriminality se dají úzce spojit s informacemi. Proto vznikla potřeba definování informační kriminality.

1.4 Informační bezpečnost

Informační bezpečností se rozumí zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěryhodnosti, integrity a dostupnosti těchto hodnot. [2]

Bezpečnost informací je pro tuto práci stěžejním pojmem, a to především ve vztahu ke způsobu nakládání s daty během celého vyšetřovacího procesu. Jednoduše se dá říct, že informační bezpečnost představuje ochranu informací.

1.5 Kybernetická bezpečnost

Bezpečnostní disciplína, vztahující se na jakákoli technická zařízení, pracující s daty. [1]

Kybernetická bezpečnost tedy znamená ochranu všech technických „strojů“, jako např. počítače, mobilní telefony, PDA, servery a jiná síťová zařízení, další druhy hardware, atd.

1.6 Informační a komunikační technologie

Veškerá technika, která se zabývá zpracováním a přenosem informací. [1]

Nejedná se ovšem pouze o výpočetní a komunikační techniku, ale také jejich softwarové vybavení.

1.7 Specializované vyšetřovací pracoviště

Jedná se o specializované centrum pro boj s kybernetickými hrozbami, které sdružuje vyspělé technické kapacity a kvalifikované odborníky z řady oborů, vztahujících se k tématu odhalování kybernetických hrozeb a zajišťování kybernetické bezpečnosti. [3]

Vlastní aktivity tohoto pracoviště nejsou zaměřeny pouze na pasivní ochranu, ale také na aktivní vyhledávání a identifikaci hrozeb či útoků. Takovéto centrum může pracovat v rámci veřejné i soukromé sféry.

Pokud mluvíme o pracovišti jako o celém objektu, můžeme pro jeho označení, kromě označení pracoviště, také využít označení centrum, respektive vyšetřovací centrum. Toto vyšetřovací centrum se pak skládá z jednotlivých pracovišť, kterým dozajista vévodí pracoviště pro odhalování a vyšetřování kybernetických zločinů. Toto vyšetřovací pracoviště je srdcem celého centra a někdy je také nazýváno vyšetřovací, respektive forenzní laboratoří. Personál v takovéto laboratoři je pak složen ze specializovaných vyšetřovatelů , respektive forenzních znalců.

V tomto dokumentu budeme ale pro zjednodušení většinou využívat obecného označení pracoviště, společně s uvedením konkrétního významu tohoto označení v daném kontextu.

2 VÝVOJ SPECIALIZOVANÉHO PRACOVIŠTĚ

Vyšetřovací pracoviště může mít rozdílnou velikost v závislosti na jeho účelu. Vyšetřovací pracoviště může dost dobře reprezentovat jeden jediný zaměstnanec nějaké společnosti, která takovéto pracoviště realizuje v rámci své bezpečnostní politiky. Na druhé straně může být toto pracoviště realizováno jako samostatný objekt určený k tvorbě zisku. Takovýto samostatný objekt bude mít definovánu svou vlastní politiku, procedury, standardy, podnikové vybavení a samozřejmě všechny další prostředky k provádění vyšetřovacích činností velkého rozměru.

2.1 Plánování výstavby

Vývoj vyšetřovacího pracoviště pro odhalování kybernetické trestné činnosti může být velmi náročný. Pokud mluvíme o náročnosti, je tímto myšlena nejenom finanční spotřeba, ale také spotřeba času a zdrojů. Vybudování takového pracoviště tedy bude vyžadovat finanční zajištění celé investice, dále čas potřebný na výstavbu a uvedení v činnost a také nemalou investici do zdrojů respektive vybavení pracoviště.

Organizace zavádějící vyšetřovací pracoviště musí mít před samotnou výstavbou dostatečné znalosti o všech požadavcích nutných pro výstavbu. Je to velmi náročná záležitost vymyslet a implementovat vyšetřovací pracoviště do již fungující organizace. Teprve po dostatečném zvážení všech problémů je možné učinit rozhodnutí. Toto je cesta vedoucí k úspěšnému zvládnutí všech nástrah, které jsou s vývojem vyšetřovacího pracoviště spojena. Pokud je vývoj pracoviště realizován v rámci fungující organizace, firmy atd., je to prakticky vždy z nějakého důvodu hrozby pro organizaci, firmu, atd. Proto ještě před samotným plánováním realizace by si měla organizace či firma odpovědět na několik základních, ale důležitých otázek. Např. na otázku jaký je problém? Nejlépe tuto otázku zodpovědět kvalitní analýzou rizik. Jak tento problém vyřešíme? Respektive má cenu stavět vlastní vyšetřovací kapacitu, nebo bude lepší požádat externí firmu. Kolik to bude stát? Pokud je implementace vlastní vyšetřovací kapacity do organizace nezbytností, je nutné realizovat kvalitní plánovací fázi vývoje pracoviště. Jaké z toho všeho budou výhody? Respektive bude to pro nás vůbec výhodné z hlediska peněz, času, výsledků. Až

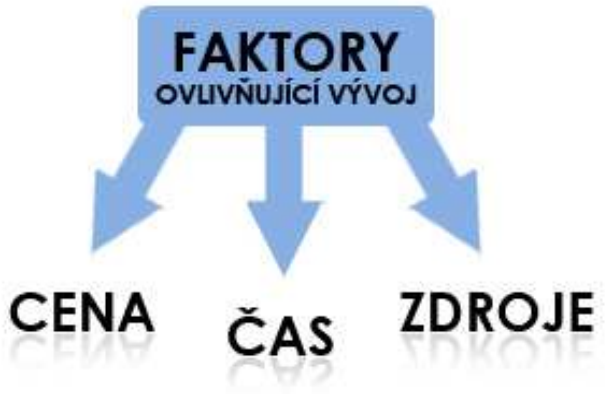
po důkladném uvážení těchto otázek je možné rozhodnout o tom, zda bude pro organizaci, firmu, atd. výhodné vyšetřovací pracoviště implementovat to své infrastruktury.

Při vývoji samostatného vyšetřovacího objektu může plánovací fáze zabrat klidně i celý rok. Je nutné zvážit mnoho okolností, kterým v prvé řadě vévodí definování rozsahu budoucích služeb. Protože těmto službám je podřízeno naprosto vše. Plánování, budování, činnost pracoviště, jeho budoucí rozvoj a mnoho dalšího úzce souvisí se stanoveným druhem služeb a jejich rozsahem. Samostatné soukromé vyšetřovací pracoviště může své digitální vyšetřovací služby poskytovat soukromým organizacím, firmám, státnímu sektoru, nebo i pouhému jednotlivci, tedy fyzické osobě. Je nutné si uvědomit, že přítomnost takovéhoto pracoviště mnohonásobně sníží potřebu výstavby stejného pracoviště jiným subjektem. Tento subjekt si raději za úplatu najme již vybudované vyšetřovací pracoviště, než aby sám nákladně toto pracoviště stavěl. A je téměř jedno, jestli se jedná o potřebu státní nebo soukromou. Všichni raději využijí toto již vybudované pracoviště, aby jim poskytlo své služby.

Pro vývoj vyšetřovacího pracoviště je jednoznačným klíčovým prvkem plánování. Pokud je plánovací část realizována nedostatečně, polovičatě či nedbale, může to mít značné následky na jeho budoucí fungování. Díky špatným postupům, metodám mohou být získané důkazní materiály k ničemu, pokud může být zpochybněna jejich pravdivost, celistvost, atd. Jenomže v takovém případě problém vzniká již v plánovací fázi, ve které nebyly brány v potaz všechny skutečnosti. Tím pádem byly posléze navrhnuty špatné postupy činnosti a z těchto špatných postupů poté vznikají trhliny v důkazních materiálech, díky kterým jsou důkazy během soudního řízení zpochybněny a zamítnuty. Soukromé vyšetřovací pracoviště by pak utržilo rány, ze kterých by se již nemuselo vzpamatovat.

2.2 Hlavní faktory ovlivňující vývoj vyšetřovacího pracoviště

V základu prvky výstavby zahrnují rozpočet pro výstavbu a fungování, výdaje za servis týkající se běžných činností pracoviště, výdaje týkající se nečekaných nepříznivých událostí a obnovení části zařízení po této události. Dále tento rozpočet zahrnuje výdaje týkající se budoucí expanze, růstu a budoucí modernizace. Obecně by se tyto konkrétní prvky výstavby daly shrnout do třech hlavních faktorů ovlivňujících vývoj tohoto pracoviště.



Obrázek 1: Hlavní faktory ovlivňující vývoj vyšetřovacího pracoviště

2.2.1 Cena

Cena je hlavním faktorem ovlivňujícím všechny aspekty výstavby specializovaného vyšetřovacího pracoviště. Plánování, výstavba, tvorba strategie, procedur, vybavení pracoviště, najmutí zaměstnanců, zajištění jejich vzdělávání, certifikace, budoucí rozvoj a mnoho dalšího bude stát peníze. Znovu je nutné zmínit, že to jak cenově náročné pracoviště bude, závisí v prvé řadě na identifikaci budoucích poskytovaných služeb. Mluvíme totiž o pracovišti jako celku. Ve skutečnosti se ale může jednat o malé pracoviště s jedním vyšetřovatelem a minimálním množstvím vybavení. A stejně tak se může jednat o budovu s desítkami vyšetřovacích specialistů, s velkým rozsahem činnosti.

Identifikování činností či služeb je tedy základním počinem v rámci plánovací fáze výstavby pracoviště. Každá takováto činnost či služba má své vlastní požadavky, které je nutné zvážit a správně implementovat. Změny za pochodu, tedy již během výstavby, vedou ke dvěma problémům. Za prvé je mnohem složitější implementovat nové prvky do již budovaného celku. Výsledkem takového snažení mohou být především u složitějších struktur nechtěné kompromisy, které mohou ve výsledku snížit věrohodnost výsledků práce specializovaného pracoviště. Za druhé všechny pozdější změny, úpravy mimo stanovený plán vývoje, znamenají vyšší finanční náklady. Závěrečným prvkem plánovací fáze je totiž stanovení reálného rozpočtu. Čím kvalitněji a podrobněji je výstavba pracoviště naplánována, tím přesnější je pak i rozpočet. Úpravy plánů výstavby během samotné

výstavby vedou pouze k dodatečným nákladům mimo stanovený rozpočet a k dalším zbytečným komplikacím

Cena za výstavbu je ovšem pouze jednou stranou mince. Provoz pracoviště jistě také bude něco stát. Proto by se plánování nemělo omezit pouze na samotnou fyzickou výstavbu, ale i na následné zajištění provozuschopnosti, definování finančních prostředků investovaných do budoucího růstu, rozvoje a také do obnovy zastaralého zařízení. Během plánovací fáze je také zapotřebí ustanovit cenu za poskytované služby. Jednou stránkou je totiž cena za technické vybavení a jeho provoz, ale finanční náklady jsou spojeny i se samotnou prací vyšetřovacího týmu. Finanční náklady za poskytované služby lze zjednodušeně rozdělit na cenu za získání, uchování a analýzu digitálních dat. Zjištění všech těchto budoucích nákladů bude mít klíčový dopad na určení výdajů za každou činnost, kterou specializované vyšetřovací pracoviště realizuje. Pokud jsou jasně vymezeny všechny náklady na činnost pracoviště, je možné definovat návrat investic. Návrat investic zahrnuje příjmy a výdaje, udává tedy zisk pracoviště. Na jedné straně jsou všechny náklady spojené s konkrétní činností, na druhé straně je cena za tuto klientovi poskytovanou službu. Zisk můžeme samozřejmě spojovat pouze se samostatnou vyšetřovací jednotkou, nikoli s pracovištěm realizovaným uvnitř nějaké organizace. Takovéto interní pracoviště je realizováno pouze z důvodů ochrany organizace a náklady na provoz pracoviště jsou hrazeny z jiných sektorů organizace, které jsou určeny k zisku. Interní vyšetřovací pracoviště není primárně určeno k tvorbě zisku.

2.2.2 Čas

Čas je nezbytným faktorem vývoje specializovaného vyšetřovacího pracoviště. Nejenom ovšem vývoje, ale týká se také činnosti pracoviště. Může trvat dlouhou dobu, než bude pracoviště připraveno ke svému poslání. Tvorba plánů, vývoj, implementace fyzických prvků a procedur může trvat roky. Nemluvě o tom, že se během této první fáze můžeme střetnout s nejrůznějšími problémy, které bude nutné řešit za pochodu a tím pádem vznikne časová ztráta se kterou se v plánovací fázi nepočítalo. Jak bylo řečeno, čas hraje klíčovou roli i během samotné činnosti pracoviště. Financování, vzdělávání, omezení zdrojů, termín dodání výsledků práce klientovi, řešení provozních komplikací, obnovení stavu po mimořádné události, krádež, atd. Vše jmenované a ještě mnohé další souvisí s časem. To

hlavní je, že čas znamená peníze. Pokud není možné splnit časový závazek ustanovený během plánovacích fází nebo během vlastního provozu pracoviště, není od věci využít outsourcing, který poskytne externí firma schopná zajistit požadované služby. Někdy může být outsourcing nezbytností. Pokud není z nějakých důvodů možné ve stanoveném čase vytvořit a implementovat určitý prvek, je lepší toto svěřit jiné firmě, než riskovat nezdar vlastní špatnou realizací. Špatně odvedená práce nebo kompromisní řešení z důvodů časové tísně se nemusí vyplatit. Výsledkem by pravděpodobně byly pozdější dodatečné náklady nebo kompletní nezdar projektu. Nezdar může pocházet ze špatně navržených procedur činnosti, špatné obchodní politiky pracoviště, může být způsoben nekompetentním personálem, nebo díky vybavení které nesplňuje běžné standardy kvality, atd. Všechny časové závazky musí učinit pouze zodpovědná osoba, která ví kolik času je za potřebí pro vývoj a realizaci specializovaného vyšetřovacího pracoviště.

2.2.3 Zdroje

Třetím neméně důležitým faktorem ovlivňujícím vývoj a činnost vyšetřovacího pracoviště jsou zdroje potřebné jak pro výstavbu, tak pro zajištění následné funkčnosti a dokonce i zdroje potřebné pro budoucí expanzi a rozvoj pracoviště. Rozhodování o zdrojích musí rovněž učinit zodpovědná osoba, která rozumí tomu, jaké prostředky jsou nutné pro danou konkrétní realizaci. Jinak bude celý projekt neúspěšný. Zdroje jsou vyžadovány pro výstavbu specializovaného pracoviště, pro ustanovení organizace práce, získání vyšetřovacích nástrojů v hardwarové i softwarové podobě, atd. Z toho plyne, že osoby rozhodující o vymezení potřebných zdrojů mají velkou zodpovědnost. Jsou zodpovědné za úspěch celého projektu.

Vzhledem k tomu, že se různé formy zdrojů se vztahují na všechny fáze vývoje pracoviště, je téměř nemožné, aby o všech rozhodovala jedna osoba. Zdroje potřebné na výstavbu nejsou stejné, jako zdroje pro specializovaný vyšetřovací tým, zdroje pro administrativu, sítě, bezpečnost, atd. To je důvod, proč by měla o každém druhu zdrojů rozhodovat jiná osoba. Tedy odborník, který tomuto konkrétnímu odvětví rozumí. Na jejich činnost by měl dohlížet projektový manager. Ten je také za výsledky této skupiny odborníků zodpovědný. Dobrý projektový manager by měl být schopen pomoci při plánování vývoje. Dobrý projektový manažer by měl usnadnit práci na vývoji systematickým plánováním. Měl by

ustanovit časový rámec a finanční požadavky. Měl by zajistit, že se všechna odvětví v stanoveném časovém období střetnou. To znamená, že v rámci stanovené časové lhůty bude např. dokončena práce na síťovém zařízení, společně s pracemi na zdrojích elektrické energie a podobně. Projektový manager by tedy jako hlavní zodpovědná osoba měl zajistit úspěch celého projektu. Je zodpovědný za celé období výstavby.Bez kvalitních znalostí o druhu vyžadovaných zdrojů by bylo velmi obtížné stanovit čas a finanční náklady potřebné pro vývoj a realizaci specializovaného vyšetřovacího zařízení.

2.3 Výběr vybavení

Stanovení potřebného technického vybavení je velmi důležité pro budoucí činnost vyšetřovacího pracoviště. Vyšetřovací specialisté budou využívat softwarové aplikace pro analýzu dat, hardwarové zařízení v čele s počítači. Analyzovaná data musejí být někde uložena. Celý vyšetřovací prostor bude propojen síťovými prvky. A tak dále. Není dobré spoléhat vždy na jeden jediný typ vybavení, především u technického vybavení pro vyšetřovací proces. Ověřování a testování nejrůznějších druhů software/hardware je velmi důležité. Spoléhat se například pouze na jeden typ nástroje pro analýzu dat se nevyplácí. Technologie se neustále vyvíjí. Vyvíjí se díky tomu i kybernetická trestná činnost. Pokud by specializovaný vyšetřovací tým spoléhal neustále jen na ty samé technické pomůcky, stal by se velmi rychle konkurence neschopným. Nebyl by tak schopen držet krok s pachateli kybernetické zločinnosti a dřív nebo později by svůj neefektivní způsob práce musel změnit nebo ukončit.

Technické vybavení nesouvisí pouze se zajištěním činnosti vyšetřovacího týmu. Prakticky celý objekt bude zaplněn technologií nejrůznějšího druhu. Výběr všech těchto technických prvků je důležitý, ale také velmi náročný. Jako příklad se dá uvést bezpečnost. Zabezpečení vyšetřovacího pracoviště hraje důležitou úlohu. Do bezpečnosti objektu ale spadají i další aspekty, jako ochrana proti působení přírodních vlivů, ochrana proti vzniku mimořádné události, ochrana zaměstnanců v objektu, bezpečnost práce a jiné.

Digitální vyšetřovací software je pro práci specialistů hlavním komponentem jejich práce. Díky těmto speciálním softwarům jsou vyšetřovatelé schopni získat potřebná data, analyzovat je a vytvořit zprávu obsahující poznatky o datech, které mají určitou hodnotu.

Vyšetřovací software může být pro pracoviště velmi nákladný. Nemluvě o tom, že většina softwaru je čas os času nahrazována novějšími verzemi, což stojí další úsilí a hlavně další peníze. Takže patřičné promyšlení nákupu softwaru je velmi důležité. Není dobré po koupi softwaru zjistit, že se pro zamýšlenou činnost nehodí. Většina výrobců software poskytuje tzv. shareware verze svých softwarových programů. Tyto shareware verze jsou plnohodnotné, pouze mají omezenou dobu jejich užívání. Většinou na 30 dnů. Není tedy nic jednoduššího, než si tyto shareware verze vyzkoušet a pak rozhodnout o koupi plnohodnotné verze programu. Je možné, že výrobce požadovaného software tyto časově omezené verze neposkytuje. Přeci jenom je odvětví našeho zájmu velmi specifické a software může být také velmi drahý. V tom případě se dá s výrobcem jistě dohodnout na alternativním způsobu řešení. Konkrétně o nákupu software pro vyšetřovací pracoviště by měl především rozhodovat vyšetřovací tým, protože právě on bude s tímto softwarem pracovat. Specializovaný vyšetřovací tým určí požadavky, potřebné pro realizaci konkrétní vyšetřovací činnosti a posléze najde vhodný software, který tyto požadavky splňuje. Takovýto výběr jistě není jednoduchý, protože každá dostupná softwarová aplikace má své výhody i nevýhody. Je především na vyšetřovacím týmu, aby našel vhodného kandidáta. Testování vhodného software by mělo být děláno v testovacím prostoru pracoviště. Nikoliv v prostoru, kde probíhají vlastní vyšetřovací práce. Zajistíme tak optimální produktivitu práce. Kdyby byl software testován přímo ve vyšetřovací laboratoři, ztráceli bychom zbytečně čas na plnění obchodních zakázek. Nemluvě o tom, že v případě testování mohou nastat situace, se kterými se nepočítalo, a bylo by nemilé díky vzniku nějaké nestandardní situace během testu poškodit regulérně využívané vyšetřovací zařízení. Testovat nové druhy metod, softwaru, hardwaru je tedy dobré pouze ve speciální místnosti k tomu určené. Pro testování software je definován určitý scénář, který pravděpodobně může za běžného vyšetřovacího procesu nastat. Tento scénář by měl být navrhnut tak, aby co nejlépe otestoval funkčnost software v situaci, kterou potřebuje vyšetřovací tým vyřešit. Následuje samotná testovací fáze a poté diskuze nad výsledky testu. Výstupem testu by měl být protokol, který uvádí co během testu fungovalo podle požadavků a co naopak požadavky nesplnilo. To poslední co musí tým vyšetřovacích specialistů udělat, je vybrat nejlépe vyhovující software. Tedy ten, který v testu obstál nejlépe.

2.4 Rozvržení prostoru

Při navrhování celkového rozložení prostoru by měl být kladen důraz přinejmenším na čtyři funkční oblasti.

Obrázek 2: Rozvržení prostoru do funkčních oblastí

- **Administrativní oblast:** je složená z „offline“ místa pro personál. Dále je složena z mítinkového prostoru pro vnitřní personál a klienty, dále míst privátního charakteru a místa pro hosty. Takovéto rozložení se postará o adekvátní prostor pro týmové porady, pohodlí a pro zákaznické aktivity.
- **Vyšetřovací oblast:** je oblast určená pro všechno technické vybavení spojené s vyšetřovacím procesem a je tzv. funkční oblastí pracoviště, ve kterém bude specializovaný technický personál trávit největší část svého pracovního času.
- **Oblast síťových zařízení:** toto místo je prostředí, ve kterém sídlí datové sítě, bezpečnostní zařízení a telekomunikační zařízení.
- **Úložiště evidenčních dat:** je potřebné z důvodu umisťování digitální evidence a jiných evidenčních prvků. Úložiště datové evidence by mělo být nejzabezpečenější místo pro přístup, nejvíce kontrolovaná oblast týkající se jakékoliv aktivity, vstupu, odchodu.

2.4.1 Administrativní oblast

V každé hlavní části objektu se nacházejí v malém či větším množství prostory, které nejsou určeny k laboratorním, respektive vyšetřovacím účelům. V rámci celého objektu by ovšem dozajista měla být realizována samostatná oblast, zaměřená přímo na administrativní požadavky. Tato administrativní oblast by měla být zcela oddělena od funkčních částí objektu, ve kterých se provádějí činnosti spojené s vyšetřováním, testováním a se všemi oblastmi budovy, ve kterých jsou umístěny technické prostředky samotné vyšetřovací činnosti a jiné technické prvky.

Administrativní oblast by se tedy dala označit za netechnickou oblast budovy. Tato část budovy zajišťuje správný chod pracoviště. Mimo složky řídící a administrativní se zde nachází mítinkový prostor pro strategické porady personálu, místnost pro klienty, místa privátního charakteru, místo pro hosty. Prostor pro tištěné dokumenty zde také může být umístěn, stejně jako knihovna s odbornou literaturou, jelikož činnost specializovaných vyšetřovatelů vyžaduje časté využívání referenčních materiálů pro konkrétní činnosti, které právě řeší.

Prakticky všechny části administrativní oblasti mohou být navrženy a realizovány jako volně přístupné kanceláře bez větších bezpečnostních restrikcí. Výjimkou jsou pouze případné privátní prostory vrcholného managementu a jiného personálu.

Administrativní část je velmi důležitou oblastí objektu i pro specializovaný vyšetřovací tým. Tito specialisté většinu času stráví na malém osobním pracovišti, proto je dobré pro ně zajistit dostatečně pohodlnou mítinkovou místnost v administrativní části budovy, kde mezi sebou můžou pohodlně řešit problémy spojené s jejich prací, porady s vedením, atd. Specializovaný vyšetřovací tým pak bude raději trávit čas na svém vyšetřovacím pracovišti.

Úvahy by měly respektovat adekvátní personální prostor, kde mohou jednotlivci vést pohodlné konverzace, telefonovat v rámci firemní komunikace a podobně, a nerušit tak probíhající procedury uvnitř vyšetřovací laboratoře. Mítinkový prostor je také velmi důležitý z hlediska budoucích klientů Pohodlný prostor zajistí ideální situaci, pro uzavírání kontraktů a nad jejich konzultacemi s klientem, včetně podání závěrečných zpráv ukončeného vyšetřování.

2.4.2 Vyšetřovací oblast

Tato oblast je srdcem celého objektu. Provádějí se zde všechny technické vyšetřovací procedury. Vyšetřovací oblast se skládá z jednotlivých pracovišť specialistů. Pokud je vyšetřovací oblast rozdělena na více funkčních celků podle konkrétního zaměření, hovoříme pak o těchto celcích jako o jednotlivých laboratořích, a tyto laboratoře pak obsahují pracoviště specialistů. Technický personál zde tedy tráví nejvíce času.

Je nutné, aby samotná vyšetřovací oblast byla dostatečně velká, a to v závislosti na počtu vyšetřovatelů. Pro každou činnost bude totiž nutné využívat nejrůznější technické prostředky, a to jak hardware, tak software. Dobrým krokem je během plánovací fáze vyšetřovacího prostoru stanovit minimální velikost prostoru na jednoho vyšetřovatele. Každé konkrétní osobní pracoviště vyšetřovatele, by mělo mít definováno svůj účel. Podle tohoto účelu by mělo být vyšetřovací pracoviště vybaveno technikou, schopnou splnit všechny, účelem dané, požadavky. Každý vyšetřovací specialista by měl mít dostatek místa i na další potřeby, které nejsou přímo spojené s vyšetřováním. Tím je myšlen například firemní telefon, malá knihovna obsahující referenční materiály, místo na zapisování průběžného postupu a závěrečných zpráv. Stejně tak je ale nutné zajistit v této oblasti dostatečný prostor pro technické vybavení.

Součástí vyšetřovací oblasti může být i technický sklad, kde bude uložena veškerá technika, která v tuto chvíli není přímo potřebná. Tato oblast bude jistě přeplněna nejrůznější technologií a je prakticky nemožné provozovat tuto činnost bez patřičného skladu. Takovýto technický sklad je výhodný z mnoha důvodů. Obsahuje záložní techniku, která je připravena k okamžitému použití v případě selhání právě využívaného technického prostředku na vyšetřovacím pracovišti specialisty. Dále slouží jako dočasný prostor pro odložení této poškozené nebo nefunkční techniky. A v neposlední řadě, pokud je sklad dobře navržen, představuje dostatečný prostor pro využití při možné budoucí technologické expanzi. Jak již bylo dříve zmíněno, vyšetřovací pracoviště je pod neustálým vývojem, proto je nutné navrhnout dostatečné zázemí pro technologickou expanzi v budoucnu. Pokud by se vyšetřovací pracoviště nepřizpůsobilo nikdy nekončícímu vývoji technologií, brzy by začalo ztrácet krok s konkurencí i s pachateli kybernetických zločinů. Technický sklad může být realizován i jako samostatná oblast, nezávislá na vyšetřovacích laboratořích. Ale i tak by měl být datový sklad co nejblíže k vyšetřovací oblasti budovy.

2.4.3 Oblast síťových zařízení

Jedná se o oblast určenou pro fyzické umístění datové sítě, bezpečnostních zařízení a telekomunikační zařízení. Síťová zařízení slouží celému objektu. Ovšem jelikož se jedná o objekt specifického zaměření, jsou v souvislosti se síťovou instalací spojeny jisté konstrukční požadavky. Síťová instalace je realizována v rámci samostatných okruhů. To znamená, že každá hlavní oblast objektu je propojena separátní samostatnou síťovou smyčkou, která je nezávislá na ostatních. Důvodem je zabezpečení datových toků a komunikace, které je podrobněji řešeno v kapitole zaměřené přímo na bezpečnost vyšetřovacího pracoviště. Není dobré spoléhat na virtuální oddělení jednotlivých okruhů. Realizace fyzického oddělení síťové instalace je vždy lepší volbou. Je možné učinit v případě nutnosti určité kompromisy, ovšem vyšetřovací prostor s úložištěm evidenčních dat by měl být vždy síťově oddělen od zbylé síťové instalace. Při nejmenším se tak zajistí, že data spojená s obchodními záležitostmi nebudou procházet stejným síťovým obvodem, jako data evidenční.

Při plánování síťových rozvodů k datovému úložišti evidence je dobré brát do úvahy pravděpodobnost velkých datových objemů procházejících přes síť. Síťová architektura zabere velký prostor v serverové místnosti. Síťové systémy vyžadují umístění v prostoru, který zvládne mimořádné náklady spojené s udržováním a uchováváním enormních datových objemů.

2.4.4 Úložiště evidenčních dat

Úložiště dat slouží k uchování elektronické evidence a jiných prvků důkazního charakteru ve fyzicky oddělené oblasti specializovaného vyšetřovacího centra. Jedná se o jednu z nejdůležitějších částí celého objektu, jelikož jsou zde zadržovány data klienta, která mohou sloužit jako případné důkazní materiály u soudu. Je tedy velmi důležité, aby toto úložiště evidenčních dat splňovalo všechny požadavky technické, bezpečnostní i administrativní povahy. Je nutné zajistit správné nakládání s daty, které úložiště obsahuje. Jakákoliv chyba během opatrovnictví evidence může mít značně negativní dopad. Od situace, kdy klient přijde o část nebo o celý objem dat, až po situaci, kdy díky špatnému nakládání s evidencí nebude tato evidence uznána jako důkaz u soudního líčení.

Je totiž nutné si uvědomit, že úložiště evidenčních dat neobsahuje pouze kopie výchozích dat poškozeného klienta, ale obsahuje i skutečné původní nosiče těchto dat, které byly cílem útoku. Jinak by nemohlo být zajištěno, že s původní evidencí nebude někdo během vyšetřovacího procesu manipulovat. Nemožnost manipulace s původní evidencí musí být podpořena správnými metodickými postupy vyšetřovacího týmu, který je průběžně zaznamenává. Pokud to situace vyžaduje, může být v rámci celého objektu realizováno několik těchto úložišť s pevně stanoveným účelem.

2.4.5 Shrnutí

Tabulka 1: Shrnutí rozvržení prostoru spec. vyšetřovacího centra

Administrativní oblast	
Netechnická oblast	Navržena převážně jako volně přístupná oblast.
Oddělena od funkčních částí objektu.	Obsahuje mítinkový prostor, prostor pro hosty, kanceláře, soukromé prostory, atd.
Vyšetřovací oblast	
Může být složena z funkčních celků – forenzních laboratoří.	Obsahuje osobní pracoviště vyšetřovacích specialistů.
Každé osobní pracoviště má definováno svůj účel.	Osobní pracoviště jsou vybavena technikou podle svého účelu.
Technický sklad je důležitý pro podporu činnosti vyšetřovací oblasti.	Výstavba vyšetřovací oblasti musí být realizována i s ohledem na budoucí možnou expanzi.
Oblast síťových zařízení	
Prostor pro fyzické umístění síťových zařízení.	Vyšetřovací a administrativní data procházejí separátně přes samostatné síťové okruhy.
Samostatné síťové okruhy jsou odděleny fyzicky, nikoli virtuálně.	Předpokládáme velké datové objemy.
Úložiště evidenčních dat	
Pro uchování elektronické evidence a jiných důkazů.	Fyzicky odloučeno od zbylých oblastí v objektu.
Zajištění správného nakládání s daty je nezbytností.	Vyžaduje ustanovení předpisů, pro nakládání s evidenčními daty.

2.5 Bezpečnost

Bezpečnost všech prostorů v objektu hraje hlavní roli v ochraně dat, se kterými se v jednotlivých oblastech vyšetřovacího centra pracuje. Hlavními oblastmi zájmu z hlediska zabezpečení jsou vyšetřovací oblast, oblast síťových zařízení a úložiště evidenčních dat. tyto tři oblasti v objektu by měly mít totožnou, vysokou míru zabezpečení. Určité kompromisy je možné učinit v oblasti síťových zařízení, a to z hlediska přísnosti kontroly přístupu do těchto prostor. Oblastí, které jednoznačně vyžaduje nejnižší míru zabezpečení je administrativní oblast.

2.5.1 Administrativní oblast

Administrativní oblast nepodléhá vyššímu stupni zabezpečení, jako je tomu u zbylých třech oblastí. Zabezpečení administrativní budovy je podmíněno zabezpečením pláště celého objektu. Jelikož je vstupní část do objektu součástí administrativní části, její zabezpečení je tedy podmíněno především kontrolou vstupu. U vstupních dveří do budovy by tedy měl být realizován přístupový systém, který bude kontrolovat a zaznamenávat příchozí a odcházející osoby. Všichni zaměstnanci by měli být při vstupu do budovy zaznamenáni do databáze pomocí identifikačního prvku, stejně tak při jejich odchodu. Provoz v celém objektu by měl být přísně monitorován. Přístupový systém by měl být navržen s ohledem na jednotlivé funkční oblasti objektu. V reálné situaci to znamená, že bude celý objekt rozdělen na jednotlivé zóny a v rámci těchto zón budou nastaveny přístupová omezení. Zóna týkající se administrativní oblasti by byla realizována pouze jako kontrola vstupu zaměstnanců a jiných osob. Jelikož budou mít s největší pravděpodobností do této části objektu přístup i klienti, hosté, externí služby a servisy a jiné subjekty, není nutné realizovat v rámci administrativní oblasti striktní bezpečnostní omezení pohybu. Výjimkou jsou MZS a EZS, které slouží jako ochrana před neoprávněným násilným vniknutím do objektu z vnějšího prostředí.

2.5.2 Vyšetřovací oblast

Pro vyšetřovací prostor by měly být učiněny striktní a velmi přísné bezpečnostní podmínky, upravující vstup do této oblasti. Do vyšetřovacího prostoru by měli mít přístup pouze členové specializovaného vyšetřovacího týmu. Vstup do tohoto prostoru by měl být upraven bezpečnostním přístupovým systémem s duální přístupovou kontrolou.

Přístup samotný můžeme definovat třídami identifikace a přístupu. Pokud mluvíme o duální, respektive kombinované metodě přístupu, uvažujeme tedy o metodě, která spadá pod 3. třídu identifikace. Identifikační třída číslo 3 využívá kombinace prvků třídy 1 a 2. Jedná se tedy vždy o kombinaci dvou odlišných identifikačních prvků, bez kterých není možný přístup do budovy.

Třída identifikace 1 vyžaduje znalost informace pro vstup jako např. heslo, PIN kód apod. Instalované zařízení porovnává tuto informaci s údajem v paměťové jednotce a při shodě umožní vstup. Třída identifikace 2 vyžaduje použití pevného identifikačního prvku, jako jsou přístupové karty, čipové klíče a nebo biometrické prvky vstupující osoby. Kombinací těchto dvou tříd vzniká třída identifikace 3, která by měla být v tomto prostoru využita. Každému zaměstnanci vyšetřovací oblasti je tak přiřazena jednoznačná elektronická identita, která je uložena do databáze přístupového systému.

Společně s třídou identifikace můžeme stanovit správnou třídu přístupu. Jelikož je provoz do tohoto prostoru nutné monitorovat, připadá do úvahy pouze třída přístupu B. Přístupové systémy v této třídě přístupu musejí používat časové filtry a musejí ukládat přístupové transakce. Vyspělé systémy ukládají do paměti informace o napadení systému, o přístupu bez oprávnění včetně lokalizace konkrétního místa, o zamítnutí přístupu apod. Aplikace přístupového systému s těmito a dalšími funkcemi je pro vyšetřovací prostor nezbytností.

Celé řešení přístupového systému je možné realizovat jako jednu ze součástí integrovaného systému budovy.

2.5.3 Oblast síťových zařízení

Již byla uvedena zmínka o potřebě oddělení síťových komponentů vyšetřovacího prostoru od hlavní sítě. Je to lepší z důvodu většího zabezpečení toku dat po síťovém vedení. Data týkající se vyšetřovacího procesu a evidenční data z datových úložišť jsou tak oddělena od jiných síťových provozů v rámci celého objektu. Nestane se tedy, že by například administrativní komunikace, obchodní komunikace a datový provoz z vyšetřovacího pracoviště či úložišť dat procházel po stejném síťovém vedení.

Jako přídavek k tomuto řešení může být realizováno oddělení síťových služeb pomocí fyzických hranic. Pokud sídlí globální a vyšetřovací síťový hardware ve stejné serverové místnosti je nutné zvážit využití zamykací skříně kolem vyšetřovací architektury. Tato zamykací skříň by měla být osazena bezpečnostními dveřmi, které sníží riziko násilného vniknutí. Pokud je tento způsob kombinované ochrany realizován, sníží se mnohonásobně pravděpodobnost případného napadení nebo jiného zneužití interní sítě, sloužící k vyšetřovacímu procesu. Zamykací skříň kolem síťové architektury určené pro vyšetřovací pracoviště a úložiště dat zamezí fyzické sabotáži a obecně zabrání jakémukoli neoprávněnému přístupu k tomuto síťovému zařízení. Zamykací skříň by měla být s časově omezeným zámkem, který se v případě zapomenutí sám po stanovené časové lhůtě zamkne.

S tímto je spojeno stanovení několika přístupových úrovní pro člověka vstupujícího do prostoru, v rámci řešení přístupového systému v objektu. Na síťovou architekturu určenou pro vyšetřovací prostor a úložiště dat musejí být aplikovány stejná bezpečnostní opatření, která jsou realizována právě pro samotné vyšetřovací prostory a pro úložiště dat.

Síťové prvky se ale jistě nebudou nacházet pouze v prostorách určených pro síťová zařízení. Všechny technické síťové prvky (servery, kabely, switche, routery, atd.) v jiných prostorách budovy (vyšetřovací oblast, oblast úložiště evidence a administrativní oblast) musejí být chráněny stejnými bezpečnostními kritériemi, které definují přístup do těchto prostor. To znamená, že pokud se např. ve vyšetřovacím prostoru nacházejí síťové prvky, musejí být zabezpečeny proti neoprávněnému přístupu k nim, a to se stejnou úrovní zabezpečení, jaká je realizována pro přístup do samotného vyšetřovacího prostoru. Všechen vyšetřovací provoz je nutný vést přes prvky k tomu určené. Tedy pouze přes switche, servery atd. určené konkrétní oblasti objektu (vyšetřovacímu prostoru, úložišti

evidenčních dat, nebo administrativní oblasti). Není dobré spoléhat na virtuální oddělení, zavedení fyzické separace síťových prvků je lepší volbou.

2.5.4 Úložiště evidenčních dat

Úložiště datové evidence by mělo být nejzabezpečenější místo pro přístup společně s vyšetřovací oblastí, nejvíce kontrolovaná oblast týkající se jakékoliv aktivity, vstupu, odchodu. Měl by to také být nejvíce fyzicky oddělený (odloučený) prostor specializovaného vyšetřovacího centra.

Systém kontroly vstupu by měl být realizován totožně se systémem přístupu k vyšetřovacímu prostoru. To znamená, že stejně jako u vyšetřovacího prostoru je implementována duální kombinovaná kontrola vstupu s třídou identifikace 3 a třídou přístupu B. Vzhledem k velkému počtu bezpečnostních a jiných systému v objektu, je výhodné tyto systémy realizovat v rámci jednoho integrovaného systému. Tímto bude zajištěna jednodušší správa jednotlivých systémů. CCTV systém by měl být u vstupních dveří do prostoru instalován. A to z obou stran, jak ze vnější vchodové strany, tak uvnitř evidenčního úložného prostoru.

Vstupní dveře do úložiště evidenčních dat by měly být konstruovány tak, aby dokázaly prodloužit dobu potřebnou pro neoprávněné vniknutí na co nejdelší dobu. Stěny v prostor, ve kterém se úložiště evidenčních dat nachází by neměly obsahovat žádná okna či jiné otvory, kterými by se dalo dostat do samotného prostoru. V ideálním případě je úložiště evidenčních dat situováno ve vnitřní části objektu tak, aby žádná ze stěn úložiště datové evidence nebyla zároveň stěnou pláště objektu.

Evidenční zabezpečení musí být realizováno a konstruováno tak, aby odolalo násilnému vniknutí nebo neoprávněnému vstupu. Musí být navrženo tak, aby jeho obsah přežil nečekané události které mohou v objektu nastat. Ideálním řešením tohoto problému je umístění evidenčního úložiště do trezoru, který odolá jak násilnému pokusu o vniknutí, tak i případnému požáru či vodě použité při hašení. Veškerý přístup do této oblasti by měl být kontrolován s největším úsilím a zpřístupněn pouze klíčovým zaměstnancům. Často pouze jednomu tzv. správci evidence. Tento správce evidence pak nese jako jediný odpovědnost

za informace v úložišti umístěné. Osoba vykonávající správce evidence by měla být důvěryhodná a dostatečně prověřená.

Silný informační systém v rámci systému přístupového by měl doprovázet úložiště datové evidence. Kontrolujíce a zaznamenávajíce všechny příchozí a odcházející osoby. Seznam pohybujících se osob by měl být podložen psaným podpisem. Informační systém týkající se provozu v úložišti evidence by měl mít robustní auditní metodologii, která garantuje kompletnost a přesnost správy informací. Pět otázek (kdo, co, kdy, kde a proč), by mělo být vždy známo a zdokumentováno u každé obecně uznávané evidence.

2.5.5 Shrnutí

Tabulka 2: Shrnutí bezpečnosti spec. vyšetřovacího centra

Administrativní oblast	
Nejnižší úroveň bezpečnosti z celého objektu.	Bezpečnost této oblasti souvisí se zabezpečením pláště objektu.
Nejrizikovější jsou vstupní dveře do objektu.	Realizace přístupového systému pro zaměstnance a vrátní služby pro hosty + CCTV na vstupu/výstupu z objektu.
Vyšetřovací oblast	
Velmi přísné bezpečnostní podmínky.	Vstup povolen pouze členům spec. vyšetřovacího týmu a vedení.
Bezpečnostní přístupový systém s duální přístupovou kontrolou.	Třída identifikace 3, třída přístupu B.
Oblast síťových zařízení	
Oddělení síťových zařízení fyzickou hranicí (pro vyšetřovací oblast a úložiště datové evidence).	Využití zamykací skříně pro síťovou architekturu (pro vyšetřovací oblast a úložiště datové evidence).
Bezpečnostní přístupový systém s duální přístupovou kontrolou.	Třída identifikace 3, třída přístupu B.
Úložiště evidenčních dat	
Přístup má pouze správce evidence. Bezpečnostní přístupový systém s duální přístupovou kontrolou + ručně psaný podpis vcházejících osob.	CCTV na vstupu/výstupu z prostoru. Třída identifikace 3, třída přístupu B.

2.6 Požární ochrana

Vyšetřovací pracoviště, speciálně velký objekt, vyžaduje promyšlený požární plán. Pokud je specializované vyšetřovací centrum vybudováno v již existujícím prostoru, vlastník už bude možná mít vlastní implementaci požární ochrany, nebo požadavky na ni. Ochrana často musí pasovat již na stávající infrastrukturu. Vzniká tak potřeba kompromisního řešení, což nemusí být u požární ochrany ideální řešení. V mnoha případech bohužel ideální požární ochranný systém vymodelujeme až po nějaké obnově mimořádné události.

V objektu se nachází technologické systémy, prostředky a jiné vybavení technického rázu. To znamená, že prioritou by u požární ochrany neměla být pouze ochrana před požárem, ale musíme vzít do úvahy i technický materiál, který by neměl být poničen. Samostatnou kategorií jsou evidenční data v datových úložištích. Tyto data nesmějí být za žádnou cenu poškozena nebo zničena vzniklým požárem, ani hasícím systémem. Nově budované zařízení má několik možností požární ochrany a konkrétní implementace bude něco stát. Při nejmenším peníze, čas, designový dopad na každý další aspekt výstavby.

Z hlediska ochrany materiálu infrastruktury a elektrických zařízení proti ohni existuje několik voleb:

- Vodní hasící systémy
- Plynové hasící systémy
- Chemické hasící systémy

2.6.1 Vodní hasící systémy

Tyto systémy využívají vodu jako tekutinu pro hašení. Ve specializovaném vyšetřovacím objektu by jsme měli brát ohled na možnost poškození technologie (počítače, evidenční elektronická úložiště, atd.) vodou během nečekané události. V každém prostředí, kde je využíváno vodních systémů pro potlačení ohně, by měly být realizovány anti-vodní návrhy. Máme na mysli např. hlavní úložiště evidence. Pořízení vodě odolného a ohni vzdorného sejfu (nebo jiného zamykacího systému) uvnitř evidenční místnosti je dobré protiopatření při použití vodních hasících systémů. Takovýto sejf může fungovat jako primární

evidenční kontejner. Tyto systémy se tedy prakticky mohou uplatnit spíše v prostorech, kde se nenachází žádné technické vybavení.

2.6.2 Plynové hasící systémy

Tyto systémy jsou známy jako tzv. čistící agenti. Poskytují high end způsob kontroly požáru v laboratorních podmínkách. Tato třída potlačení ohně pracuje jedním ze dvou způsobů. Jedna skupina je schopna odstranit teplo při vznícení rychleji, než jaké je vůbec schopné toto vznícení generovat. Druhá skupina spotřebuje kyslík, aby zabránila vzniku požáru. Tyto systémy nezanechávají žádné vlastní následky po použití. Proto je čas zotavení mnohem kratší, než u jiných systémů. Navíc jsou tyto materiály nevodivé a nenechávají za sebou žádný vodivý materiál. Jsou tedy ideální volbou pro prostory s elektronickým zařízením. Pokud je tento systém použit, je nutné navrhnout kapacitně dostatečně velké evakuační trasy. A to i přes to, že samotný plyn nemusí být pro organizmus škodlivý.

Plynové hasící systémy jsou systémy využívající CO_2, inertní plyny, nebo halon. Jejich princip činnosti je v podstatě na stejné bázi jako vodní hasící systém, pouze hasící náplň je plynová. Takže při zjištění požáru automatickým hlásičem, respektive při spuštění ručního hlásiče se přes požární ústřednu spustí poplašná zařízení. Po uplynutí doby, která je stanovena pro objekt nebo jeho část, se elektricky otevře láhev s plynovým hasicím prostředkem a plyn začne proudit tryskami do místnosti.

Hasicí účinek plynové náplně spočívá v absorpci tepla z plamenů. Plyn je navíc šetrný k technickému vybavení, a proto je ideální volbou pro specializované vyšetřovací centrum. Plyny používané jako hasební látka mají navíc velmi krátkou dobu rozpadu, takže nezanechávají žádné následky po hašení. Jediným nedostatkem je poměrně vysoká cena za realizaci a následnou údržbu.

2.6.3 Chemické hasící systémy

Většina chemických hasících metod vyžaduje specifické investice týkající se realizace a zvyšuje tak cenu v mnoha jiných oblastech výstavby. Pro příklad neprodyšně uzavřené prostředí může být nutnou podmínkou pro správnou funkčnost chemických požárních systémů. Tyto systémy také dělají velký nepořádek, jelikož se objevují v práškové či kapalné formě. Tato hasící chemická látka zůstane na místě požáru i po jeho eliminování. Musí se po požáru dodatečně odstranit. Nemohou se využívat tam, kde jsou zaměstnanci. Jejich využití ve specializovaném vyšetřovacím centru je tedy značně limitováno.

2.7 Elektrická instalace a zdroje energie

Jakékoliv specializované vyšetřovací centrum bude mít nadprůměrné množství poptávky po energii k tomu, aby mohlo fungovat. Je důležité udržet všechny rozličné technologie stabilní, a to bude zajištěno pouze dostatečnou zásobou primární a záložní energie. Jednoduše řečeno, cena energie vyšetřovacího centra bude narůstat s vyšším počtem čtverečních metrů. A to ve větší míře, než u běžného firemního prostředí. V podmínkách největších realizací mohou být využita samostatná zařízení určená k výrobě energie. V takové situaci je nutné zvážit místo pro nádrže paliva. Tyto úvahy by měly být zahrnuty do plánu energetické spotřeby.

V rámci plánu energetické spotřeby by měly být před výstavbou stanoveny kategorie elektrické energie. Při nejmenším by měly být zahrnuty tyto 3 oblasti:

- Běžná spotřeba zařízení
- Spotřeba síťových zařízení
- Lokální spotřeba vyšetřovacích pracovišť

2.7.1 Běžná spotřeba zařízení

První kategorie je tedy globální spotřeba běžných zařízení. Tento typ spotřeby se řeší u každé výstavby jakéhokoli zařízení. Jedná se o požadavek celé hlavní infrastruktury na elektrickou energii. Zahrnuje např. osvětlení, nouzové osvětlení, klimatizační systémy, bezpečnostní systémy, automatizované dveře a okna, telefonní a komunikační systémy, firemní vybavení, hlavní elektrické náklady na zaměstnance, atd.

Elektrické zásoby by měly být navrhnuty dostatečně a při jejich návrhu je nutné zvážit budoucí růst, až některé ze zařízeních dosáhne 100% využití a eventuelně bude fyzicky expandovat. Realizace rozvodů elektrické energie a připojování konkrétních spotřebičů musí být učiněno tak, aby byla celá elektrická síť stabilní, a to za všech možných podmínek.

2.7.2 Spotřeba síťových zařízení

Druhou kategorií je lokální síťová specifická spotřeba. Tato spotřeba se týká každého vyšetřovacího centra, protože síťová zařízení jsou v tomto objektu využívány denně. Realizace síťového plánu, s ohledem na úroveň nákladů a na technologický standard, je dobrý základ pro proces výstavby. Serverové místnosti mají všeobecně speciální řešení, ale elektrické zdroje pro síťovou technologii ve vyšetřovacím centru jsou řešeny jinak, než je běžné. Filozofie přístupu k řešení elektrické instalace pro síťová zařízení je obdobná, jako řešení samotné instalace síťových rozvodů. Jak už bylo řečeno dříve, síťové rozvody jsou z důvodu bezpečnosti v objektu řešeny pomocí samostatných, na sobě nezávislých, okruhů. Je tak zajištěno, že datové toky obchodního nebo vyšetřovacího nebo evidenčního charakteru nikdy nebudou posílány přes totožné síťové vedení. V případě elektrického napájení síťových zařízení je situace obdobná, pokud má vyšetřovací objekt vlastní zdroj napájení. Dodávka elektrické energie pro síťová zařízení, určená pro vyšetřovací oblast a úložiště datové evidence, by měla být realizována samostatným zdrojem energie, který je oddělen od primárního zdroje elektrické energie. Tento Primární zdroj energie slouží pro síťová zařízení administrativní oblasti a pro zařízení jiného typu ve zbylých částech budovy. Znovu je nutné podotknout, že samostatný zdroj elektrické energie může být realizován pouze u specializovaného vyšetřovacího centra velkého rozměru. Pokud by jsme mluvili o malém samostatném objektu, nebo o pracovišti v rámci organizace, instalování

samostatných zdrojů energie by bylo neefektivní, finančně náročné. V rámci plánovací části vývoje je také dobré stanovit plán selhání a plán nadbytnosti, s ohledem na zásobu a spotřebu elektrické energie. Plán selhání stanoví postup, který se bude aplikovat v případě dočasné nebo dlouhodobé ztráty dodávky elektrické energie. Plán nadbytnosti stanový možné scénáře využití přebytečného množství elektrické energie

Správné řešení separace zdroje energie pro síťová zařízení vyšetřovací oblasti a oblasti úložišť dat je velmi důležitá. Chceme tímto zajistit, aby síť pro tyto dvě oblasti byla první, která se obnoví po výpadku a poslední část síťových zařízení, které přestane fungovat při nestandardní či dokonce mimořádné události.

Pro všechny hlavní oblasti specializovaného vyšetřovacího centra, by měly být realizovány sekundární, respektive záložní zdroje energie. Nejinak je tomu i u síťových zařízení. Specielně u síťových zařízení, určených pro vyšetřovací oblast a oblast úložišť dat, je nutné realizovat jak primární, tak sekundární samostatný zdroj elektrické energie. Při výpadku energie tak zajistíme, že bude síť odpojena postupně a bezpečně díky sekundárnímu záložnímu zdroji a to i během nejtěžších podmínek. Pokud by byla síť napájena pouze z primárního zdroje, výpadek proudu by znamenal okamžité vypnutí této sítě, což by mohlo způsobit nemalé škody.

Prvky energetických zásob síťových zařízení pro vyšetřovací prostor a pravděpodobně i všech dalších energetických zásob můžou vyžadovat speciální zabezpečení a bez kompromisní řešení, závisející na stupni zabezpečení, ve kterém speciální vyšetřovací objekt pracuje.

2.7.3 Lokální spotřeba vyšetřovacích pracovišť

Třetí kategorie je lokální spotřeba vyšetřovacích pracovišť. Je tím myšlen jak celkový vyšetřovací prostor, tak specifické osobní vyšetřovací prostory zaměstnanců. Vyžaduje speciální řešení pro neobvyklou spotřebu energie, která je vyžadována vyšetřovacím technickým týmem. Průměrná vyšetřovací skupina může fungovat na 20 ampérových okruzích, napájejících vždy jednu pracovní stanici, monitor nebo laptop a další napájení pro několik dalších zařízení na osobu. Specializovaný vyšetřovatel je schopen zaplnit 30

ampérový obvod napájení jedním vyšetřovacím vybavením. Takže je možné, že bude vyšetřovatel spouštět několik technologických procesů zároveň na různých pracovištích.

Jednotlivé oblasti speciálního vyšetřovacího objektu mají různou míru energetické spotřeby. To znamená, že např. energetická spotřeba vyšetřovacího prostoru a spotřeba jeho vybavení je mnohem vyšší, než spotřeba v administrativní části objektu.

Množství elektrických zásuvek by mělo být zdaleka největší ve vyšetřovacím prostoru. Zásuvky jsou přeci zdrojem energie pro zařízení, které jsou aktivovány na pracovišti. Pro příklad klonování jednoho jediného harddisku může vyžadovat následující: vyšetřovací pracovní stanici, monitor k pracovní stanici, write blocker, externí USB harddisk a originální externí evidenční harddisk. Což je dohromady 5 elektrických zásuvek. Vyšetřovatel může mít aktivovaných několik klonovacích procesů paralelně. Ergonomie přístupu k těmto zásuvkám také potřebuje dobré zvážení s tím, že nejpodstatnější je samozřejmě kvalita přístupu k zásuvkám. Pokud je zapojeno velké množství zařízení, je potřeba zvážit nejenom četnost elektrických zásuvek, ale také objem spotřeby elektrických obvodů.

2.7.4 Další možné problémy

Je důležité chránit evidenci před nadpěťovými a podpěťovými stavy. Významná pracovní nebo strojní časová investice může být ztracena díky náhlému výpadku elektrické energie. Technologie, využité při výstavbě elektrických obvodů, by měly být mnohem kvalitnější v prostoru vyšetřování, něž jaký by měl být implementován ve standardním prostředí. Využití samostatného elektrického obvodu na každé pracoviště jistě také připadá do úvahy.

Elektrická vedení ve zdech by měla být chráněna z důvodu prevence před elektromagnetickými poli. Nechtěné elektromagnetické pole by mohlo porušit magneticky uložená data v evidenční místnosti.

Plán umístění zařízení by měl obsahovat pečlivé rozložení transformátorů a jiných elektrických jednotek z důvodu snížení nepříznivých elektrických polí.

2.8 Úprava parametrů prostředí

V každém prostředí, kde sídlí kritické výpočetní systémy a magnetická nebo optická datová úložiště je nutné vzít do úvahy parametry prostředí, které tyto zařízení mohou negativně ovlivnit. Stejně tak mohou tyto parametry negativně ovlivnit zaměstnance na jednotlivých pracovištích.

Velký počet přístrojů vyústí v enormní generování tepla. Je nezbytné učinit velmi konzervativní kalkulace týkající se druhu a objemu chlazení vyžadovaného pro technický prostor, ve kterém sídlí velké množství přístrojů generujících teplo. Kalkulace úpravy parametrů v prostředí musejí být učiněny podle aktuálního vybavení a podle individuálních specifikací každé oblasti, nikoliv podle hypotetických odhadů. Mějme na paměti také to, že lidská těla také generují teplo v závislosti na druhu činnosti. Jednoduše by se dalo říci, že čím namáhavější práce, tím větší energetický výdej člověka. Do plánů je nutné zahrnout budoucí růst technického vybavení. Ventilační požadavky pro chlazený prostor musejí být splněny. Pasivní a aktivní návraty čerstvého vzduchu musejí být směrovány na správná místa. To znamená převážně na jednotlivá osobní pracoviště zaměstnanců. Pokud je na místě požární ochranný systém využívající plynové směsi, je nutné opatřit aktivní větrací systém k obnovení stavu prostředí po tom, co byl oheň potlačen. Do úvah také spadají dostatečné chladící zásoby pro každou chladící jednotku sloužící více oblastem najednou. Klimatizační jednotky vytvářejí hluk. Je tedy dobré vzít do úvahy snížení těchto šumových hodnot. Klimatizační jednotka umístěná nad vyšetřovacím prostorem může vytvářet akustický šum v závislosti na laboratorním řešení jednotlivých komponentů. Takovéto akustické znečištění je nutné odstranit.

Během plánovací fáze výstavby pracoviště by jsme měli zvážit následující parametry prostředí a tyto parametry neustále sledovat i během provozu.

2.8.1 Základní sledované parametry

Jedná se o základní sledované parametry vnitřního prostředí, které mohou ovlivnit činnost technických zařízení a také kvalitu práce, především zaměstnanců vyšetřovacího prostoru, ale i všech dalších zaměstnanců v objektu.

2.8.1.1 Teplota

Teplo vzniká v prostředí mnoha způsoby. Proudění, vedení, sálání, odpařování, dýchání a mnohé další generuje teplo. Teplo tedy generuje i člověk, nikoli pouze technická zařízení. Z našeho pohledu je potřeba zajistit správnou teplotu v místnostech. Prostory v nichž je tepelná pohoda, zpravidla poskytují přítomným osobám dobré podmínky pro optimální pracovní výkon.

Je známo, že tepelná pohoda člověka má daleko větší vliv na jeho subjektivní pocit celkové pohody, míru odpočinku i skutečnou produktivitu práce, než nežádoucí emise či obtěžující hluk. Provedené studie dokazují, že při fyzicky lehčí práci (což je případ specializovaného vyšetřovatele) dochází ke stoprocentnímu výkonu člověka při teplotě vzduchu 22 °C, při teplotě 27 °C klesá schopnost podávat plný výkon o 25 %, při 30 °C se dosahuje pouze 50% z optima.

Ideální teplotní rozsah se ovšem netýká pouze pracovníků, ale i všechno zařízení má stanoven teplotní operační rozsah, který je žádoucí dodržet.

Celková vzduchotechnika musí být schopná poskytnout stabilitu teploty ve stanovených rozsazích, a to i během možných poruch vzduchotechnických zařízení. Přenosné chladící zařízení jako součást rezervního plánu je dobrou volbou.

2.8.1.2 Vlhkost

Při relativní vlhkosti vzduchu pod 35 % se projevuje zvýšená prašnost a pod hodnotou 45% se může vytvářet elektrostatický náboj, především na površích plastových materiálů, vysoká relativní vlhkost však může vést k šíření plísní. Tolerance člověka k relativní vlhkosti je poměrně vysoká. Relativní vlhkost vnitřního vzduchu je doporučuje udržovat v rozmezí 30% až 70% s tím, že optimum pro datové prostory i pro osoby je 50% relativní vlhkosti vzduchu. Instalovaný systém by měl být schopen velmi přesně regulovat úroveň vlhkosti ve vnitřním prostředí. Tolerance by neměla být vyšší než 5%.

2.8.1.3 Proudění vzduchu

Rychlost proudění vzduchu může být způsobena jak vnějšími vlivy, tak např. větracím systémem v objektu. Míra rychlosti proudění vzduchu má vliv na pocit tepelné pohody zaměstnanců. Proudění vzduchu ve vnitřním prostředí objektu o rychlosti vyšší než 0,2 m/s je často negativně pociťováno jako průvan.

2.8.1.4 Statická elektřina

jak bylo již zmíněno dříve, teplota a vlhkost jsou dva hlavní faktory prostředí, které upravujeme z důvodu předcházení statické elektřiny. K zamezení negativních projevů statické elektřiny je potřeba zamezit vzniku nábojů. Např. antistatické nástřiky povrchů nebo zajistit stálý odvod náboje vodivým spojením, např. uzemněním.

2.8.1.5 Elektromagnetická kompatibilita

Elektromagnetická kompatibilita určuje, jaké rušení generované technickým zařízením nebo rušení ze strany jiných technických zařízení či vlivem prostředí je příslušné technické zařízení schopno zvládnout bez omezení jeho funkčnosti. Tato podmínka kompatibility zabezpečí, aby se více technických zařízení navzájem nerušilo nebo aby neovlivňovaly své funkce. V podmínkách specializovaného vyšetřovacího zařízení je tato podmínka velmi důležitá, z důvodu používání velkého počtu elektronických systémů na zpracování údajů. Plánování elektrických instalací tedy musí být opatrné, aby se minimalizovalo generování elektromagnetických polí v datových úložištích a archivech. Vyžadována je izolace hlavní elektrické instalace jako transformátorů atd. Není od věci realizovat globální izolaci kolem celé vyšetřovací laboratoře. Stejně tak izolování prostoru evidenčních úložišť k snížení elektromagnetických polí na minimum. Lze umístit gauss metry v laboratorním prostoru. Lze tak pravidelně kontrolovat stav elektromagnetických polí a zjišťovat anomálie. Regulace elektromagnetické interference přímo souvisí s ISO plánováním. Souvisí s každou činností specifickou držením elektronických dat.

2.8.1.6 Akustická rovnováha

Během plánování je velmi důležité definovat způsoby snížení hluku v laboratorních prostorách. Hladina akustického tlaku je základní veličinou charakterizující zvuk v místě jeho příjmu. Pracovat celé dny v hlučném prostředí může způsobit nepozornost, může snížit produktivitu práce. Nemluvě o tom, že vysoká úroveň akustického tlaku může způsobit i zdravotní chronické problémy. Ovšem i příliš tiché prostředí není ideální. Mnoho pracovišť intenzivně vydává akustický tlak do okolního prostředí. Dělá to záměrně. Je to z důvodu vytvoření akustického maskování, z důvodu soukromí, a z důvodu toho, aby nebyl prostor až příliš tichý. Vyšetřovací laboratoř bude mít pravděpodobně mnoho ploch odrážejících akustické vlny. Je tedy dobré zároveň instalovat plochy, které tyto vlny pohlcují.

2.8.1.7 Osvětlení

Míra osvětlení představuje další parametr, který může ovlivnit produktivitu práce osob na pracovišti. Vizuální pohoda udává, zda je v oblasti zrakového úkolu dostatečná intenzita osvětlení a zda je bráněno vzniku oslnění. Nedostatek nebo přemíra světla působí negativně. Při realizaci je pak v úvahu potřeba brát jak umělé tak denní světlo.

2.8.2 Vzduchotechnika

V případě specializovaného vyšetřovacího pracoviště jsou úspěšná řešení ve větrání a klimatizaci založena vždy na dobré znalosti konstrukčních a tepelně-technických vlastností objektu pro které jsou vzduchotechnické systém určeny a na dobré znalosti údajů o vnitřních i venkovních tepelných a vlhkostních zátěžích. Větrací a klimatizační systémy umožní regulovat základní parametry prostředí ve stanoveném rozsahu. Tento vymezený rozsah by měl být co nejmenší.

2.8.2.1 Větrání

Obecným principem větrání je výměna znehodnoceného vzduchu za vzduch čerstvý. Čerstvým vzduchem se rozumí vzduch z vnějšího prostředí, tedy vzduch venkovní.

Proudění vzduchu ve větraném prostoru je způsobeno nuceným, mechanickým pohybem, nebo přirozeným tlakovým rozdílem. Rozlišujeme tedy větrací systémy nucené, kde je pohyb vzduchu způsoben ventilátory. Nebo větrací systémy přirozené, kde je pohyb vzduchu způsoben vlivem rozdílných hustot vzduchu vně a uvnitř větraného prostoru i vnějšího účinkem větru. V podmínkách specializovaného vyšetřovacího centra leze využít kombinaci obou systémů.

- **Nucené větrání:** Celkové nucené větrání je ideálním druhem větracího systému pro podmínky vyšetřovacího centra. Zajišťuje rovnoměrné provětrání pracovních oblasti, nebo jinak definovaného technologického prostoru. Jelikož v podmínkách vyšetřovacího pracoviště jsou vzniklé škodliviny způsobeny převážně lidmi, jsou všechny tyto škodliviny v prostoru rozmístěny rovnoměrně. Z tohoto důvodu je využití celkového nuceného větrání pro výměnu vzduchu ideální volbou.
- **Přirozené větrání:** Lze využít ve formě dodatečného systému pro výměnu vzduchu. Místní přirozené větrání, respektive odsávání je dobrou volbou, jelikož primárně slouží k přirozenému odvodu vzduchu od zdrojů tepla. Částečně přispívá i k výměně celkového vzduchu v místnosti. Vzduch do prostoru vybaveného šachtovým větráním proniká vlivem přirozeného podtlaku.

2.8.2.2 Klimatizace

Klimatizační systémy upravují vzduch převážně z důvodů hygienických v místnostech pro pobyt osob a také technologických. Podle dispozičního uspořádání se klimatizační systémy třídí na jedno-zónové a více-zónové. V případě malého vyšetřovacího pracoviště, lze využít jedno-zónový systém pro úpravu parametrů v jedné místnosti. Pokud jde o výstavbu celého specializovaného vyšetřovacího centra, je nutné využít klimatizační systém více-zónový. Rozvod tepelné energie do prostoru jsou klimatizační jednotky schopny provádět vícero způsoby. Existují vzduchové systémy, vodní systémy, kombinované systémy, nebo tzv. chladivové systémy. Výběr konkrétního systému je předem jasný, a vždy záleží na konkrétních požadavcích.

2.9 Shrnutí

Tabulka 3: Shrnutí vývoje spec. vyšetřovacího pracoviště, 1. část

Plánování výstavby	
Plánovací fáze má zásadní vliv na výstavbu a následnou funkčnost pracoviště.	Zodpovězení základních otázek před zahájením plánovací fáze.
Vymezení rozsahu budoucích služeb.	Samostatné vyšetřovací centrum nebo vyšetřovací pracoviště v rámci stávající organizace.
Plánování nejen výstavby ale také metod činnosti, budoucí expanze, energetické spotřeby, kvality, atd.	Vyšetřovací pracoviště budované za účelem zisku či nikoli.
Hlavní faktory ovlivňující vývoj	
Cena je hlavním faktorem, který ovlivňuje všechny aspekty výstavby a provozu pracoviště.	Čas potřebný pro vývoj, uvedení do funkčního stavu, dále čas procedur a jiných činností pracoviště, atd. Časová tíseň je během činnosti běžná.
Zdroje pro výstavbu, funkčnost, budoucí expanzi. Stanovit v rámci plánování.	
Výběr vybavení	
Výběr vybavení v závislosti na konkrétních činnostech, nebo na poskytovaných službách.	Více typů vybavení, sloužící jednomu účelu. O výběru rozhoduje především spec. vyšetřovací tým.
Periodická obnova vybavení vzhledem k neustálému vývoji technologií.	Testování nových typů SW/HW ve speciální testovací laboratoři.
Rozvržení prostoru	
Administrativní oblast netechnického charakteru.	Vyšetřovací oblast je srdcem objektu.
Oblast síťových zařízení, členěných podle svého účelu.	Úložiště evidenčních dat, kde se nacházejí všechna data získaná z místa činu.
Bezpečnost	
Administrativní část je volně přístupná, zabezpečení souvisí s bezpečností pláště objektu.	Vyšetřovací oblast podléhá striktním bezpečnostním opatřením. Vstup jen pro vyšetřovací tým a vedení.
Síťová zařízení členěna do fyzicky zabezpečených sektorů.	Podpis při vstupu, možná instalace CCTV. Stanovit správce evidence.
Požární ochrana	
Vodní, plynové a chemické požární systémy.	Pro podmínky spec. vyšetřovacího pracoviště nejvhodnější plynový hasící systém.

Tabulka 4: Shrnutí vývoje spec. vyšetřovacího pracoviště, 2. část

Elektrická instalace a zdroje energie	
Běžná spotřeba zařízení, spotřeba síťových zařízení, specifická spotřeba vyšetřovacích pracovišť.	V rámci velkých objektů realizace vlastních zdrojů elektrické energie. Zdroj primární pro celý objekt, zdroj sekundární pro síťová zařízení sloužící vyšetřovacímu prostoru a úložišti dat.
Realizace záložních zdrojů energie pro všechny funkční oblasti v objektu.	Realizace bezpečnostních opatření pro případné samostatné zdroje el. energie.
Úprava parametrů prostředí	
Pro zajištění optimálních pracovních podmínek pro zaměstnance i technická zařízení.	Využití větracích a klimatizačních systémů.

3 ADMINISTRATIVNA

Administrativní požadavky jsou totožné, ať už se jedná o malé pracoviště nebo velké vyšetřovací centrum. Každý datový vyšetřovací objekt představuje více druhů činností. Základy těchto činnosti budou vždy stejné, ať už se jedná o malé vyšetřovací pracoviště nebo velké vyšetřovací centrum. Tyto hlavní aspekty činnosti jsou obchod, technologie, vědecká praxe a kreativita. Vyšetřovací pracoviště musí zvládat obchodní praktiky, musí pracovat s nejlepší technologií, s vysokým technologickým talentem a musí podporovat kvalitu metod a jejich rozmanitost, kreativní pohled na řešení technologických vyšetřovacích problémů.

Pokud mluvíme o samostatně výdělečném objektu, je jasné, že obchodní stránka činnosti bude na prvním místě. Vyšetřovací pracoviště musí vykazovat zisk. Pokud mluvíme o pracovišti v rámci organizace, takovéto pracoviště je realizováno jako součást bezpečnostní politiky organizace. V takovém případě pracoviště není určeno pro tvorbu zisku, ale pro ochranu organizace. I tak musí být ale financováno, aby mohlo provozovat svou činnost.

Pachatelé kybernetických trestných činů si neustále pořizují nové vybavení a touží po nejkomplexnějších technologiích, aby skryli své zločiny. Z toho důvodu musí vyšetřovací objekt neustále obnovovat svou technologii tak rychle, jak se technologie vyvíjí. Komerční nabídka přichází neustále s novými technologiemi, aby mohli jejich zákazníci, tedy i vyšetřovatelé, držet krok s útočníky, ale i krok s potřebou pokroku zákazníka. Tudíž je nutné prozkoumávat a využívat každou technologii, která může pomoci v jejich snažení.

Pochopení a správné využívání technologií nestačí. Praxe v odvětví našeho zájmu je praxe vědecká. Specializovaní vyšetřovatelé se snaží konat své úkoly podle metod, které jsou spolehlivé, opakovatelné, ověřitelné, objektivní, důsledné a přesné. Odkryjí tak fakta pomocí běžných vědeckých činností jako jsou pozorování, deduktivní zdůvodňování, úprava hypotéz k demonstrování pravdivosti faktů atd.

Vyšetřovací proces je víc než jen předem stanovený set procedur. Během provádění jednotlivých metod hraje pro specializovaného vyšetřovatele intuice a kreativita velkou roli. Nalézání faktů v technologicky obrovsky různorodém světě vyžaduje vysokou úroveň technické zručnosti, stejně jako flexibilní mysl.

3.1 Hlavní cíle a služby

Během uvažování nad specializovaným vyšetřovacím objektem je potřeba navrhnout obchodní plán. Navrhnout jaké služby bude vyšetřovací pracoviště poskytovat a rovněž s jakým rozměrem bude tyto služby poskytovat. Je nutné jasně formulovat budoucí hlavní cíle laboratoře. Stanovený objem a rozměr jednotlivých služeb poskytne pevný dohled nad každým aspektem objektu a nad jeho činnostmi. V závislosti na objemu služeb může dobrá vyšetřovací laboratoř sídlit v jediné místnosti, nebo může vyžadovat celou budovu s různými týmy specialistů, kteří vykonávají rozličné výzvy týkající se mnoha disciplín. Komerční zařízení, zjednodušeně řečeno, typicky definuje servisní balíček a pak balíček prodává zákazníkům.

3.2 Financování

Zajištění správného financování je součástí obchodního plánu nebo chcete-li strategického plánu. Takovýto plán, by měl obsahovat způsob financování objektu a měl by být realizován na několik let dopředu. Obchodní plánování je klíčovým faktorem pro zisk zařízení, stejně jako pro úspěšný růst. Je dobré definovat milníky, kterých je potřeba ve stanoveném časovém horizontu dosáhnout. Realizované obchodní plánování musí plně sloužit potřebám vyšetřovacího objektu jak v aktuálních činnostech, tak v realizaci strategických vizí.

Obchodní plánování podléhá jednoduché úvaze, kdy proti sobě stojí dva faktory. Na jedné straně je to cena za business (tedy to co mě to bude stát) a na straně druhé je ziskovost produktů práce (tedy to co za to dostanu). Každá činnost vyžaduje návrat investice, a to podle růstu rizika. To znamená, že čím rizikovější činnost je, tím větší zisk by z této činnosti měl plynout.

Cena za business obsahuje materiální prvky (věci nutné pro výstavbu a provoz zařízení), stejně jako administrativní prvky, tvorbu procedur a jejich implementací a také nikdy nekončící proces zdokonalování techniky i lidských zdrojů. Není radno zapomínat na to, že vybavení potřebuje údržbu a obnovu. Definování výdělečnosti ve světle jakékoliv dané návratnosti investice se tedy bude také lišit v závislosti na hlavních servisních opatřeních v zařízení.

Celý způsob financování se liší podle toho, o jakou konkrétní realizaci vyšetřovacího objektu se jedná. na jedné straně máme specializované vyšetřovací pracoviště, které je integrované do organizace v rámci její bezpečnostní politiky. Na straně druhé máme samostatné specializované vyšetřovací centrum, které je závislé pouze samo na sobě. Odlišnost těchto dvou druhů vyšetřovacích objektů je jak v důvodu jejich výstavby, tak v jejich činnosti a financování.

3.2.1 Nákladové financování

Vyšetřovací pracoviště a jeho specializovaný tým odborníků je financován organizací, pro kterou vykonává svou činnost. Pracoviště je integrováno do této organizace za účelem její ochrany. Zisk tedy není primárním cílem tohoto pracoviště. Toto vyšetřovací pracoviště pak financují zisku schopné jednotky organizace. Toto financování by se tedy dalo definovat jako nepřímé. Požadavky pro správnou činnost pracoviště se budou týkat personálu, vybavení a času na svou činnost. Cena za tyto požadavky bude využita k ochraně informací a technických zařízení proti kybernetické trestné činnosti.

3.2.2 Financování ziskem

Komerční vyšetřovací servis je placen ze služby, kterou poskytuje a musí vykazovat čistý zisk nad cenou činností, které provádí. Je nutné v rámci obchodního plánu vyvinout cenový model, který definuje cenu za poskytované služby. Cenový model může mít různé formy. může být velmi jednoduchý, ale také velmi komplexní. Za příklad jednoduchého cenového modelu by se dala považovat cena za odpracovaný čas. Tedy například cena za hodinu práce vyšetřovacího týmu. Za komplexnější, tedy složitější způsob cenového modelu by se daly považovat například individuální poplatky za konkrétní vyšetřovací praktickou metodu, kterou vyšetřovací tým musí provést v závislosti na typu hrozby či útoku. Komplexnější cenové modely je složitější implementovat. Navíc složitější cenové modely mohou být pro zákazníka nic neříkající, protože zákazník nemůže vědět jaké typy a kombinace metod budou použity v rámci jeho případu. Je tedy nutná podrobná konzultace s klientem. K tomuto nejlépe poslouží mítinková místnost v administrativní oblasti objektu.

3.3 Organizace práce

Organizace práce vymezí to, jak budou zaměstnanci v objektu strukturováni. Pro příklad, pokud je vyšetřovací tým interní součástí bezpečnosti organizace, musí být definována vzájemná interakce mezi vyšetřovacím pracovištěm a jinými pracovišti v organizaci. Jednoduše řečeno, musí být definován způsob jejich součinnosti.

Struktura organizace práce také stanoví jakým způsobem se bude nakládat s konkrétním případem. Je tím myšlena posloupnost procesů, kterými se bude postupovat v rámci případu, a tím pádem i posloupnost činnosti jednotlivých strukturovaných pracovišť v rámci objektu. Bez patřičného strukturování pracovišť a bez organizace jejich práce, by byla práce na případu chaotická a bez předem stanoveného postupu. Výsledek takové práce by byl nekvalitní a časově zbytečně náročný. Správnou organizací práce zajistíme, že bude každý případ vyřešen v nejkratším možném čase a že se při jeho řešení bude postupovat vždy podle stanoveného procesu.

3.4 Program pro záruku kvality

Kvalita jako taková je subjektivní termín, pro který má každá osoba nebo oblast svou vlastní definici. V technické oblasti může mít kvalita dva významy.

- Kvalita je vlastnost produktu nebo služeb, která má schopnost uspokojit stanovené nebo skryté potřeby. [4]
- Kvalita je produkt služby bez nedostatků. [4]

Řízení kvality je nikdy nekončící činnost. Programy které se snaží zajistit kvalitu jsou vpodstatě metody, jak splnit požadavky a očekávání klienta. Je to schopnost adaptovat se na změnu požadavků klienta. Je to snaha o zvíšení úrovně kvality. Při realizaci systému řízení kvality je nutné vědět jak bude tento systém implementován ve specializovaném vyšetřovacím objektu, jaké budou výhody implementace kvalitního systému pro řázení kvality, a je také dobré vědět na jaké úskalí můžeme při jeho implementaci narazit.

3.4.1 Management řízení kvality

Podstatným krokem při plánování systému řízení kvality je stanovení managera pro řízení kvality. Tato osoba musí mít stanovenu pravomoc a zodpovědnost za řízení systému kvality. Právě tento manager zadává úkoly výkonnému managementu, který tyto úkoly spojené s programem kvality vykonává. Činnost managera kvality má tedy hlavní a naprosto zásadní vliv na splnění požadavků kvality, daných organizací/vyšetřovacím centrem a zákazníkem. Pro úspěch implementování a řízení systému kvality je tedy zásadní správný výběr managera kvality. Tento manager by měl znát všechny aspekty činnosti vyšetřovacího objektu. Musí mít vysokou úroveň autority, jinak se mu v přiměřeném čase systém řízení kvality nepovede implementovat. je to dáno tím, že implementovaný systém řízení kvality musejí respektovat všichni zaměstnanci ve vyšetřovacím objektu. Je zodpovědností managera kvality, aby se tak stalo. V případě, že část personálu tento systém kvality nebude respektovat, stává se tento systém neefektivním, za což nese zodpovědnost manager kvality.

Management řízení kvality poskytuje záruku kvality jak vlastníkovi vyšetřovacího objektu, tak jeho zákazníkům. Záruka kvality má mnoho definic. Pro naše konkrétní potřeby by se demonstrace záruky kvality mohla definovat jako aplikování plánovaných, systematických činností k zajištění toho, že se využívané procedury střetnou s potřebou zákazníka. Jinými slovy, jde o využití prostředků, které zajistí, že naše poskytované služby budou mít zákazníkem vyžadovaný standard kvality.

Činnost managementu řízení kvality ovšem není jednorázová. Implementování systému řízení kvality je pouze prvním krokem, i když nejtěžším. Manager kvality musí splnit požadavky zákazníka s pojené s kvalitou poskytovaných služeb, vybavení, atd. Musí být ale také schopen včas odhalit změny v potřebách zákazníka a na tyto změny včas reagovat změnou části systému řízení kvality. Nemluvě o tom že objemnost systému řízení kvality souvisí úzce s objemem poskytovaných služeb. Pro každou službu/činnost je nutné využít jiné procedury, postupy vyšetřování, vybavení, atd. Z toho plyne, že systém řízení kvality se musí zaměřit na jednotlivé poskytované služby individuálně.

3.4.2 Certifikace

Demonstrace kvality činnosti je důležitá v jakékoli obchodní činnosti. Obecně lze říci, že nezávislý orgán (certifikační společnost) ověří, že vybudovaný systém odpovídá normě, na základě které byl vybudován. Certifikace může být udělena až po auditu. Hlavní cestou, využívanou mnoha subjekty, je ISO certifikace, což je zkratka Mezinárodní organizace pro standardizaci.

V podmínkách vyšetřovacího objektu lze využít normu ISO/IEC 17025. Tato konkrétní norma se týká všeobecných požadavků na způsobilost zkušebních a kalibračních laboratoří. Norma obsahuje všechny požadavky, které musí tyto laboratoře splňovat, pokud chtějí prokázat, že provozují systém řízení kvality. Že jsou způsobilé a schopné dosahovat technicky platných výsledků. Specializované vyšetřovací pracoviště či celé centrum musí pro obdržení této normy splnit nejrůznější požadavky na systém řízení objektu, interní komunikaci, či požadavky na ochranu dat a informací. Po úspěšném splnění požadavků bude ovšem výsledkem zvýšení kvality vyšetřovacího objektu, spokojenost zákazníka a s tím spojená možnost vyššího zisku.

Další normou je systémy managementu jakosti ISO/IEC 9001. Tato norma nemá až takové konkrétně zaměřené využití, jako norma předchozí. Týká se prakticky jakékoliv organizace. V našich podmínkách specializovaného vyšetřovacího objektu je ale dobré ji využít.

3.4.3 Audit

Zajištění kvality činnosti zahrnuje potřebu zavedení několika kontrolních auditů. Individuální procedury musejí být testovány na platnost metod a věrnost postupu. Hardware a software vyžaduje patřičnou kontrolu z důvodu prokázání jeho funkčnosti. Úroveň odpovědnosti jednotlivců musí být testována. Průběh práce vyžaduje audit pro garanci kvality činnosti. Kontrola dokumentů a způsobu nakládání s nimi je vyžadována z důvodu prokázání kompletnosti. Funkčních procedury, respektive činnosti a jejich řízení vyžaduje častou změnu původních odhadů. Kvalitní auditní systém je nutný pro docílení vyžadované úrovně procesů, respektive činností.

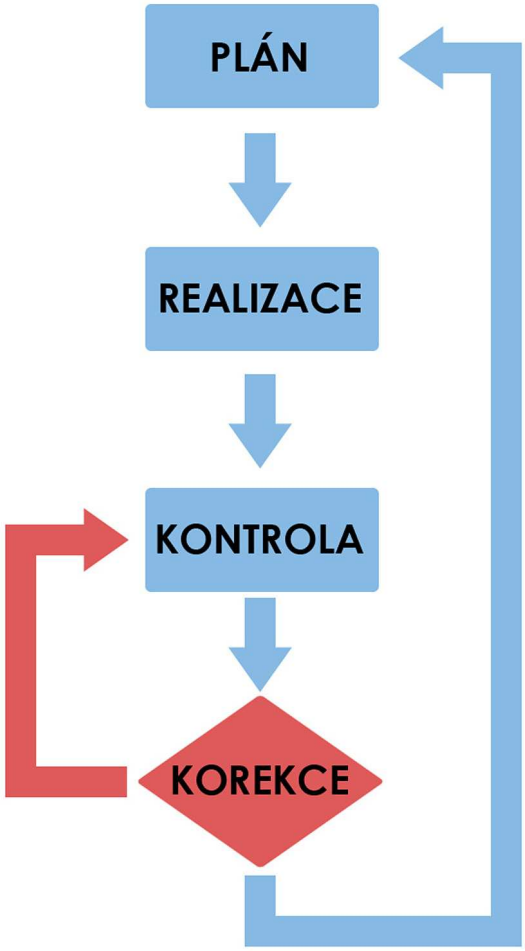
Aby bylo možné zdokonalovat konkrétní prvky specializovaného vyšetřovacího objektu, je nejdříve nějakým způsobem nutné identifikovat prvky, které jsou neefektivní a které je tak možné zlepšit. Audit je jedním z nejefektivnějších metod, vedoucích k zdokonalování systému kvality. Bez kvalitního auditu, by jsme nemohli vědět, kde má náš specializovaný vyšetřovací objekt své nedostatky. Aby bylo možné tyto nedostatky odstranit, je nejdříve nutné je vůbec odhalit. K tomu nám pomohou právě audity. Audit můžeme provést sami, nebo můžeme požádat externí firmu, která tuto kontrolu poskytne za úplatu. Výhodou při využití externí sufitní firmy je fakt, že tato externí firma nebude zasažena profesní slepotou. Během dlouhodobé činnosti je totiž možné, že zaměstnanci přestanou vnímat určité nedostatky ve své práci. Buďto nevědí, že lze činnost provádět lépe, časově efektivněji, s menším finančním nákladem, nebo si některé činnosti přizpůsobují vlastním potřebám a samotná kvalita se stává podřadnou. V takové situaci jistě pomůže externí audit, které může odhalit některé netušené nedostatky. Sice takováto externí auditní služba něco stojí, ale návratnost pro náš specializovaný vyšetřovací objekt bude zaručena, díky eliminaci nedostatků a tím pádem snížením finančních, časových a dalších nákladů na naši činnost.

Každé zdokonalení, učiněné díky auditu, by mělo být řádně zdokumentováno. Zamezíme tak možnému budoucímu opětovnému snížení kvality. Audit jako takový se může týkat prakticky všech aspektů specializovaného vyšetřovacího objektu. Od kontroly konkrétních činností, procedur, bezpečnosti, produktivity práce, po audity strategie, marketingu, rentability, atd. Nejdůležitější typy kontrol jsou ovšem ty, které mají přímý vliv na spokojenost zákazníka a na zisk specializovaného vyšetřovací objektu, respektive obecně na kvalitu produktu činnosti.

3.4.4 Zdokonalování systému řízení kvality

Neustálé kontinuální zdokonalování systému managementu kvality je úzce spojeno s již dříve uvedenou normou ČSN EN ISO 9001. Tato norma se týká nejrůznějších principů řízení kvality. Jedním z těchto principů je právě nepřetržité zdokonalování. Tento princip mimo jiné říká, že cílem pro organizaci by mělo být zajištění neustálého zdokonalování výkonu organizace.

Pro zavedení tohoto nepřetržitého zdokonalování systému řízení kvality je nutné stanovit metodický postup.



Obrázek 3: Proces nepřetržitého zdokonalování systému kvality

Na obr. 3 vidíme základní proces pro kontinuální zdokonalování systému kvality. Takovýto proces je adaptabilní potřeby zákazníka a je také adaptabilní na změnu jeho potřeb. Pokud chceme zdokonalit nějaký konkrétní aspekt činnosti, je nutné nejdříve stanovit plán. Ten bude obsahovat při nejmenším zodpovězení tradičních otázek (kdo, co, kdy, kde, proč). Pokud je plán stanoven, víme co chceme zdokonalit, víme jak na to a podobně, přistoupíme k realizaci tohoto plánu. Po úspěšné realizaci následuje fáze pozorovací, čili kontrola funkčnosti. Tato kontrola by měla být řádně zdokumentována. Základním výstupem kontroly by mělo být vymezení bodů, které vedly ke zlepšení a bodů které oproti předpokladům zlepšení nepřinesly či dokonce znamenaly zhoršení oproti předchozímu

stavu. Pokud tedy během kontroly zaznamenáme body, které neznamenaly zlepšení, následuje případná korekce. Jejím účelem je napravit nedostatky původního plánu a tyto nedostatky posléze implementovat. Po implementování nedostatků následuje opětovná kontrola. Celou smyčku kontrol a korekcí opakujeme do té doby, dokud budeme během kontrolní fáze nacházet nedostatky. Pokud nenajdeme další nedostatky, je celá implementace zdokonalení u konce.

3.4.5 Ověření kvality nástrojů

Využívání pouze certifikovaných a ověřených nástrojů je nezbytností a výběr těchto nástrojů má zásadní vliv na kvalitu poskytovaných služeb. Všechny nástroje, využívané pro činnost specializovaného vyšetřovacího objektu, jsou určeny pro práci s daty. Těmito nástroji získaná a analyzovaná data jsou poté využita jako důkazní materiál. Proto je nutné zajistit důvěryhodnost těchto evidenčních dat tím, že pro jejich získání a analýzu využijeme pouze všeobecně uznávané a certifikované softwarové a hardwarové nástroje.

Dalším důvodem proč využívat pouze ověřené softwarové a hardwarové nástroje je skutečnost, že žádný s těchto testováním ověřených nástrojů nebude mít negativní vliv na interní technické zařízení v objektu, a to především na lokální datovou síť.

Ověřování kvality by mělo probíhat v rámci vyšetřovacího pracoviště. Již během výstavby specializovaného vyšetřovacího objektu byla zmíněna potřeba testování nových nástrojů. Pokud tyto nástroje testujeme mi sami, nikoli externí subjekt, získáme tak velmi důležitý materiál, respektive dokumentaci proběhlého testu. Samotný test nám poslouží nejenom k výběru ideálního nástroje pro konkrétní danou činnost, ale také podá důkaz o tom, že využívaný nástroj nemá žádný negativní vliv na vyšetřovanou datovou evidenci. To znamená, že tato dokumentace o testu zaručuje, že informace analyzované nástrojem jsou tímto nástrojem nenarušené, respektive že je zachována jejich integrita a tím pádem jejich důvěryhodnost.

Samotný test nástroje má určité fáze. První fází je příprava. V této fázi je třeba připravit nástroj, který bude testován. Dále je potřeba připravit prvek, na kterém se bude nástroj testovat. To znamená, že pokud budeme například testovat softwarový nástroj pro analýzu dat, připravíme si harddisk s uloženými daty. S těmito daty bude pak softwarový nástroj

během testu pracovat. Tímto ovšem přípravná fáze nekončí. Následuje stanovení scénáře. Tedy určitá posloupnost kroků, které budou během testu prováděny. Mluvili jsme o nástroji pro analýzu dat jako o příkladu. V tomto konkrétním příkladu by byl scénář realizován tak, že by definoval postup analýzy prováděné nástrojem. Takže například analýza smazaných, přesunutých, zakódovaných a jiných dat, jejich znovuzískání, atd. Jednotlivé kroky by byly stanoveny v rámci jednoho celkového testovacího postupu. Po testu následuje dokumentační fáze. Takže ze získaných výsledků testu, vytvoříme dokument, ve kterém je jasně zdokumentován celý průběh testu a jeho výsledky. Výsledky mohou být ve smyslu pozitivním či negativním. To znamená zda nástroj splnil požadavky, splnil s výhradami, či nesplnil stanovené požadavky. Takovýmto způsobem můžeme ověřit kvalitu využívaných nástrojů a v případě nedostatků sjednat nápravu.

3.4.6 Vzdělávání a talent

Specializované vyšetřovací pracoviště je pouze tak dobré, jako talent a iniciativa jeho zaměstnanců. Systém řízení kvality tedy musí brát v potaz i kvalitu personálu, a to především u obsazení specializovaného vyšetřovacího týmu. Zkušenosti vytvářejí vědění. Stálé vzdělávání a seriózní investování do rozvoje lidských zdrojů jsou nepostradatelné pro celkový úspěch vyšetřovacího pracoviště. Jelikož se technologický svět stále vyvíjí, je nejdůležitější vlastní iniciativa vyšetřovatele. Jedině tak bude schopný držet krok se svým rivalem, kybernetickým zločincem. Existuje nespočet škol, ať už v České republice nebo v zahraničí,které mohou zajistit základní i pokročilé vzdělávací programy. Existují tuzemské i zahraniční firmy, poskytující poradenské služby. Před využitím těchto služeb je nutné pečlivě ověřit, zda je tato poradenská služba v oboru našeho zájmu dostatečně kvalifikována, abychom měli jistotu přínosu této služby pro náš specializovaný vyšetřovací objekt, respektive pro naše zaměstnance. Stejně ale pořád platí fakt, že hlavní podíl na svém vzdělání a odbornosti má sám zaměstnanec. Jak už bylo mnohokrát řečeno, svět technologií se neustále vyvíjí, a proto je specializovaný vyšetřovatel ten, který musí zapojit iniciativu a talent, aby byl skutečným odborníkem a potřebným zaměstnancem našeho specializovaného vyšetřovacího objektu.

3.5 Shrnutí

Tabulka 5: Shrnutí administrativní činnosti spec. vyšetřovacího pracoviště

Hlavní cíle a služby	
Vymezení budoucích služeb a jejich rozsahu.	Od budoucích služeb se odvíjí vývoj pracoviště, jeho vybavení a velikost.
Financování	
Součást obchodního plánu.	Plán financování navržen na několik let dopředu.
Zaručení návratnosti investice.	Nákladové financování nebo financování ziskem v závislosti na druhu pracoviště.
Organizace práce	
Strukturování spec. vyšetřovacího objektu na části z hlediska druhu činnosti konkrétních částí.	Definování procedur, které vymezí činnost jednotlivých částí spec. vyšetřovacího objektu.
Program pro záruku kvality	
Metody, jak splnit požadavky a očekávání zákazníka.	Implementace systému řízení kvality.
Certifikace je způsob demonstrace kvality.	ČSN EN ISO 17025, ČSN EN ISO 9001, ČSN EN ISO 17799.
Bez auditu nelze docílit vyšší úrovně kvality.	Pokud audit odhalí nedostatky, je nutné zavést obecný metodický postup jejich odstraňování.
Kvalita SW/HW musí být testována.	Lidský faktor ovlivňuje kvalitu práce.

4 OBECNÁ METODIKA ČINNOSTI VYŠETŘOVATELE

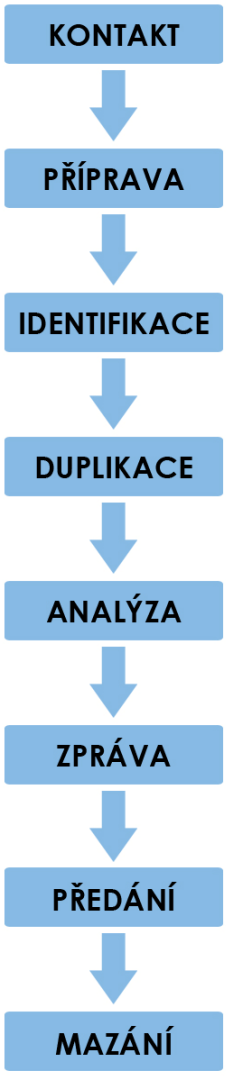
Vyšetřovatel kybernetické kriminality následuje určité stádia a procedury, když pracuje na svém případu. Za prvé identifikuje zločin, společně s počítačem a dalšími nástroji použitými k spáchání zločinu. Poté postupně získá evidenci, tedy důkazy. Jakmile získá potřebná data musí je duplikovat a pak analyzovat tuto duplikovanou evidenci. Poté co byla evidence analyzována, vyšetřovatel zdokumentuje výsledek své práce. Pověřená osoba následně předá tuto dokumentaci klientovi. Klient poté zváží, zda jsou zjištěné důkazy natolik závažné, aby podal trestní oznámení. V případě, že se tak stane, vyšetřovatel vystoupí jako expertizní znalec, respektive svědek a prezentuje zjištěné důkazy u soudu. Konkrétní vyšetřovací metody a procedury by měly být stanoveny pro zajištění toho, že vyšetřovatel během své činnosti bude postupovat stanoveným, nejefektivnějším postupem.Vyšetřovatel musí dodržovat tyto předem stanovené procedury jak jen to je možné.

Skutečnost je taková, že většina dat je v elektronické podobě. Schopnosti, vyžadované k hledání dat, nejsou v žádném případě zanedbatelné. Ba právě naopak. Specializovaný vyšetřovatel musí prozkoumat naprosto všechna data. Nemluvě o tom, že některá data nemusejí být na první pohled vidět, respektive jsou skrytá, smazaná a podobně. Proto musí být specializovaný vyšetřovatel velmi vzdělanou osobou v tomto oboru. Právě on ručí za získaná data,. ručí za výsledek celého případu. Nemluvě o tom, že digitální evidence je velmi citlivá záležitost ve smyslu obnovování smazaných, zakódovaných, nebo porušených dat ze systému. Díky všem těmto skutečnostem je nutnost specifického přístupu specializovaného vyšetřovatele. Dat s kterými manipuluje nejsou jeho, jsou klienta. Proto během vyšetřovacího procesu nesmí porušit integritu těchto dat, musí pracovat důsledně, nesmí data zneužít ani je jakkoli upravovat. Jedině tak mohou mít získaná evidenční data patřičnou důvěryhodnost,a jedině tak mohou tyto evidenční data usvědčit pachatele.

Metodické postupy činnosti během vyšetřování by měly být stanoveny obecnými procedurami v rámci činnosti specializovaného vyšetřovacího týmu. Během vyšetřovací fáze je celý vyšetřovací postup zaznamenáván. Lze tak posoudit odlišnosti během vyšetřování od předem stanovené obecné metodické procedury.

4.1 Posloupnost událostí

Pro lepší pochopení činnosti specializovaného vyšetřovacího pracoviště, uveďme obecný příklad sledu událostí, které nastanou bezprostředně po zjištění napadení, útoku, respektive po zjištění nestandardní situace.



Obrázek 4: Posloupnost událostí

- Personál společnosti zavolá specializované vyšetřovací pracoviště pro radu.
- Specializovaný vyšetřovatel připraví první kroky, jako odpověď na událost. Například výběr vhodných nástrojů, výběr vhodných obecných metodických procedur, atd.

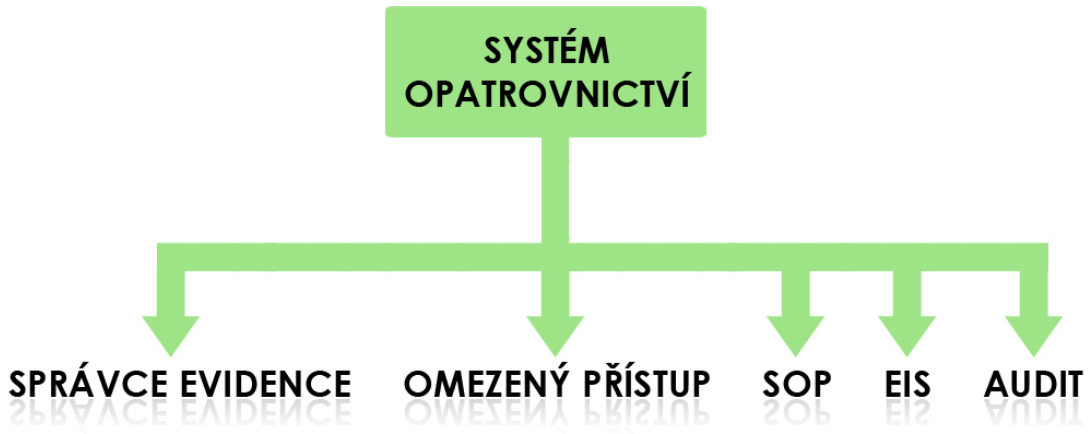
- Specializovaný vyšetřovatel shromáždí pomocí předem vybraných nástrojů evidenci na místě činu a přepraví ji do vyšetřovací laboratoře. Pokud jsou potřebná data příliš objemná, lze provést kopírování dat přímo na místě činu. Mluvíme v tomto bodě o originálních datech a jejich duplikované verzi, která poslouží k pozdější analýze.
- Specializovaný vyšetřovatel připraví bit-streamové obrazy dat a vytvoří MD5 těchto dat. Bit-streamový obraz je přesný duplikát počítačového harddisku, nebo jiného datového média. Disk je tedy kopírován z jednoho disku na druhý bit po bitu. Takovýto obraz je autentický k originálu díky shodnému digitálnímu podpisu, který je vytvořen matematickým algoritmem (obvykle MD5 standard). Díky tomu nelze tento obraz zaměnit s jinou evidencí a je jisté, že v něm nebudou učiněny jakékoli změny.
- Specializovaný vyšetřovatel prozkoumá pomocí hardwarových a softwarových nástrojů získaná evidenční data pro potvrzení zločinu a připraví vyšetřovací zprávu před ukončením vyšetřování.
- Citlivá zpráva je předána klientovi. Ten ji zhodnotí a na základě ní rozhodne, zda chce podat trestní oznámení či nikoli.
- Specializovaný vyšetřovatel zničí jakákoli nepotřebná citlivá data klienta. V případě, že se po konzultaci klient rozhodne nepodávat trestní oznámení, jsou všechna duplikovaná data zničena. Pokud klient bude chtít zužitkovat zjištěné informace, zničí se pouze nepotřebná data a data evidenční jsou archivována.

Je velmi důležité aby specializovaný vyšetřovatel postupoval podle všech těchto kroků. Stejně tak je důležité, aby celý proces neobsahoval žádné desinformace. Tyto desinformace, respektive neúplné informace o evidenci mohou vzniknout jedině za předpokladu, že osoby nakládající s evidenčními daty nedodrží stanovené procedurální postupy. Tyto nedostatky v činnosti personálu se odrazí na neúplné či upravené evidenci, a takováto evidence by mohla zničit reputaci vyšetřovatele nebo reputaci organizace, ve které pracuje.

4.2 Systém opatrovnictví

Systém opatrovnictví je precizní, správný způsob pohybu a držení každé části evidence. A to od času, kdy jsou data převzata do opatrovnictví, až do doby než je evidence předložena u soudu. Tento systém pomůže předejít falšování či obcházení evidence. Systém opatrovnictví také prokáže, že byla evidence uchována v legálně akceptovatelné lokaci a dokumentuje, kdo je v opatrovnictví a kdo nakládá s evidencí během vyšetřovací analytické fáze. Kriticky důležité je zachovat integritu a důvěryhodnost evidenčních dat. K tomuto právě poslouží vhodné zavedení systému opatrovnictví v rámci specializovaného vyšetřovacího pracoviště. Cílem tohoto systému je také zajistit, že za každou část evidenčních dat bude někdo konkrétně zodpovědný. Za každou činnost spojenou s konkrétní částí datové evidence budou nést konkrétní osoby zodpovědnost. Systém opatrovnictví také zajistí, že každá část evidence bude po vyšetřovacím procesu navrácena vlastníkovi, nebo bude po domluvě s vlastníkem evidenčních dat zničena.

Každá osoba, která přijde s evidenčními daty do styku, by tedy měla mít v rámci systému opatrovnictví stanoven procedurální postup nakládání s evidencí a tento postup by měla dodržovat. Tyto postupy jsou označeny jako standardní operační procedury. Následující prvky jsou nutným minimem toho, co by měl systém opatrovnictví obsahovat.



Obrázek 5: Základní prvky systému opatrovnictví

- **Správce evidence:** Je nezbytné stanovit správce evidence, a to jak té původní datové evidence, tak té duplikované datové evidence. Tento správce je zodpovědný za archivovaná data v úložišti datové evidence.

- **Omezený přístup:** Limitovaný přístup do prostoru úložišť evidenčních dat je nezbytností. Obvykle má do těchto prostor přístup pouze správce evidence. Všechen přístup do prostoru datových úložišť by měl být zaznamenáván. Jakákoliv aktivita uvnitř tohoto prostoru také.
- **SOP:** Stanovení tzv. standardních operačních procedur, pro všechny aktivity spojené s evidenčními daty. Sběr, přeprava, uchovávání, označování, mazání evidence a podobně. Pro všechny tyto činnosti by měla být stanovena procedura, která definuje způsob nakládání s evidencí během jedné z těchto konkrétních činností.
- **EIS:** Evidenční informační systém je v podstatě databázový systém, do kterého se ukládají informace o evidenčních datech. Každá část evidenčních dat by měla být označena jedinečným identifikačním kódem. Mělo by být uvedeno kdo, kde, jak, kdy a proč tuto část evidence získal. V tomto systému by také mělo být zaznamenáváno, které osoby během vyšetřovacího procesu konkrétní evidenční data využívaly, včetně času a jiných podrobností, a to průběžně během vyšetřovacího procesu. Evidenční informační systém v podstatě obsahuje data o evidenčních datech.
- **Audit:** Audit podléhá všem výše zmíněným součástím systému opatrovnictví. Od kontroly standardních operačních procedur, až po kontrolu správné funkčnosti evidenčního informačního systému. Je nutné kontrolovat správné zaznamenávání provozu v evidenčním úložišti dat. Stejně tak je důležité využívat audit ke kontrole činnosti správce evidence.

Správná implementace systému opatrovnictví zaručí důvěryhodnost a celistvost evidenčních dat. Celistvost a důvěryhodnost dat jsou totiž základní prvky informační bezpečnosti. A o ochranu informací nám pří integrování systému opatrovnictví jde především.

4.3 Metodický postup vyšetřování

Postup specializovaného vyšetřovatele během vyšetřování se dá v obecné rovině shrnout do několika hlavních kroků, které během své činnosti pokaždé vykonává. Celý postup se skládá v podstatě ze třech fází. První fáze je fáze poznávací. V ní se specializovaný vyšetřovatel snaží získat všechny možné informace o události jeho zájmu, identifikuje data, která utrpěla újmu a jiná data, která mohou být užitečná během celého vyšetřování. Druhou fází je analytická činnost, která probíhá přímo ve vyšetřovací laboratoři. Zde, v závislosti na dané situaci, specializovaný vyšetřovatel využije konkrétní analýzy k zjištění podrobností o události, pro identifikaci důkazů, atd. Poslední fází je fáze dokumentační. Ta probíhá prakticky během celého procesu vyšetřování. Postupně jsou zaznamenávány kroky, které byly uskutečněny v rámci vyšetřování. Specializovaný vyšetřovatel průběžně zapisuje svůj postup, další dokumentace probíhá v rámci evidenčního informačního systému, zmíněném výše. Vyšetřování tedy vždy probíhá podle posloupnosti obecných kroků, a to identifikace dat, sběr vhodných dat, analyzování těchto dat, dokumentování informací o získaných datech a postupu vyšetřování, nakonec prezentace výsledků vyšetřovacích procesů.

4.3.1 Příprava a identifikace

Identifikační proces je prvním krokem vyšetřování. Jde o proces, který je realizován zpravidla přímo na místě činu. Tedy tam, kde bylo zjištěno podezření na spáchání kybernetického zločinu. Cílem je získat všechna data, díky kterým bude možné zjistit druh útoku a která mohou být nápomocna při odhalení a usvědčení pachatele tohoto útoku. Vyšetřovatel musí disponovat vysokou mírou odborné znalosti, aby byl schopen prozkoumat naprosto všechny lokace, kde by se mohly nalézat potřebná data. Způsob na jakých místech a jakým způsobem data hledá je podmíněno druhem kybernetického útoku. Není od věci konzultovat všechny možnosti nalezení dat s jinými znalci, kteří tak mohou být nápomocni při hledání dalších evidenčních dat. Samozřejmě takováto konzultace platí pouze v případech, kdy hledaná data mají stálou povahu. Data dočasná, která mohou být po určité době ztracena, je nutné získávat přednostně.

Před samotným identifikováním evidenčních dat je nutné realizovat důkladnou přípravu. Administrativní sekce specializovaného vyšetřovacího objektu přijme zakázku a tu pečlivě zdokumentuje, vypíše formulář obsahující základní informace o zakázce a klientovi. Administrativní sekce musí také pečlivě ověřit, zda má klient právní nárok na jeho zakázku, respektive informace, kterých se tato zakázka týká. To znamená, zda-li není realizace této zakázky protizákonná. Specializovaný vyšetřovatel, který je pověřen vykonáním této zakázky, poté obdrží od administrativní sekce vyplněný formulář se všemi důležitými informacemi o případu. Jakmile tento formulář vyšetřovatel obdrží, může se připravit a realizovat první kroky. Zvolí potřebné vybavení, které bude na místě činu potřebovat, formuluje hlavní otázky, které je potřeba během vyšetřování zodpovědět, připraví si dokumentační listy, které využije k zapisování posloupnosti jeho kroků na místě činu. Specializovaný vyšetřovatel musí být technickým odborníkem, který ovšem mimo technické stránky věci zná i své pravomoci a povinnosti.

Přímo na místě činu platí zásada, že by se všechna data měla zkoumat, respektive analyzovat až po převozu ve vyšetřovací laboratoři. Naskytnou se ovšem i případy, kdy tento převoz dat není z nějakého důvodu možný. Pokud je tedy situace taková, že je třeba zjištěná data analyzovat přímo na místě činu, je nutné zvážit několik zásadních otázek, před samotným započetím analýz. Předem je nutné zvážit zda s sebou má vyšetřovatel vhodné vybavení, měl by zvážit čas potřebný pro získání a prozkoumání dat, měl by zvážit dopad jeho činnosti na obchodní či jiné zájmy společnosti, která si jej najala, určit možné komplikace vzhledem k místu kde bude analytickou činnost provádět, zvážit zda má dostatečné právní a zaměstnanecké pověření k provádění nestandardních kroků přímo na místě činu a podobně.

Může se stát, že během identifikační fáze vyšetřovatel nalezne jiná data, která vedou k jinému zločinu. V takovém případě musí zvážit všechny právní aspekty, které s těmito novými nečekanými daty souvisejí. To znamená v podstatě zopakovat část přípravného procesu a nejlépe tyto nové skutečnosti konzultovat s nadřízeným orgánem a případně i s klientem.

V této fázi vyšetřování přichází na řadu také kontinuální dokumentování činnosti. Během celého procesu na místě činu jsou dokumentovány postupy vyšetřovatele. Základem je vnější prohlídka, která probíhá obdobně jako u vyšetřování jakéhokoliv trestného činu. Vyšetřovatel provede obhlídku místa činu a přitom pořídí fotografie. Na nich se snaží

zachytit jakékoliv nestandardní skutečnosti, jako např. porušené pečeti na krytech zařízení, chybějící části vybavení, chybějící štítky a podobně. Stejně tak je provedena fotografická dokumentace vnitřních prostor hardwarových vybavení. Zjistíme tak všechny HW prvky, které zařízení obsahuje, jejich rozšíření oproti standardu a podobně. Společně s fotodokumentací se zapisují jednotlivé kroky, učiněné vyšetřovatelem během jeho práce na místě činu.

4.3.2 Sběr

Po identifikování všech důležitých dat je nutné tyto data získat a ve standardním případě také převést do vyšetřovací laboratoře k podrobné analýze. Během získávání evidenčních dat vzniká choulostivá situace, kdy vyšetřovatel za žádnou cenu získávaná data nesmí nějakým způsobem upravit, poškodit, či zničit. To ovšem může být v některých situacích značně obtížné. Je potřeba učinit taková opatření, aby byla zajištěna celistvost a důvěryhodnost získávaných dat, jak už bylo mnohokráte řečeno. Naprosto nezbytné je v této souvislosti využití tzv. blokování zápisu. Jedině tak, mohou být získaná data považována za důvěryhodná. Všechna data získávaná z technického zařízení je dobré kopírovat na systému vyšetřovatele. To znamená, že pokud to situace umožňuje, je dobré všechny datové média bezpečně vyjmout z původního technického zařízení a stanoveným postupem data klonovat na operačním systému znalce. Během klonování se využívá hardwarových zařízení, či softwarových programů, které chrání původní datová média před chtěným či nechtěným zápisem. Samotné klonování dat, po aktivaci ochrany proti zápisu, provádíme softwarovými či hardwarovými nástroji k tomu určenými, jako např. forenzní duplikační software nebo specializovaná hardwarová forenzní zařízení.

Jak už bylo řečeno, je dobré využít pro klonování dat vybavení specializovaného vyšetřovatele. Mohou ovšem nastat situace, kdy vyšetřovatel své vybavení použít nemůže a musí tak kopírovat data přímo z původního technického zařízení, respektive původního operačního systému. K získání evidenčních dat může být potřeba vybavení, které vyšetřovatel nemá. To se stává např. v situaci, když musí využít síťová zařízení. Nebo u starších datových médiích se může stát, že nejsou s novým operačním systémem kompatibilní, vykazují chyby v činnosti podobně.

V situaci, kdy není možné datová média odpojit od původního technického zařízení, využijeme externí harddisky, které připojíme k původnímu technickému zařízení. I zde využijeme ochranu proti zápisu. Jelikož ale kopírujeme data z původního technického zařízení, je dobré nabootovat zkoumaný systém pomocí speciálního forenzního systému z datového nosiče. Díky tomuto forenznímu systému jsme posléze schopni díky jeho funkcím zjistit všechny potřebné informace o operačním systému původním, ale máme jistotu, že tento původní operační systém a hardware, na kterém běží, nijak neporušíme. Ovšem vzhledem k možným úskalím, která mohou vzniknout v případě získávání dat z původního zkoumaného systému, je dobré tento nestandardní způsob získávání dat využít pouze v naléhavých a nikterak jinak řešitelných situacích.

Do dokumentace je nutné zapsat všechna specifická identifikační data o všech datových médiích, která během vyšetřování kopírujeme. Při získávání dat za použití původního zkoumaného systému, je nezbytně nutné věnovat zvýšenou pozornost dokumentování všech skutečností. Je to z důvodu, že při takovémto způsobu získávání dat hrozí mnohem větší riziku porušení integrity dat, než při běžném způsobu kopírování. Pokud během kopírování dojde ke změně dat, máme díky pečlivé dokumentaci přehled o tom, jaký je skutečný rozsah změn a zda-li tyto změny mají vliv na důvěryhodnost získaných informací.

4.3.3 Analýza

Analytických metod pro zkoumání evidenčních dat je mnoho. Využití konkrétních analytických metod závisí vždy na konkrétní situaci, na povaze získaných dat a na našem cíli. Tedy na tom, jaké typy informací chceme z těchto dat získat. Jelikož rozměr této problematiky je velmi rozsáhlý, je dobré mít na vyšetřovacím pracovišti více specialistů, s rozdílným zaměřením. Každý vyšetřovatel by měl být zaměřen na konkrétní typ činnosti a měl by být samozřejmě na tuto činnost řádně vyškolen. Před započetím analytické činnosti je ovšem nutná důkladná příprava. V rámci vyšetřovací forensní činnosti je dobré stanovit v rámci vyšetřovacího pracoviště obecné analytické procedury, respektive postupy, a to v závislosti na druhu analýz. Tento obecný procedurální postup vyšetřovatel využívá při své analytické činnosti jako referenční základ.

Celé analytické zkoumání je prováděno výhradně na kopiích originálních dat. Analytická činnost specializovaného vyšetřovatele je zaměřena v obecné rovině nejdříve na

extrahování dat a posléze jejich analýzu. Analýzou se snažíme zjistit nejrůznější skutečnosti, které jsou s konkrétními daty spojeny. Důvodem je snaha zjistit jakékoliv důležité informace, které mohou posloužit jako důkazní materiál.

Pokud mluvíme o extrakci, respektive obnovení získaných dat, pak musíme obecně rozlišit tuto činnost na extrakci fyzickou a extrakci logickou.

- **Fyzická extrakce:** Je podstatě základem obnovování získaných dat. Data extrahujeme podstatě na fyzické úrovni. To znamená, že nevyužíváme souborový systém na datovém médiu. Využíváme nástroje pro extrahování souborů, hledáme podle zadaných klíčových slov a podobně. Zkoumáme data, která nejsou nikterak spojena s operačním systémem či souborovým systémem. Jsou to v podstatě data, která jsou fyzicky přítomna a my je můžeme vizuálně detekovat.
- **Logická extrakce:** Rozdílem je, že bereme v úvahu existující systém souborů. V této situaci obnovujeme data z na první pohled nepřístupných míst, jako nepoužitý prostor disku., zkoumáme atributy souborů, umístění souborů v adresářové struktuře, obnovujeme smazaná dat, získáváme komprimovaná data, obnovujeme zakódovaná data a podobně.

Pokud chce vyšetřovatel prozkoumat celé datové úložiště, musí využít obě metody extrakce. Jedině tak může získat kompletní informace, které mohou být klientem využity jako důkazní materiál. Prozkoumání všech uložených dat je naprosto zásadní, protože neúplná informace může být lehce zpochybněna.

Obnovením dat z datového nosiče ovšem celý vyšetřovací proces ve forensní laboratoři teprve začíná. Následuje analytická činnost, jejíž cílem je určit důležitost jednotlivých dat pro konkrétní případ. Využívaných analýz, ať už v obecné či praktické rovině, je mnoho a proto nemá smysl tyto analýzy uvádět. Jednotlivé principy analytické činnosti popíšeme až v nadcházející kapitole. Analyzovat můžeme skrytá data, aplikace, běžné soubory, časové informace o datech, vlastnictví dat či nakládání s daty a podobně. Konkrétní výsledky jednotlivých analýz nemusejí být dostatečně průkazné. Proto jen s těží můžeme využít jeden typ analýzy a poté učinit závěr. Závěry z jednotlivých analýz je nutné posuzovat společně, protože mohou být tyto závěry navzájem provázané. Dostaneme tak mnohem komplexnější a věrohodnější informace o trestném činu. Naprostou samozřejmostí je v tuto

chvíli opětovná nutnost zhotovení podrobné dokumentace o celé analytické fázi vyšetřování. Protože jediné informace, které lze posléze využít jako důkaz, jsou ty informace, které jsou pečlivě zdokumentovány. Dokumentování celkové závěrečné zprávy o případu je poslední fází vyšetřování.

4.3.4 Dokumentace a prezentace

Po ukončení analytické činnosti a po nalezení dostatečného množství faktů o případu, následuje vyhotovení závěrečné správy. Tato závěrečná zpráva obsahuje shrnutí celé dosavadní činnosti, včetně získaných informací. Je důležitá z mnoha důvodů. Základem je zdokumentování získaných důkazů, ale jsou zde i další důležité věci. Dokumentace o případu je ve specializovaném vyšetřovacím objektu archivována pro případ pozdějšího využití. Takovéto dokumentace jsou navíc nezbytnou podmínkou realizace pravidelných auditů, které právě díky dokumentaci mohou odhalit nedostatky v činnosti vyšetřovatelů či nedostatky v definovaných obecných operačních procedurách. Tato dokumentace může být psána ručně do předpřipravených formulářů, nebo jsou skutečnosti o případu zapisovány do elektronických formulářů v rámci informačního systému.

Celá dokumentace musí být přesná, komplexní a pravdivá. Zodpovídá za ni ten, kdo ji napsal, což většinou nebývá pouze jedna osoba. Na případu se dozajista bude vždy podílet několik zaměstnanců najednou, nebo postupně podle stanovených kompetencí. V případě odhalení nedostatků, pak tito zaměstnanci musí nést následky.

Průběžná dokumentace, psaná během vyšetřování, má zpravidla technickou povahu. Ovšem při realizaci závěrečné zprávy je dobré tuto zprávu psát v závislosti na cílové skupině. Nejlepším řešením je realizovat vždy několik druhů závěrečné zprávy, týkající se stejného případu. Jiný typ závěrečné zprávy pro archiv, jiný typ pro klienta a podobně.

Ustanovení způsobu dokumentování případu a ustanovení konkrétních typů dokumentačních listů je na vedení specializovaného vyšetřovacího centra. Těchto dokumentů může být opravdu hodně.

Závěrečná zpráva je ovšem nejpodstatnějším dokumentem, protože obsahuje závěrečný souhrn informací z celého objemu dokumentace, který byl postupně sepsán během řešení případu. Tato závěrečná zpráva by měla obsahovat při nejmenším tyto informace:

- Identifikace případu, jeho stručný popis, informace o klientovi, atd.
- Identifikace forenzních laboratoří a vyšetřovatelů, kteří se na případu podíleli. A jak konkrétně.
- Datum převzetí případu a datum jeho ukončení. Datumem ukončení se zpravidla rozumí datum vyhotovení závěrečné zprávy.
- Identifikace a popis všech prvků, které byly během vyšetřování zkoumány.
- Seznam otázek, které měly být během vyšetřování zodpovězeny. A zda-li se tak stalo.
- Seznam všech externích znalců a jiných pracovníků, kteří se na případu podíleli, a jak.
- Seznam kroků, které byly během vyšetřování provedeny.
- Závěrečné výsledky vyšetřování.

Tato závěrečná zpráva by měla být vyhotovena v několika verzích, v závislosti na tom, komu je určena. Jejím cílem není podrobně informovat o všech aspektech vyšetřování, ale podat stručnou a jasnou zprávu o tom, jak vyšetřování proběhlo, kdo se na vyšetřování podílel a jaké jsou výsledky vyšetřovacího procesu.

Závěrečná zpráva je archivována, nejlépe v tištěné i elektronické podobě. V elektronické podobě by měla být uložena do databáze informačního systému specializovaného vyšetřovacího centra, pro zajištění jednoduché správy těchto dokumentů.

Vyhotovená zpráva je předložena klientovi. U předání by měl být také odborník, který je schopen klientovi poskytnout veškerý poradenský servis. Jedině tak bude klient moci po zvážení rozhodnout o dalších krocích v tomto případu. To znamená, zda-li bude chtít získané informace využít či nikoli. Všechna nepotřebná data jsou po konzultaci s klientem zničena.

4.4 Shrnutí

Tabulka 6: Shrnutí obecné metodiky činnosti vyšetřovatele

Posloupnost událostí	
Představuje obecnou posloupnost kroků, které musí nastat jako odpověď na požadavek klienta, respektive na nastalou událost.	
Systém opatrovnictví	
Systém opatrovnictví je precizní, správný způsob pohybu a držení každé části evidence.	Správná implementace systému opatrovnictví zaručí důvěryhodnost a celistvost evidenčních dat.
Metodický postup vyšetřování	
První fáze je fáze poznávací. Získáme informace o události, identifikuje data.	Po identifikování všech důležitých dat je nutné tyto data správným způsobem získat.
Třetí fází je extrahování dat a posléze jejich analýza.	Pečlivá dokumentace všech učiněných kroků je nezbytností.
Závěrečná zpráva je výsledkem vyšetřovacího procesu.	Závěrečná zpráva je předána klientovi.

5 PRAKTICKÉ METODY ČINNOSTI VYŠETŘOVATELE

Praktická analytická činnost zahrnuje metody forenzního vyšetřovatele, využívané jak přímo na místě činu pro získání potřebných dat, tak další praktické metody spojené s následnou analýzou těchto dat. Současně uvedeme nástroje využívané k provádění této činnosti.

Nejdříve je ovšem nutností se zmínit o tzv. blokování zápisu. Jsou to softwarové či hardwarové nástroje, které umožňují ochranu proti nechtěnému či chtěnému zápisu. Vzhledem k nákladům se mohou využít forenzní distribuce operačního systému Linux, kde nedochází k zápisu na zkoumaný harddisk ani při jeho připojení. Takový postup je obhajitelný z forenzního hlediska. Během praktické činnosti musí vyšetřovatel tyto nástroje využívat, jedině tak může totiž prokázat, že během jeho činnosti nebyla data upravena, že jsou původní. Zajistí tak důvěryhodnost svojí práci i důvěryhodnost dat, které získal.

5.1 Získání dat

Získávání dat je proces, kdy se forenzní vyšetřovatel snaží identifikovaná data kopírovat z původního datového média na svůj osobní externí harddisk. Základem této procedury je využití takových nástrojů, které v žádném případě nezmění původní získávaná data. Využití blokování zápisu nebo forenzní distribuce operačního systému Linux je nezbytností. Duplikovaná data musejí být naprosto přesnou kopií originálních dat.

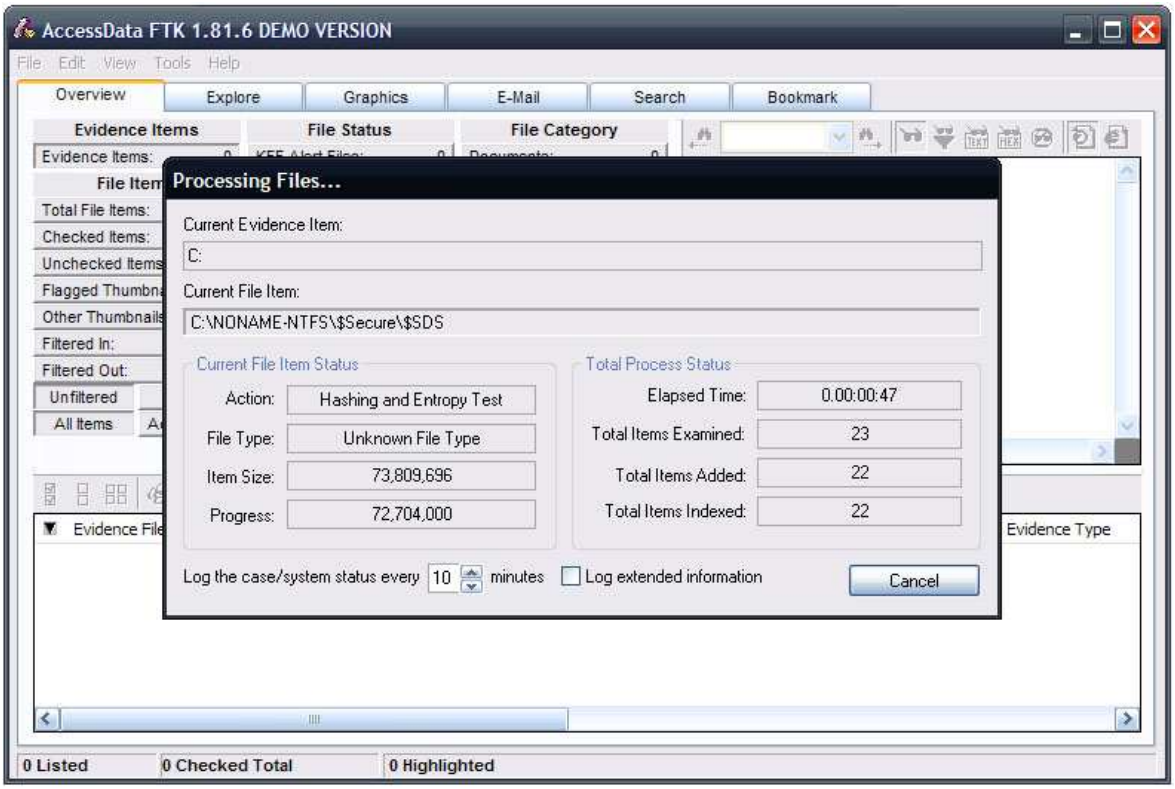
Klonování dat se zpravidla provádí vytvoření obrazu datového disku. Pokud vytvoříme bit-streamový obraz datového disku, máme jistotu, že jsou na tomto obrazu všechna data. Tedy všechna data z originálního datového media v nezměněné podobě, a to data jak na první pohled viditelná, tak dat skrytá.

Pokud provádíme duplikaci dat z harddisku osobního počítače, je nutné si uvědomit jednu zásadní věc. Pokud je výchozí počítač vypnutý, v žádném případě nesmíme duplikovat data tím, že počítač zapneme a poté data kopírujeme. I samotný bootovací proces může zničit některá z důležitých dat. proto je nutné vždy původní harddisk z počítače vyjmout a připojit na počítač vyšetřovatele.

FTK Imager, neboli *Forensic Tool Kit Imager*, je velmi kvalitní nástroj, který je schopen identifikovaná data nejenom získat, ale umožňuje i nejrůznější funkce pro analyzování těchto dat. Tento softwarový nástroj je velmi kvalitním nástrojem pro vyšetřovatele. jeho možnosti jsou velké. Má mnoho předností, z nichž můžeme zmínit i například interoperabilitu. To znamená, že tento nástroj dokáže pracovat i se sobory z jiných forenzních nástrojů. Pokud je např. nutná spolupráce s externí vyšetřovací laboratoří, která využívá jiné softwarové nástroje, *FTK Imager* dokáže tyto data bez problému zpracovat.

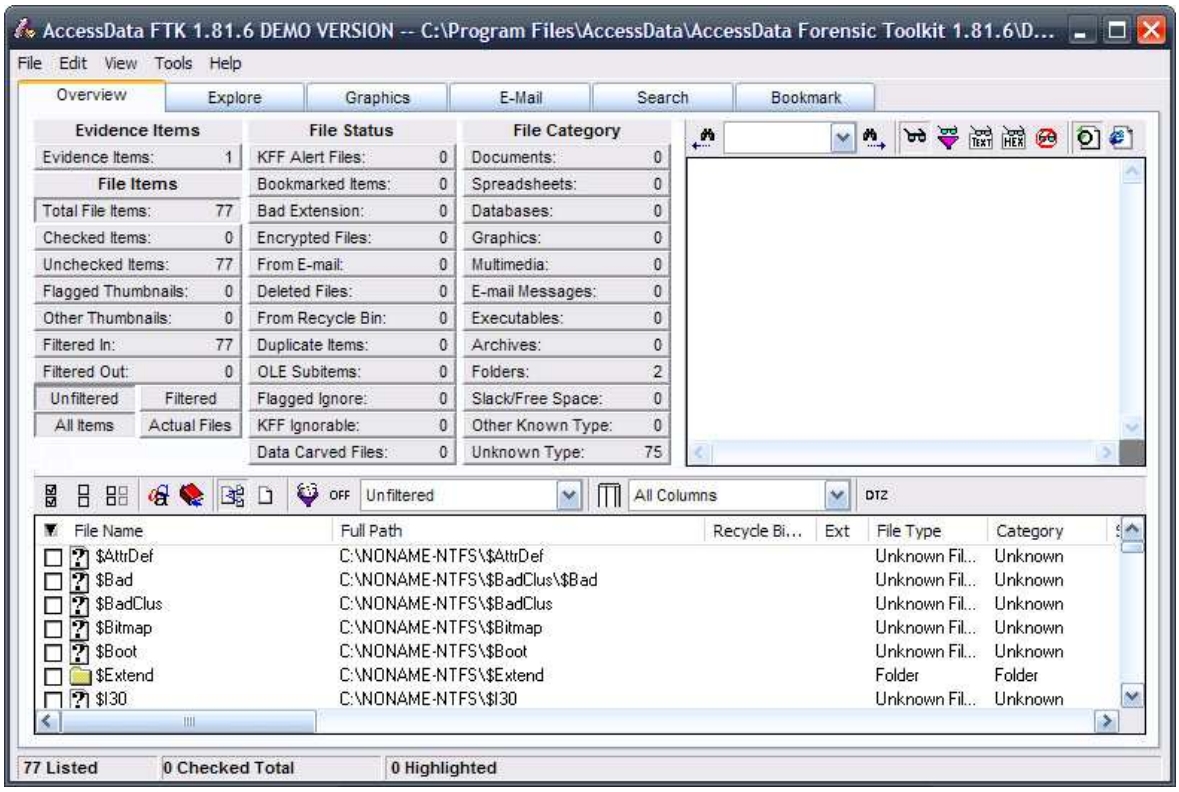
Základním krokem při práci v tomto programu je vytvoření případu. zde můžete zadat podrobné informace o všech skutečnostech souvisejících s případem. Komplexnost tohoto programu je enormní, což jde vidět hned po prvním spuštění. Tento program využívá databázi, do které lze ukládat nejrůznější informace ohledně celého případu. Od identifikace evidence, přes její sběr, až po jednotlivé analytické činnosti.

Po vytvoření případu následuje prohledávání připojených harddisků či jiných datových nosičů.



Obrázek 6: Identifikace dat na harddisku pomocí *FTK Imager*

Po prohledání a identifikaci všech dat na datovém nosiči nástroj automaticky rozdělí tato data do nejrůznějších kategorií. Je tak značně zjednodušen přístup k těmto datům. Dalším krokem bude většinou vytvoření obrazu disku tzv. bit po bitu s využitím MD5 algoritmu, jehož funkce byla vysvětlena již dříve.



Obrázek 7: Nalezená data členěná do kategorií v *FTK Imager*

Funkce nástroj *FTK Imager* ovšem u pouhé tvorby přesných kopií datových nosičů nekončí. Tento nástroj je komplexním nástrojem pro forenzního vyšetřovatele. *FTK Imager* dokáže soubory identifikovat, posléze duplikovat, ale je schopen i konkrétních analytických činností, které pomůžou vyšetřovateli v odhalení důležitých evidenčních dat. Je schopen například získat data, které jsou zakódovaná. Jeho největší předností je ovšem jeho databázová funkce. Díky ní má vyšetřovatel nepřeberné množství funkcí, které může využít pro identifikaci a popis jednotlivých evidenčních důkazů. takovýto komplexní materiál je pak naprosto ideálním podkladem pro případné soudní řízení.

5.2 Obnovení dat

Smazaná dat jsou taková data, která byla logicky smazána ze systému souborů, ale můžou stále zůstat fyzicky uložena na datovém mediu. Podstatnou věcí ovšem je, že data mohou být smazána nejrůznějšími způsoby. Pro znovuzískání smazaných dat můžeme využít nejrůznější nástroje. Tyto nástroje často disponují vícero funkcemi. Často jsou schopny obnovit nejen smazaná data, ale i data porušená nebo alespoň jejich část.

5.2.1 Způsoby mazání dat

Způsobů, jak smazat data může být hodně. Může být vykonáno jednoduchým přesunutí souboru do Koše, nebo stisknutím SHIFT + DELETE, ale způsobů je mnohem více.

- Mazání přes příkazový řádek operačního systému. Využitím příkazu DEL nebo ERASE.
- Přesunutí souboru. Pokud je soubor přesunut v rámci stejného oddílu na harddisku, jeho fyzické umístění v podstatě zůstane zachováno, pouze se změní tzv. pointer, čili ukazatel na soubor. Pokud se ovšem přesun provádí z jednoho harddisku na druhý, nebo z jednoho oddílu na druhý, je situace složitější. Nejdříve je vytvořena kopie souboru v cílovém oddílu. Poté se původní soubor smaže. Provádí se také úprava FAT tabulky, kdy se mění informace o obsazení místa v souborovém systému.
- Vyčištění disku. V této situaci operační systém maže data, která již nejsou potřebná a zabírají zbytečně místo na harddisku. Operační systém uživateli nabídne soubory, které mohou být bezpečně smazány. Ovšem některé z těchto souborů lze pomocí softwarových nástrojů obnovit.
- Mazání přes *Koš* v operačním systému nebo stisknutím SHIFT + DELETE. Pokud při mazání není funkce koše obejita, je možnost tyto data znovu získat.
- Některé dočasné soubory se po ukončení potřebné akce automaticky mažou. Častým příkladem jsou dočasné soubory, potřebné k instalaci software. po této instalaci se nepotřebná data smažou.

- Formátování datového media. Pokud formátujeme harddisk nebo jiné datové medium neznamená to, že jsou všechna data nenávratně ztracena. Především u rychlého formátování, kde je pouze definováno umístění souborů na mediu, ale tyto data nejsou smazána.
- U operačního systému Linux jsou pro mazání využity tzv. *rm commands*. Pokud jsou data tímto způsobem mazána, operační systém se již neptá na potvrzení mazání. data jsou pak prostě nadobro smazána.

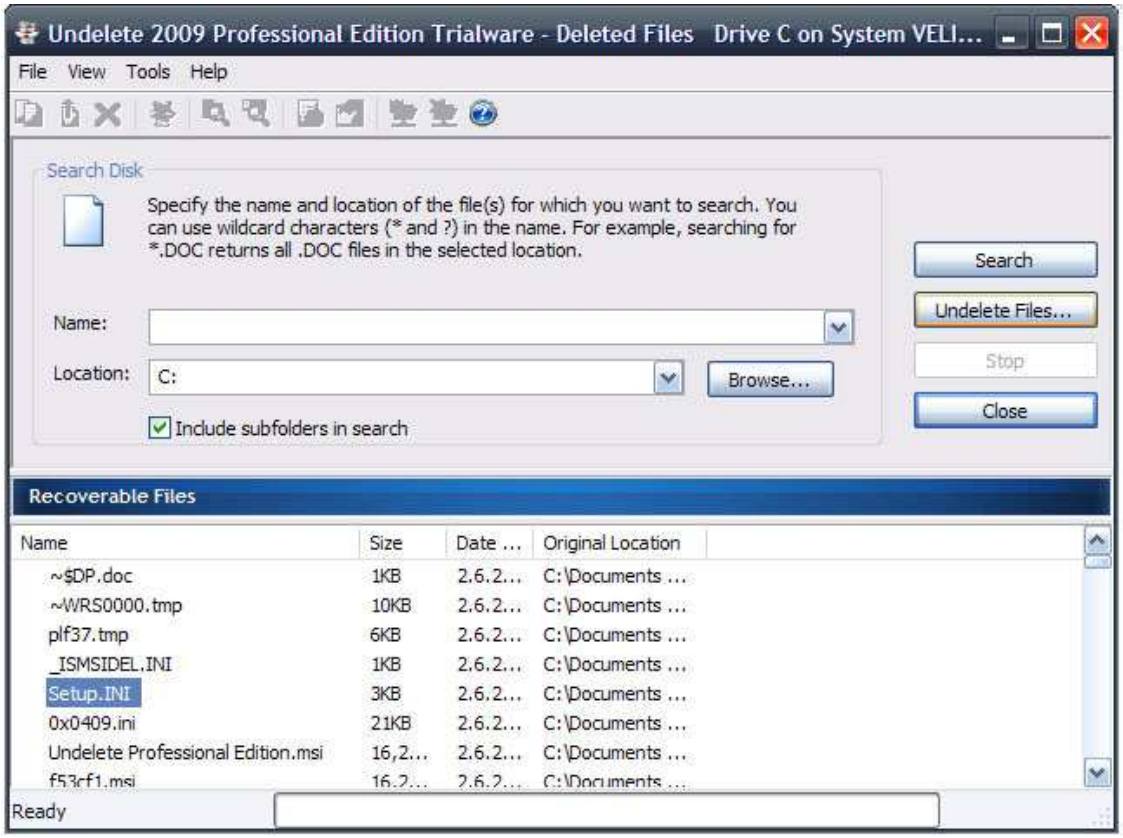
Existuje nepřeberné množství nástrojů, které slouží k získání smazaných dat, k obnovení porušených dat apod. Zaměříme se tedy na programy v závislosti na jejich konkrétním určení. Často jsou tyto nástroje určeny k obnovování konkrétních druhů dat, nebo jsou zaměřeny na získání dat ze specifického datového media. Zaměříme se tedy na nástroje pro obnovení logicky smazaných dat, nástroje pro obnovení dat z *Recycle Bin*, nástroje obnovování dat z CD a DVD, obnovení *MS Office* souborů, nástroje pro obnovení komprimovaných dat, nástroje pro obnovení obrázků a nástroje pro obnovení smazaných oddílů disku.

5.2.2 Obnova logicky smazaných dat

Jak bylo již řečeno dříve, data která jsou mazána často zůstávají fyzicky na disku. Je to dáno tím, že se mažou pouze logickou cestou, tedy upravují se pouze informace o těchto datech v systému souborů, ale fyzicky jsou stále přítomna. Při mazání standardní cestou jsou data uložena v souboru s označením *Recycle Bin*. Z něj se tyto data dají získat nazpět bez využití softwarového nástroje. Ovšem pokud při mazání použijeme příkaz SHIFT + DEL, obejdeme *Recycle Bin*. V takovéto situaci je pro obnovu dat nutné využít externí nástroj.

Undelete jedním ze základních nástrojů pro obnovu logicky smazaných dat je volně dostupný nástroj s názvem *Undelete*. Tento nástroj disponuje velmi jednoduchou obslužností. je schopen detekovat data, která byla smazána a poté je obnovit. Při manuálním obnovování dat, stačí zadat cestu k souboru, který má být obnoven a zadat *Start*

Undelete. Je to jednoduchý program disponující základními funkcemi. Je ovšem nejen díky své jednoduchosti účinným nástrojem pro obnovení smazaných dat.



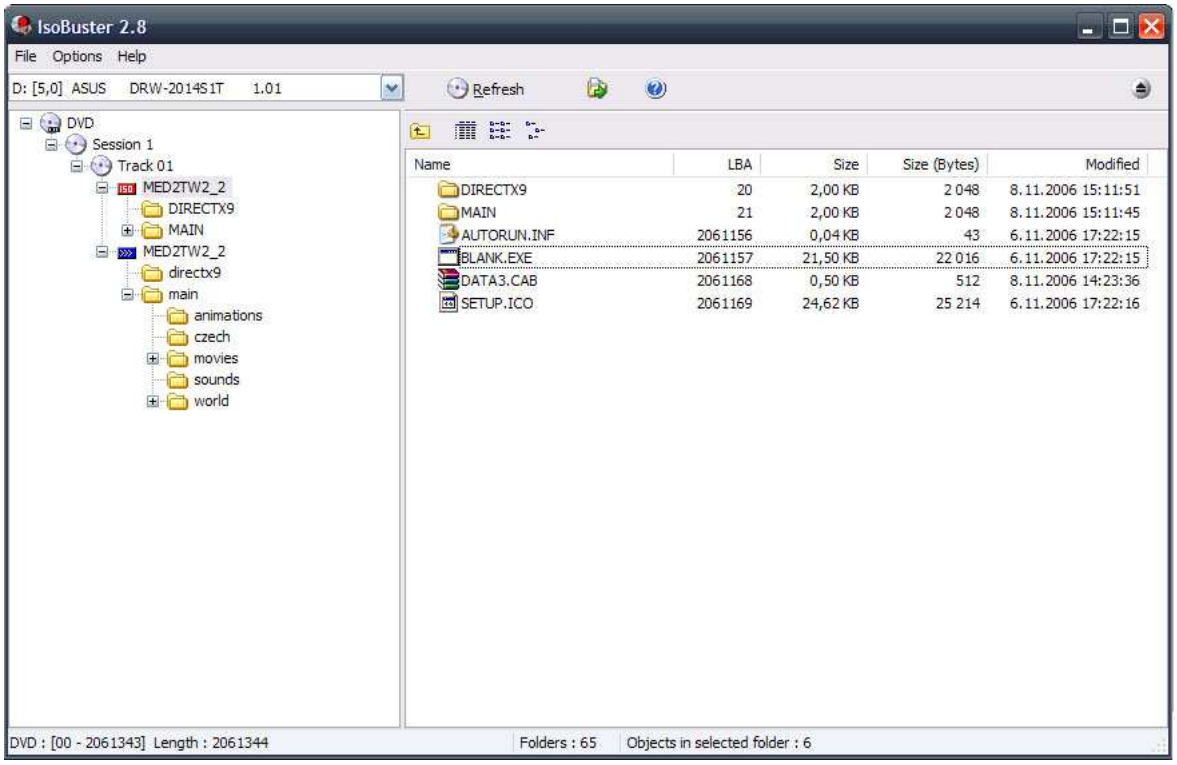
Obrázek 8: Obnova dat nástrojem *Undelete*

5.2.3 Obnova dat z Recycle Bin

Recycle bin je soubor, který si většina uživatelů Win OS představí spíše pod pojmem *Koš.* Tento soubor je umístěn ve složce s operačním systémem a dává uživateli druhou šanci pro získání svých dat, pokud změní svůj názor. Funkci tohoto nástroje mohou ovšem nahradit mnohem sofistikovanější aplikace, které přidávají k této základní funkci obnovy dat i funkce přídavné. Pro příklad můžeme uvést nástroj s názvem *Diskeeper Undelete*. tento nástroj nahradí funkci *Recycle Bin* svou vlastní. uživatel pak může mnohem jednodušeji přistupovat ke smazaným datům, která byla původně umístěna právě v *Recycle Bin* souboru.

5.2.4 Obnova dat z CD a DVD

Ne všechna data jsou uložena na pevných discích počítače. Existuje velké množství softwarových aplikací, jejichž cílem je obnovit smazaná nebo porušená data uložená na CD a DVD nosičích. Data uložená na těchto discích mohou být smazána, můžou být také porušena fyzickou deformací disku, data se mohou porušit během zápisu a podobně.



Obrázek 9: Obnova dat z DVD nástrojem *IsoBuster*

Nástroj s názvem *IsoBuster* je schopen provádět tyto obnovovací činnosti na nejrůznějších druzích nosičů. Je schopen obnovit data z běžných CD a DVD. je ale také schopen pracovat s *Blue-Ray* disky. je také schopen pracovat s audio a video formáty souborů. Tento program také pracuje se standardem ISO 9660. Což je standart týkající se způsobu uložení souborů na CD a DVD discích. Na těchto nosičích vznikne po uložení dat souborový systém právě podle tohoto standardu. Využití nástroje, který je tímto standardem podporován nám zaručí, že souborový systém na CD a DVD nosičích bude možné tímto nástrojem přečíst.

5.2.5 Obnova komprimovaných dat

Komprese dat slouží ke snížení velikosti dat pomocí komprimačního algoritmu. Často se ovšem stává, že především u větších objemů dat dojde k chybám a poškození částí komprimovaných souborů. Pro obnovení takto poničených dat slouží speciální nástroje.

Jeden z nástrojů, který lze využít k obnovení porušených komprimovaných dat se nazývá *Zip Repair*. tento softwarový program je schopen obnovovat velké objemy dat, řádově GB dat.

5.2.6 Obnova MS Office souborů

V zhledem k tomu, že nástroje *MS Office* jsou hojně využívány po celém světě, zaměříme se tedy i na obnovu těchto souborů. Obnovení těchto typů souborů připadá do úvahy v situaci, kdy jsou soubory poškozené. Může se tak stát z nejrůznějších důvodů, např. pokud před uložením textového souboru dojde k výpadku elektrického proudu. data se mohou poškodit a nelze je běžným způsobem získat zpět.

K tomuto účelu můžeme využít nástroje pro obnovu jako např. *OfficeFIX*. Tento nástroj je velice komplexní. Dokáže získat data nejenom z části souboru, který je nepoškozen. Dokáže také obnovit a opravit data ze souborové části, která byla poškozena. Pracuje se soubory *MS Word*, *MS Excel*, ale i *Outlook* a se všemi dalšími aplikacemi z řady *MS Office*.

5.2.7 Obnova obrazových dat

Obrazová informace je jedinečná. Pokud je zničena např. fotografická dokumentace, nebo jiný fotografický materiál, je to ztráta která je nenahraditelná. Obraz jako takový je totiž vždy jedinečný a nahradit jej za jiný nelze. Proto byly navrženy nástroje, které jsou schopny získat původní obrazová data.

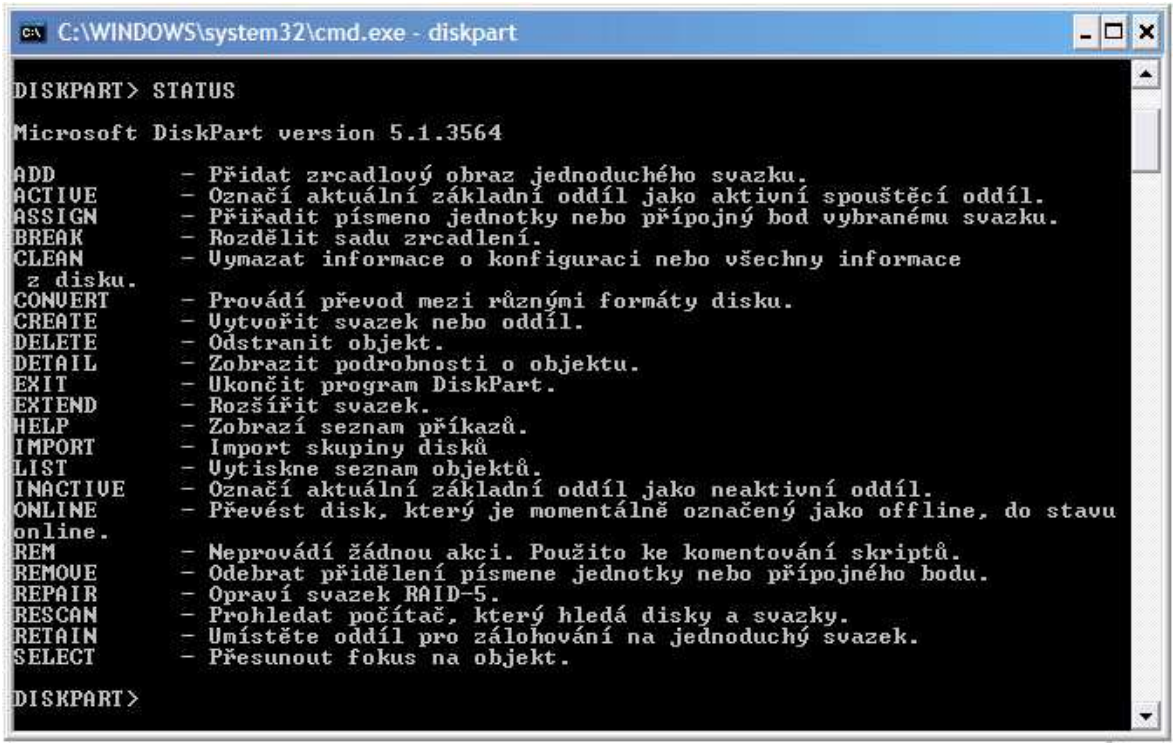
Jedním ze softwarových nástrojů pro tento účel je nástroj *eIMAGE Recovery.*Tento nástroj je schopen obrazová data nejenom obnovit v případě smazání, je ovšem také schopen obrazová data opravit v případě jejich poškození. Tento program je schopen získat smazaná obrazová data z široké škály datových nosičů. Od počítačového harddisku

počínaje, po paměťovou kartu fotoaparátu konče. Pracuje jak s obrazovými formáty, tak s video formáty.

Obrázek 10 Obnova obrazových dat nástrojem *eIMAGE Recovery*

5.2.8 Obnova oddílů disku

Oddílem disku se rozumí logické rozdělní harddisku na několik na první pohled samostatných celků. V operačním systému jsou poté tyto oddíly zobrazeny jako samostatné datové disky. Důvodem členění harddisku na několik samostatných oddílů je přehlednější organizace uložených dat. Pokud ovšem mluvíme o problematice oddělení harddisku na samostatné celky, nejedná se pouze o funkci vytvoření nového oddílu, či jeho smazání. Obecně lze s oddíly harddisku provádět nejrůznější věci, což práci vyšetřovatele značně ztěžuje.



Obrázek 11 Příkazový řádek pro oddíly harddisku

Pokud je oddíl disku smazán, je odstraněn zápis o oddílu v souborové tabulce oddílů. Takže na první pohled to vypadá, že byl celý oddíl z harddisku odstraněn. Je tomu tak, oddíl byl odstraněn, ovšem data v oddílu obsažená se stále na harddisku nacházejí. Jediné co zmizelo je zápis o tomto oddílu v souborové tabulce oddílů, která obsahuje informace o těchto oddílech. Data jsou tedy stále fyzicky přítomna na disku a pomocí speciálních nástrojů je lze získat, i když jsou v operačním systému neviditelná.

Mezi nástroje, které lze k tomuto účelu využít, můžeme uvést *DiskInternals Partition Recovery*, *GetDataBack*, nebo *Active@ Partition Recovery*.

5.3 Analýza dat

Analytických metod je nepřeberné množství. Jejich využití je vždy závislé na typu dat, které analyzujeme a na druhu informací, které se z těchto dat snažíme získat. Specializované vyšetřovací pracoviště by mělo disponovat odborníky, kteří se zaměřují na konkrétní analytické metody dat. Kybernetická trestná činnost je extrémně obsáhlou problematikou, proto není možné, že by jeden specializovaný vyšetřovatel byl schopen kvalitně řešit všechny druhy případů. V následujících odstavcích vymezíme základní kategorie analýz. Právě pro každou z těchto kategorií by měl být v rámci specializovaného vyšetřovacího pracoviště stanoven odborný forenzní znalec, který se bude zabývat pouze případy, spadající pod jeho oblast zájmu. Zajistíme tak vyšší míru odbornosti.

5.3.1 Operační systémy

K správnému provádění analýz operačních systémů je ideální pochopit jejich přednosti a slabiny. V dnešní době má majoritní zastoupení Win OS, dále v mnohem menší míře LINUX a Mac OS. Je tak jasné, že většina kybernetické trestné činnosti je páchána na nejvíce rozšířeném operačním systému, tedy na Win OS.

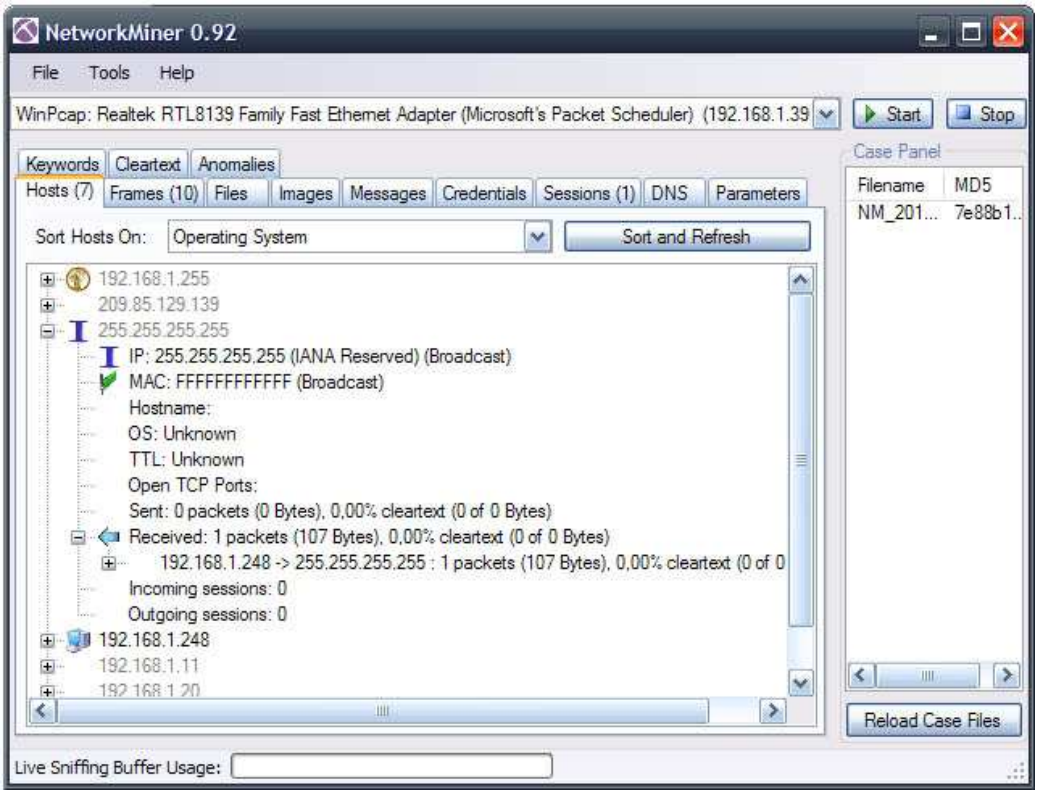
Pokud mluvíme o analyzování operačních systémů, je nutné si uvědomit, že se jedná snad o nejsložitější druh analytické činnosti. Vyšetřovací proces je v tomto případě velmi složitý a závisí vždy na konkrétním druhu útoku. Jako základní lokace, kde je předpoklad výskytu důležitých evidenčních dat, jsou místa s dočasnými daty jako Win host, dále Win souborový zásobník, Win registry a také systémové zálohy. Největším problémem u tohoto typu vyšetřování jsou dočasná data. Běžným vyšetřovacím postupem je vytvoření duplikovaného obrazu disku a následné zkoumání. To ovšem při zkoumání dočasných dat není možné. Je nutné aplikovat analytické metody v reálném čase.

Pro kvalitní a úplné analytické zkoumání je tedy nutné využít takové nástroje, které jsou schopny analýz následných i analýz v reálném čase.Jedním z takových nástrojů může být tzv. *Helix*. Tento nástroj dokáže mimo standardní tvorbu obrazů disku mnoho dalšího. Dokáže identifikovat a analyzovat dočasná data, která by po vypnutí operačního systému byla ztracena. Je schopen identifikovat nejenom povahu incidentu, ale také dokáže zjistit jak a kdy se tento incident přihodil. Je to dáno jeho obrovskou komplexností. *Helix* totiž

není pouze jeden nástroj. Ve skutečnosti je to směsice desítek nástrojů, určených k nejrůznějším analytickým činnostem.

5.3.2 Síťový provoz

Vyšetřování síťového provozu by se dalo definovat jako sniffing, nahrávání a analyzování síťového provozu a jiných událostí. Vyšetřování sítí se provádí za účelem objevení zdroje bezpečnostních incidentů, útoků a dalších možných problémů. Klíčovou roli u této problematiky hrají routery. Přes ně se útočník, hacker, snaží dostat. Základem znalosti forenzního specialisty je tedy znalost postupů hackera, nutných k prolomení ochrany routerů. Pro vyšetřování routeru můžeme využít jako základní pomůcku běžné příkazové zkratky routeru, které nám mohou dobře posloužit k analýze routeru. Příkazy které mohou dopomoci k získání základních informací a sledování činnosti hackera jsou následující: *show access list*, *show clock*, *show ip route*, *show startup configuration*, *show users*, *show wersion*.

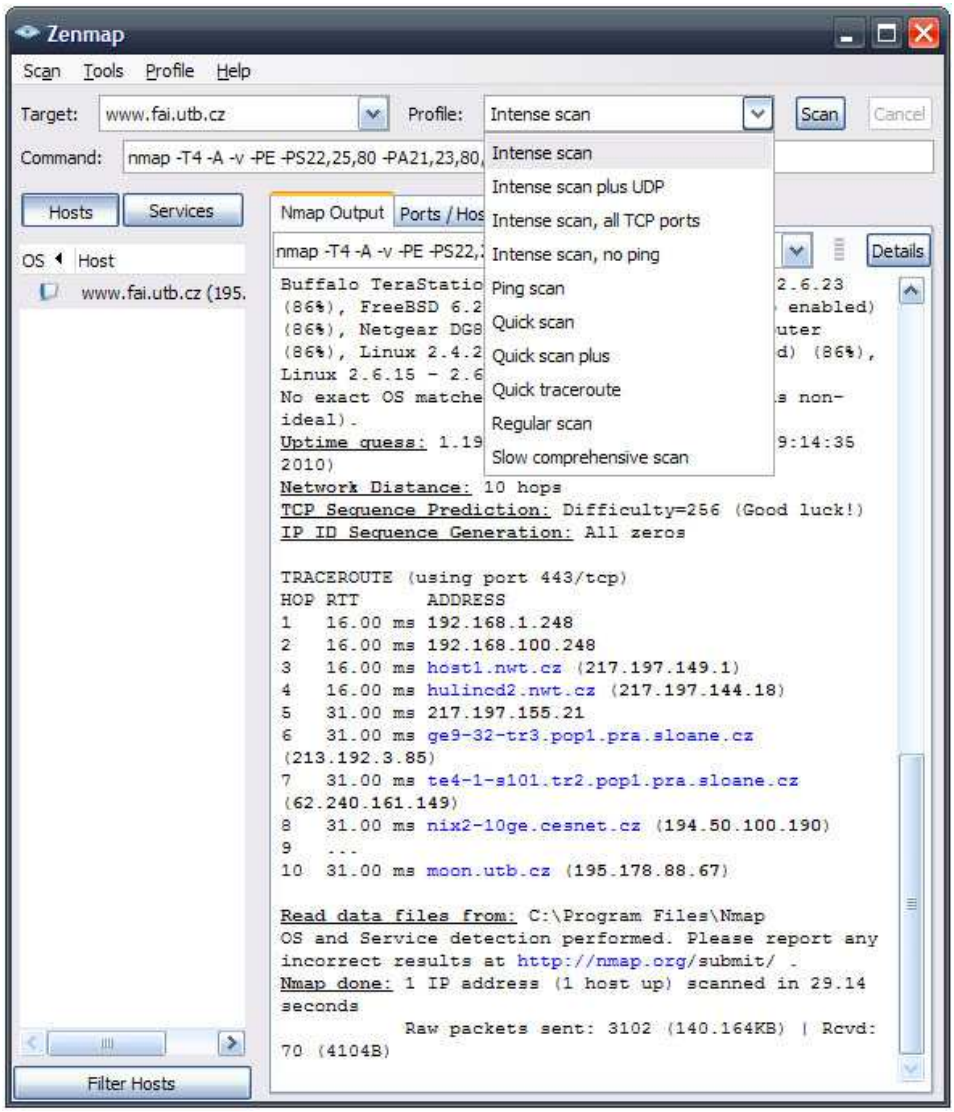


Obrázek 12: Nástroj pro síťovou forenzní analýzu *Network Miner*

5.3.3 Bezdrátové útoky

Bezdrátový přístupový bod vytvoří z tradiční sítové struktury strukturu bezdrátovou, která jednoduše umožní uživatelů posílat data vzduchem. Na první pohled by se dalo říci, že bezdrátové sítě jsou jasným krokem dopředu. Ve skutečnosti je situace složitější. Bezdrátové sítě jistě disponují mnoha vylepšeními oproti běžným sítím. Mají ovšem také nedostatky, které je nutné brát do úvahy.

Za klady bezdrátových sítí se dá jistě považovat především zjednodušení přístupu k síti, snížení nákladů na realizaci díky absenci fyzických kabelů a zvýšená produktivita práce. Naopak zápory bezdrátových sítí jsou bezpečnost, složitost, spolehlivost a výkon sítě.

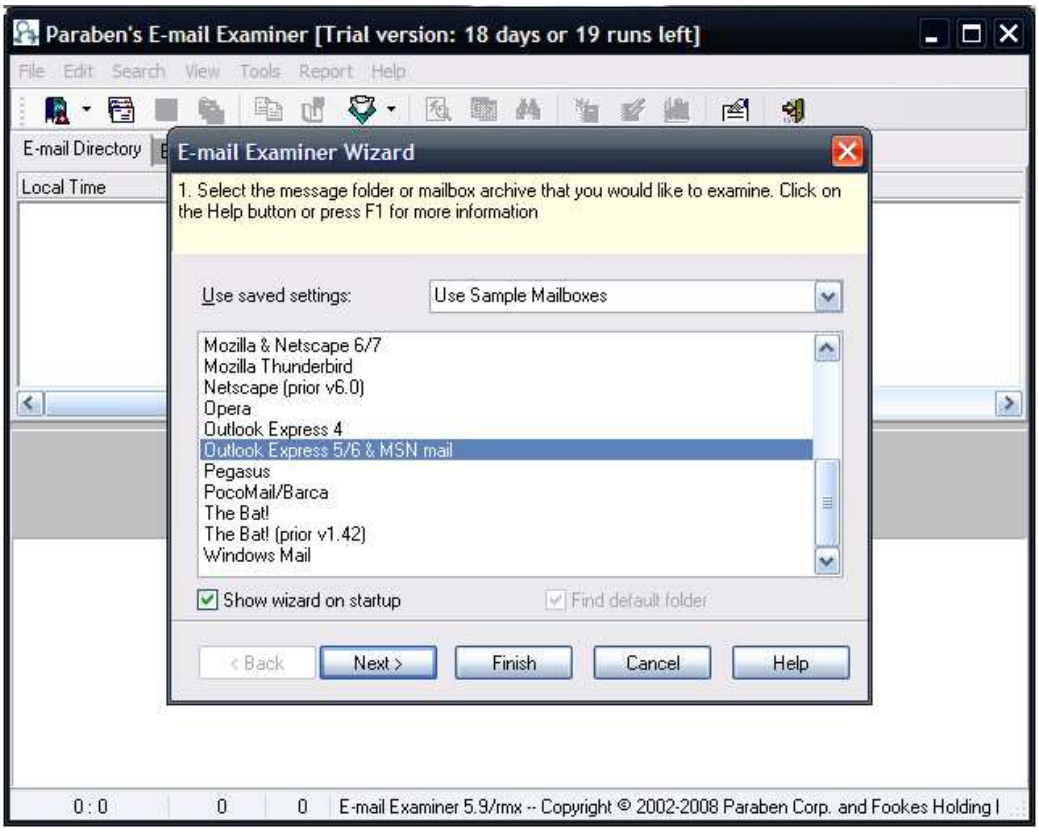


Obrázek 13: Nástroj pro mapování sítí *Nmap*

Jak už bylo zmíněno, to že může uživatel bez problémů využívat bezdrátovou síť je dán přístupovým bodem. Ten umožňuje připojení k této bezdrátové síti. Proto právě přístupový bod by měl být hlavním prvkem zájmu vyšetřovatele. Pro skenování bezdrátového přístupového bodu slouží nejrůznější nástroje. Jedním z nejpopulárnějších nástrojů je *Nmap*. Tento nástroj je ideálním nástrojem pro mapování sítí. Disponuje mnoha módy, které dokáží usnadnit práci.

5.3.4 Elektronická pošta

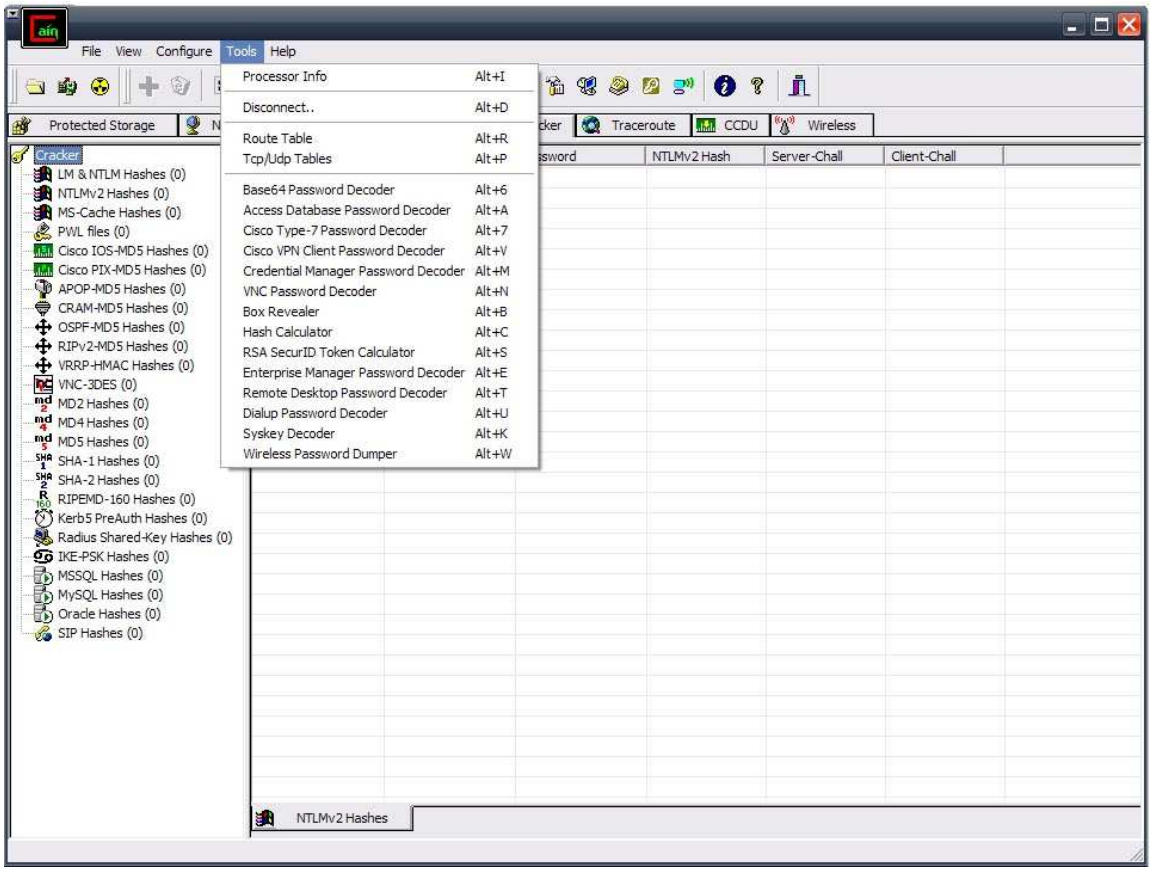
Pokud mluvíme o analyzování emailových zpráv, mluvíme o jejich získání a následném zpracovávání. Emailová komunikace může poskytnout důležité informace, které mohou nakonec být tím hlavním důkazním materiálem, které prokáže trestný čin. Respektive dokáže usvědčit pachatele. Jedním z využitelných programů pro tento účel je nástroj *Paraben's E-mail Examiner*. Tento program je navržen pro zpracování a analýzu nejrůznějších druhů emailových archivů. Po zpracování archivu lze využít nejrůznějších forenzních analýz.



Obrázek 14: Výběr emailových archivů v *Paraben's E-mail Examiner*

5.3.5 Zašifrovaná data

Prolomení bezpečnostní ochrany v podobě kódu je velmi důležité i pro forenzního vyšetřovatele. Zde se velmi prolíná činnost pachatele trestného činu s činností samotného vyšetřovatele. K prolomení ochrany je využíváno nejrůznějších nástrojů, jako *Cain and Abel*, *LCP*, *Ophcrack*, *Rock XP* a jiné. Jsou to aplikace, jejichž obecným smyslem je obnova hesel.



Obrázek 15: Nástroj pro obnovu hesel *Cain and Abel*

ZÁVĚR

Cílem této práce bylo vymezit problematiku týkající se vývoje a činnosti specializovaného pracoviště pro odhalovaní a vyšetřování kybernetické trestné činnosti. Vývoj takového pracoviště je odezvou na stávající situaci v oblasti informačních a telekomunikačních technologií. Vzhledem k neustálému vývoji těchto technologií vznikají i nové hrozby s touto problematikou spojené. Cílem práce bylo podat komplexní informace o způsobu vývoje a činnosti vyšetřovacího pracoviště se zaměřením na privátní sféru.

Vývojem vyšetřovacího pracoviště se rozumí období od započetí plánování výstavby až po období odstartování vlastní činnosti pracoviště. Vymezení požadavků nutných pro výstavbu pracoviště a následnou činnost je nezbytnou součástí plánovací fáze. Požadavky na vývoj je ovšem nutné chápat nejenom v rovině finanční. Tento dokument si dal za cíl mimo jiné upozornit na všechna úskalí, která jsou s touto částí vývoje pracoviště spojena. Plánovací fáze je podmíněna konkrétní budoucí činností vyšetřovacího pracoviště. Z úvodní kapitoly jasně vyplývá, že problematika kybernetické trestné činnosti je značně obsáhlá. Proto je před započetím samotné výstavby nezbytně nutné znát budoucí konkrétní služby, které bude vyšetřovací objekt poskytovat. Důležité bylo upozornit na to, že tyto vyšetřovací pracoviště se mohou v závislosti na druhu poskytovaných služeb značně lišit. Poznatkem z plánovací fáze vývoje vyšetřovacího pracoviště je tedy fakt, že způsob vývoje vyšetřovacího pracoviště je extrémně závislé na konkrétním vymezení budoucích poskytovaných služeb.

V rámci pracoviště je nakládáno s citlivými daty. Proto bylo nutné stanovit i procedury, které zajistí správné nakládání s těmito daty. Všechna technická a metodická opatření byla navržena s cílem zajistit důvěryhodnost a celistvost informací, se kterými přijde vyšetřovací tým a další zaměstnanci vyšetřovacího objektu do styku. Z vypracovaného materiálu je zřejmé, že ochrana dat by měla být na prvním místě zájmu. Jedině tak budou mít tyto informace patřičnou hodnotu pro klienta. Za tímto účelem bylo v dokumentu definováno několik konkrétních způsobů, jak s informacemi nakládat, aby nemohlo dojít ke ztrátě důvěryhodnosti a celistvosti získaných informací. Je zřejmé, že jedině zajištěním správných procedurálních postupů je možné zajistit správné nakládání s evidenčními daty. Pravidelný audit kvality těchto procedur je nezbytností.

Práce si také kladla za cíl uvést v teoretické rovině metodické postupy vyšetřovacího týmu expertů. Smyslem stanovení obecné posloupnosti událostí bylo v podstatě definovat základní sled událostí a postup činnosti vyšetřovacího týmu. Vyšetřovací činnost je ovšem chápána v teoretické a praktické rovině. V praktické rovině byl kladen důraz na výběr vhodných nástrojů pro vyšetřování. Ten je stěžejním faktorem pro úspěšné vyšetřování kybernetické trestné činnosti.

Světový vývoj v oblasti informačních a komunikačních technologií jasně ukazuje, jak jednoduché je získat různé druhy informací. Získání informací může posloužit k páchání trestné činnosti. Stejně tak ale slouží získávání informací k odhalení této trestné činnosti a k dopadení pachatele. Specializované vyšetřovací centrum pro odhalování kybernetické trestné činnosti je nástrojem pro získávání těchto evidenčních informací. Důvodem tvorby tohoto materiálu byl fakt, že v českém prostředí je velmi obtížné najít publikace zabývající se vývojem podobného specializovaného pracoviště. Zajímavým zjištěním během tvorby tohoto materiálu je to, že činnost specializovaného vyšetřovacího centra nemusí být zaměřena pouze na odhalování a vyšetřování trestné činnosti. Obecným posláním tohoto specializovaného pracoviště je získávání informací z digitálních dat. Nezáleží přímo na tom k čemu tyto informace slouží. Z tohoto důvodu má specializované vyšetřovací pracoviště velkou šanci v komerční sféře uspět.

ZÁVĚR V ANGLIČTINĚ

Main objective of this work was delimitation of problems connected with development and activities of specialized workplace for cyber crime investigations. The development of this kind of workplace is answer to today's situation in information and telecommunication technology sphere. New kinds of threats are rising because of the continuous technology development. One of the objectives is to give complete informations about way of development and activities of investigative workplace in private sphere of business.

Development of investigative workplace means activities from stage of planning start of the build up to stage of start up of workplace activities. It is very important to define requirements for workplace build up and subsequent workplace activity during planning stage. But requirements for development are understand not only in financial way. The objective of this document is among others to call attention to every difficulties of this kind od development. Planning stage depends on concrete future activities of forensic workplace. From the first chapter clearly result, that cyber crime problems is greatly extensive. Before initiation of build up process we need to know expected services provided by forensic object. It was very important to call attention to difference between individual forensic workplaces based on different kinds of provided services. The way of forensic workplace development is extremly subordinated on concrete upcoming services.

In forensic workplace are delicate data. Because of that fact it is very important to define procedures, which are able to ensure credibility and integrity of informations maintained by forensic team and other personnel of forensic workplace. From document is clearly evident, that security of data is on the first place of our interest. It is only way to achieve propriate value for our client. This is the reason why we have defined several concrete methods for treating with informations in order to achieve credibility and integrity of collected informations. It is evident, that only with reinsurance proper procedure processes si possible to ensure proper evidence data treating. Periodic quality audit of procedures is necessary.

Another objective of this work was delimitate metodical procedures of investigative team of forensic experts in theoretical and methodical way. Definition of basic chain of events and activity processes of forensic team was purpose of general chain of custody assesment. Investigative activities are comprehend in theoretical and practical manner. In practical

manner was accentuated selection of suitable tools for forensic investigations. That is a pivotal factor for successful investigations of cyber crime.

World's evolution in information and telecommunication technology sphere is clearly showing us how easy is getting different kinds of informations. Acquiring of informations is usefull for conducting crime. But it is also very important for acquiring informations for detecting this crimes and for capturing perpetrator. Specialized investigative centre for cyber crime investigations is the tool for acquiring this kind of evidence informations. The reason for craiting this document was fact, that in czech environment is very difficult to find publications about development of similar specialized workplace. A interesting finding during the document creatinon was fact, that activities of specialized investigative centre may not be focused only on detecting and investigating crime. It doesn‘t matter for what purpose are informations meant. This is the reason why have specialized investigative workplace purpose to success in commercial sphere.

SEZNAM POUŽITÉ LITERATURY

[1] JIROVSKÝ, Václav. HNÍK, Václav. KRULÍK, Oldřich. *Základní definice, vztahující se k tématu kybernetických hrozeb.* [online]. 2006. s. 1-2. [cit. 2010-05-15]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf >.

[2] JAŠEK, Roman. *Informační a datová bezpečnost*. UTB Zlín, 2006. ISBN 80-7318-456-7. s. 7-10. [cit. 2010-05-15].

[3] JIROVSKÝ, Václav. HNÍK, Václav. KRULÍK, Oldřich. Kybernetické hrozby: Výzva pro moderní společnost . *Přítomnost a budoucnost krizového řízení.* [online]. T-Soft, 2006. s. 10-11. [cit. 2010-05-15]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf>.

[4] REYES, Anthony. WILES, Jack. *The Best Damn Cybercrime and Forensics Book Period*. Elsevier, Inc., 2007. ISBN 13: 978-1-59749-228-7. s. 699. [cit. 2010-05-15].

[5] STRAUS, Jiří. *Kriminalistická metodika*. Plzeň : Aleš Čeněk s.r.o., 2006. ISBN 80-86898-66-0. s. 271-286.

[6] MUSIL, Stanislav. *Počítačová kriminalita: nástin problematiky, kompendium názorů specialistů*. Praha : Institut pro kriminologii a sociální prevenci, 2000. ISBN 80-86008-80-0. s. 301.

[7] Ministerstvo vnitra ČR. *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení.* [online]. 2006. s. 52. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/dokument/2006/informacni.pdf>.

[8] HNÍK, Václav. KRULÍK, Oldřich. *Zahraniční inspirace související s tématem kybernetických hrozeb.* [online]. 2007. s. 25. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zahranicni_inspirace.pdf>.

[9] *Forenzní zkoumání digitálních důkazů.* [online]. Risk Analysis Consultants, s.r.o., 2005. s. 48. Dostupný z WWW: < http://www.qualys.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328 >.

[10] RENO, Janet. FISHER, Raymond. ROBINSON, Laurie. BRENNAN, Noel. TRAVIS, Jeremy. *Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving.* [online]. U. S. Department of Justice, 1998. s. 71. Dostupný z WWW: <http://www.ncjrs.gov/pdffiles/168106.pdf>.

[11] SPIVEY, Mark. *Practical hacking techniques and countermeasures*. Auerbach Publications, 2007. ISBN 0-8493-7057-4. s. 738.

[12] KRAUSE, Micki. TIPTON, Harold. *Handbook of Information Security Management.* [online]. Auerbach Publications. Dostupný z WWW: <http://www.cccure.org/Documents/HISM/ewtoc.html>.

[13] PALMER, Gary. *A Road Map for Digital Forensic Research.* [online]. MITRE Corporation, 2001. Dostupný z WWW: <http://www.dfrws.org/2001/dfrws-rm-final.pdf>.

[14] *Computer Forensics Tool Testing (CFTT) Project.* Dostupný z WWW: <http://www.cftt.nist.gov/>.

[15] *Technology and Tools – National Institute of Justice.* Dostupný z WWW: <http://www.ojp.usdoj.gov/nij/topics/technology/welcome.htm>.

[16] *International Journal of Digital Evidence (IJDE).* Dostupný z WWW: <http://www.utica.edu/academic/institutes/ecii/ijde/>.

[17] *International Organization for Standardization (ISO).* Dostupný z WWW: <http://www.iso.org/iso/home.html>.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SEZNAM SW NÁSTROJŮ

- **Získání dat:**

FTK Imager	www.accessdata.com
DriveSpy	www.digitalintelligence.com
SafeBack	www.forensics-intl.com
Mount Image Pro	www.getdata.com
DriveLook	www.runtime.org/drivelook.htm
DiskExplorer	www.runtime.org/diskexpl.htm
SCSIPAK	www.vogon.co.uk/
SnapBack DatArrest	www.datarrest.com
R-Drive Image	www.drive-image.com
QuickCopy	www.shaffstall.com/
Save-N-Sync	www.savensync.com

- **Obnova logicky smazaných dat:**

Undelete	www.diskeeper.com/defrag.aspx
Active@ UNDELETE	www.active-undelete.com
Active@ UNERASER	www.uneraser.com
R-Undelete	www.r-undelete.com
WinUndelete	www.winundelete.com
Easy-Undelete	www.easy-undelete.com
Restoration	www.snapfiles.com
Mycroft V3	www.dibsusa.com
Recover My Files	www.getdata.com
eData Unerase	www.octanesoft.com
File Recover	www.pctools.com/filerecover
VirtualLab	www.binarybiz.com
Recover4all Professional	www.recover4all.com

File Scavenger	www.quetek.com
Badcopy Pro	www.jufsoft.com/badcopy
Zero Assumption Recovery	www.z-a-recovery.com
O&O Unerase	www.oo-software.com
Filesaver	www.file-saver.com
Restorer 2000	www.restorer2000.com
R-linux	www.data-recovery-software.net
PC ParaChute	www.unitrends.com
Stellar Phoenix	www.stellarinfo.com
Search and Recover	www.iolo.com
DiskInternals Uneraser	www.diskinternals.com
NTFS Recovery	www.diskinternals.com
SUPERFileRecover	www.superfilerecover.com

- **Obnova dat z Recycle Bin:**

Diskeeper Undelete	www.undelete.com
Fundelete	www.fundelete.en.softonic.com

- **Obnova dat z CD a DVD:**

CDRoller	www.cdroller.com
IsoBuster	www.isobuster.com
CD Data Rescue	www.naltech.com
InDisk Recovery	www.octanesoft.com

- **Obnova komprimovaných dat:**

Zip Repair	www.getdata.com
Data Recovery Wizard	www.easeus.com
Zip File Recovery	www.recoverdatasoftware.com

- **Obnova MS Office souborů:**

OfficeFIX	www.cimaware.com
Repair My Excel	www.repairmyexcel.com
Repair My Word	www.repairmyword.com

- **Obnova obrazových dat:**

eIMAGE Recovery	www.octanesoft.com
ImageRecall	www.imagerecall.com
DiskInternals Flash Recovery	www.diskinternals.com
Canon RAW File Recovery SW	www.getdata.com
RecoverPlus Pro	www.arcksoft.com
PC Inspector Smart Recovery	www.pcinspector.de

- **Obnova oddílů disku:**

Active@ Partition Recovery	www.partition-recovery.com
Active@ Disk Image	www.disk-image.net
DiskInternals Partition Recovery	www.diskinternals.com
GetDataBack	www.runtime.org
NTFS Deleted Partition Recovery	www.techddi.com
Acronis Recovery Expert	www.acronis.com
Scaven	www.pjwalczak.com
Recover It All!	www.dtidata.com
Partition Table Doctor	www.ptdd.com

- **Analýza operačních systémů:**

FTK Imager	www.accessdata.com
Helix3 Pro	www.e-fense.com
PsTools Suite	www.technet.microsoft.com/en-us/sysinternals/bb896649.aspx
Process Explorer	www.technet.microsoft.com/en-us/sysinternals/bb896653.aspx
PC On/Off Time	www.neuber.com/free/pctime/index.html
WinAudit	www.pxserver.com/WinAudit.htm
ReSysInfo	www. resysinfo.updatestar.com
Rootkit Revealer	www.technet.microsoft.com/en-us/sysinternals/bb897445.aspx
SecReport	http://www.smartx.com/?CategoryID=164&ArticleID=84&sng=1
PC Inspector File Recovery	www.pcinspector.de
MEMDump	www.tssc.de/products/tools/memdump
Galleta	http://www.foundstone.com/us/resources/proddesc/galleta.htm

- **Analýza síťového a bezdrátového provozu:**

Kismet	www.kismetwireless.net
NeSA	www.cyberforensics.in
TCPdump	www.tcpdump.org
Windump	www.winpcap.org/windump
NetworkMiner	www.networkminer.sourceforge.net
Xplico	www.xplico.org
E-Detective	www.edecision4u.com
Wireless-Detective	www.edecision4u.com
NetDetector	http://www.niksun.com/product.php?id=4
Netcat	www.netcat.sourceforge.net
Nmap	www.nmap.org

- **Analýza elektronické pošty:**

Paraben’s E-mail Examiner	www.paraben-forensics.com
LoPe	www.emailforensics.com
Email Detective	www.hotpepperinc.com/emd

- **Analýza zašifrovaných dat:**

Cain and Abel	www.oxid.it/cain.html
LCP	www.lcpsoft.com
Ophcrack	www.ophcrack.org
Brutus	www.hoobie.net/brutus
John the Ripper	www.openwall.com/john
Rock XP	www.korben.info/rockxp
THC Hydra	www. freeworld.thc.org/thc-hydra
Aircrack	www.aircrack-ng.org
L0phtcrack	www.l0phtcrack.com