Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Digitální stopy a informační kriminalita

Bc. Vladan ČERNÍN

! ! !

Místo této strany vložíte zadání diplomové práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Digitální stopy a informační kriminalita" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. dubna 2009 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi. Dále bych rád kolegům v zaměstnání za věcné připomínky a rodině za podporu při mém studiu.

Digitální stopy a informační kriminalita

Digital evidence and informatic crime

Souhrn

Tato diplomová práce se zabývá uceleným popisem problematiky informační kriminality, jejími obecnými druhy a možnostech boje proti ní. Přibližuje problémy, které vyvstávají při detekci této nezákonné činnosti, a navrhuje některá opatření vedoucí ke zvýšení informační bezpečnosti. Jsou popsána specifika digitálních stop a možnosti detekce digitálních stop v souvislosti s trestním řízením. Pozornost byla věnována technickým a finančním aspektům vyhotovování duplikátů pevných disků.

Summary

The diploma work has been aimed at problems of informatics crime in all general aspects and possibilities its detection. It has been shown problems rising in the course of this unlawful activity and suggests of security measures. It has been mentioned of specification of digital evidence and possibilities of detection of digital evidence in connection with criminal procedure. Individual part presents technical and cost comparison of all aspects at creation of duplicate of hard disks.

Klíčová slova: Informační kriminalita, digitální stopa, duplikát digitální stopy, počítačová kriminalita, bezpečnost IT.

Keywords: Informatic Crime, Digital Evidence, Duplicate Digital Evidence, Cyber Crime, IT security

1. Úvod

Vývoj lidské společnosti v průběhu času přinesl mnoho prvků, které jednotlivcům slouží k usnadnění a ke zkvalitnění jejich životů ve všech oblastech. Rozmach technické oblasti přinesl lidstvu obrovský potenciál rozvoje, který vedl k rozsáhlému využívání nejen toho, co nám nabízí naše planeta v podobě surovin, ale také k rozsáhlému využití zkušeností lidstva nasbíraných v průběhu věků. Tyto zkušenosti a informace se stávaly postupem času stále důležitějšími a pronikaly do všech aspektů života. Člověk se naučil získané zkušenosti, moderní technologie a vědecké výzkumy aplikovat do praxe a tím vytvářet technické vymoženosti, které slouží k jeho potřebám. Jedním z nejmladších technických výdobytků lidstva jsou technická zařízení obecně nazývané „POČÍTAČ“. Pod tímto pojmem si většina lidí představí stolní stanici nebo notebook. Jiní lidé si představí počítačové sítě, elektronickou poštu nebo třeba počítačové hry. Jsou ale i lidé nebo skupiny lidí, kteří si s vyslovením tohoto pojmu představí zisk nebo způsobení nějaké škody. Tito lidé jsou pachatelé informační kriminality.

Informační kriminalita je negativní jev, který doprovází nejen počítačové a informační technologie. Tento celosvětový fenomén je všude tam, kde se nachází moderní technologie obecně a vzhledem ke „zmenšování planety“ z důvodu rozvoje informačních systémů a telekomunikačních technologií zažívá v dnešní době svůj boom.

2. Cíl práce a metodika

Cílem této diplomové s názvem „Digitální stopy a informační kriminalita“ bude snaha přiblížit si pojem informační kriminalita, definovat její strukturu a popsat změny v jejím dosavadním vývoji. Práce umožní uvědomit si fakt, že informační kriminalita má svá specifika, mezi něž patří její minulost a rozvoj. Představíme si nejen pachatele informační kriminality a jejich motivaci, ale vysvětlíme si také základní pojmy a termíny spojené s daným tématem.

Práce se také zabývá digitálními stopami, které nám pomáhají informační kriminalitu odhalovat a bojovat proti ní. Popíšeme si, co to vlastně digitální stopy jsou a také problematiku jejich zajišťování.

V praktické části budou provedeny a porovnány dva odlišné způsoby vyhotovování duplikátů digitálních stop. Důraz bude kladen nejen na metodickou stránku problému, ale hodnocena budou i ekonomická hlediska.

Při zpracovávání diplomové práce je použito informací z různých zdrojů. Jedná se zejména o odborné publikace z dané oblasti, internet, ale také aktuální poznatky z praxe týkající se dané problematiky.

3. Informační kriminalita

3.1. Obecné pojetí

Informační kriminalita je jedním z negativních jevů, které rozvoj informačních, komunikačních a počítačových technologií přináší. Její vývoj je stejně rychlý jako vědeckotechnologický pokrok a je s ním velmi těsně spjatý. Při svém zdokonalování a vývoji dokáže tento druh kriminality velmi pružně reagovat na všechny možnosti, které mu tyto technologie umožňují.

K podrobnější specifikaci jednotlivých forem informační kriminality byly postupem času zaváděny i jejich odlišující pojmy. Státy Evropské unie informační

kriminalitu jako celek definují jako nemorální a neoprávněně jednání, zahrnující zneužití údajů získaných prostřednictvím informačních a komunikačních technologií. Nejčastějšími základními pojmy používanými v souvislosti s informační kriminalitou jsou pak počítačová kriminalita, informační kriminalita a informatická kriminalita.

Informační kriminalitou označovanou jako **informatic crime** přitom obvykle rozumíme takové protiprávní jednání, při kterém jsou zneužity informace bez ohledu na to, jakým způsobem byly získány.

Informatická kriminalita – **IT crime** je pak v podstatě oblastí informační kriminality, při které dochází k narušení celého informačního systému nebo jeho části. U počítačové kriminality – **cyber crime** resp. **computer crime** je touto částí buď samotný počítač, jeho data, programy nebo jeho uživatel, správce nebo provozovatel.

Takovéto rozlišovaní je však podle mého názoru velmi diskutabilní. Neuvěřitelný nárůst a rozmanitost trestných činů v této oblasti způsobuje také velká provázanost mezi jednotlivými takto definovanými činnostmi. Často se proto informační kriminalitou rozumí i trestná činnost, obecně označovaná jako počítačová kriminalita.

Oblast je specifická tím, že se jedná o trestné činy, které jsou prováděny nestandartními formami v porovnání s běžnou trestnou činností. Jejich hlavními rysy je obvykle absence fyzického násilí a nebo používání klasických zbraní. Dalším rysem oproti běžné trestné činnosti je délka časového úseku, kdy ve velmi krátkých časových intervalech při provedení samotného „útoku“ (s cílem získání informačních dat nebo s cílem způsobení škody) může být napadeno více míst najednou. Po provedení takového činu pak nastávají dvě varianty, se kterými se v dané problematice setkáváme nejčastěji. První je rychlé provedení útoku a následně jeho rychlé ukončení. Druhou variantou je rychlé provedení útoku za účelem vytvoření přístupu k datům a následné dlouhodobé „čerpání“ informací.

Pachatelé obvykle operují ze vzdálených míst, většinou nejsou přítomni u cíle svého útoku.

3.2. Historie informační kriminality, její vývoj a její pachatelé

Vznik informační kriminality, jak již bylo uvedeno v úvodu, nelze samozřejmě určit. Její masivní nástup začal až po přechodu od industriální společnosti. Současná éra, často označovaná jako počítačový věk, přispěla k rozšiřování IT technologií a tím i k větším možnostem získávání, přenášení a uchovávání informací. Informace v digitální formě jsou teoreticky mnohem snadněji napadnutelné.

Pokud ale budeme používat pojem informační kriminalita v souvislosti s informačními technologiemi a počítačovou technikou, byly útoky pachatelů zaměřeny na zneužívání telefonních linek. První vážnější pokusy se zrodily v 70. letech 19. století. Snahy pachatelů byly zaměřeny na proniknutí do systému telefonních společností zevnitř samotnými zaměstnanci, později i zvenčí. Výše způsobených škod nebyla tehdy nijak závratná, neboť účelem útoků byly snahy o umožnění hovorů zdarma. Byly to také i jen žertíky jako odpojování a přepojování k sobě nepatřících hovorů. Velký vzestup informační kriminality nastal až od 80. let 20. století. Počítače tehdy začaly být propojovány do sítí pomocí serverů s textovým rozhraním. Byl to jakýsi předchůdce dnešního internetu. Propojování serverů však bylo uskutečňováno přímou volbou čísla. Razantní nástup zprostředkovatelů připojení ISP nastal až později.

Na vzniku informační kriminality a jejím velkém rozvoji se podílí hned několik faktorů [18]:

1. Složitost informačních technologií – pro mnohé uživatele je svět IT neuchopitelný, neproniknutelný.

2. Důvěra uživatelů - málokoho třeba napadne kontrolovat počítač, správnost jeho výpočtů.

3. Objem dat – kontrola velkého objemu dat je neefektivní. Je to ideální prostředí pro pachatele.

4. Snadnost a anonymita – vyloupení banky od terminálu je snazší než klasickým způsobem se zbraní v ruce.

5. Nízké právní vědomí – IT je velmi rozšířená, ale pro mnohé stále složitá. Příslušné právní normy jsou pro mnohé nepochopitelné a jejich obecná znalost a povědomost je malá.

6. Nedokonalost legislativy - právní normy reagují na vývoj v IT často se zpožděním, navíc jsou příliš komplikované a obtížně vyložitelné.

Pachateli trestných činů se často stávali sami zaměstnanci firem, kteří zpočátku pronikali do systému, aby jej zdokonalili. Bývají to také například neúspěšní kritici, kteří napadají IT systém proto, aby upozornili na jeho slabiny. V minulosti to byli spíše náhodné a pokusné útoky, než promyšlené činy. Osvěta v této oblasti, která je v poslední době čím dál tím kvalitnější, působí preventivně a pomáhá minimalizovat následky činů páchaných v minulosti z nevědomosti. Informování veřejnosti o činech, následcích a postizích a to nejen u informační kriminality, pomáhá odrazovat nové potenciální pachatele.

Pachatelé informační kriminality jsou podle vztahu k informacím rozdělováni na [19]:

- **Amatéry** – zde jsou zařazováni hackeři, crackeři, neúspěšní kritici, mstitelé. Jejich cíle a motivace jsou různé.

- **Profesionály** – softwaroví piráti, teroristé, detektivové, žurnalisté, specialisté informatici.

Trestná činnost bývá prováděná nejen samostatně. Častěji dochází k jakémusi sdružování do skupin a společenstev, kdy jednotlivé osoby mají stanoveny přesné úkoly podle své specializace. Ve většině případů se členové takovýchto uskupení mezi sebou osobně vůbec neznají, veškerá komunikace totiž probíhá elektronicky.

Podle specifických oblastí a činností jsou pachatelé informační kriminality označováni zvláštními pojmy [19].

Mezi ty základní patří:

- Označení **hacker** prošlo v průběhu let vývojem. Zatímco v minulosti to byl člověk, specialista a nadšenec, ke kterému se vzhlíželo s úctou pro jeho znalosti, nyní je považován za kriminálníka. V skutečnosti se jedná o osobu, která proniká do chráněných systémů proto, aby prokázala své schopnosti a dovednosti. Jejím zájmem není chráněný systém narušit nebo zneužít. Hackerovi jde především o získání respektu a uznání. Správci resp. majitelé těchto „nabouraných" systémů bývají také na takový průnik často sami upozorněni. Pro hackera je každé zdokonalování bezpečnosti systému chápáno jako další výzva, meta k překonání.

- Jako **crackera** označujeme osobu resp. osoby, které vnikají do chráněného systému s cílem jeho poškození nebo zneužití. Z takového systému odstraňují ochrany, prolamují jeho kód nebo jinak narušují jeho integritu. Cracker zpravidla nepracuje sám, obvykle je členem organizované skupiny, kde má starost určitou oblast. Jednotlivé skupiny, které jsou většinou tematicky zaměřeny na určitou oblast, mezi sebou soupeří o prestiž. U crackerů je také patrné uspokojení z destrukce.

- **Phreaker/phracker** – útočníci využívající slabin a pronikající do telefonních sítí.

- **Phisher** – útočníci, kteří vytvářejí identické webové stránky a jejich aplikace, obvykle bankovních institucí. Jejich snahou je získat a zneužít citlivé informace.

- **Looser/Lamer** – uživatelé s minimálními znalostmi, využívají již vytvořené utility nebo mírně upravené zdrojové kódy.

Podobných pojmů, kterými jsou pachatelé tohoto druhu kriminality označováni, je nepřeberné množství a další stále vnikají. A mnoho oblastí své zvláštní označení zatím nemá. Mezi ně patří například pachatelé kyberšikany, kopírovači bankovních nebo telefonních karet (carding), crackeři kryptovacích karet a podobně.

3.3. Druhy informační kriminality ve vztahu k legislativě

Při vyšetřování informační resp. počítačové kriminality jsou trestné činy obecně rozdělovány na dvě základní skupiny [18].

První skupinu tvoří trestné činy, ve kterých je počítač nebo IT technologie prostředkem k jeho spáchání. Počítač se stává nástrojem.

Druhá skupina jsou trestné činnosti, kdy je počítač terčem útoku. Například jeho krádež, poškození SW a podobně.

Ne vždy je samozřejmě taková kategorizace možná, obě skupiny velmi často prolínají. K průniku do chráněného systému je používán počítač, takže je zároveň jeho terčem i nástrojem.

Pokud má být informační kriminalita považována za trestnou činnost, musí mít z hlediska trestního zákona určité znaky. Mezi tyto znaky vedle úmyslu patří také stupeň nebezpečnosti. Pokud je stupeň nebezpečnosti nepatrný nejedná se o trestný čin, ale o přestupek nebo jiný správní delikt. Pro jednotlivé trestné činy je pak důležitá skutková podstata trestného činu. Ta ale v současném klasickém trestním zákoně příliš s informační kriminalitou nepočítá. Ke konkrétnímu jednání je tak přiřazována skutková podstata – to bývá označováno jako subsumpce. Pokud se při posuzování trestné činnosti nenajde skutková podstata, pod kterou by mohlo být jednání subsumováno, nezbude než konstatovat, že daný čin není podle českého právního řádu trestným činem.

Václav Smejkal [20] definuje trestné činy v této oblasti jako soubor všech možných jednání souvisejících s informačními systémy. Ty dále dělí na:

- *Trestné činy ve vztahu k hmotnému majetku jako věcem movitým* – zde se jedná o klasickou **majetkovou kriminalitu**
- *Trestné činy ve vztahu k nehmotnému majetku* – databáze, programy – **informatická kriminalita**

- *Trestné činy, při nichž je počítač prostředkem k jejich páchání* – podvody, šikana,…

- hospodářská kriminalita

Seznam jednotlivých skutkových podstat obsažených v současném trestním zákoně [10]. K tomu je informační kriminalita vztažena:

- **§124** Porušování předpisů o oběhu zboží ve styku s cizinou,
- **§150** Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu,
- **§151** Porušování průmyslových práv,
- **§152** Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi,
- **§178** Neoprávněné nakládání s osobními údaji,
- **§198** Hanobení národa, etnické skupiny, rasy a přesvědčení,
- **§198a** Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod,
- **§199, 200** Šíření poplašné zprávy,
- **§205** Ohrožování mravnosti,
- **§206** Pomluva,
- **§239** Porušování tajemství dopravovaných zpráv,
- **§249** Neoprávněné užívání cizí věci,
- **§249b** Neoprávněné držení platební karty,
- **§250** Podvod,
- **§257a** Poškození a zneužití záznamu na nosiči informací.

Zda jsou uvedené skutkové podstaty použitelné na všechny páchané delikty v oblasti informační kriminality, je přinejmenším velmi diskutabilní. Nejen český právní řád na vývoj v oblasti informační kriminality reaguje jen velmi pomalu a jsou stále častější případy, kdy se stávají některé delikty nepostihnutelnými.

Typickým příkladem je hacking. Ustanovení § 249 – neoprávněné užívaní cizí věci, na něj použít nelze. Nejsou totiž splněny znaky daného trestného činu – …*zmocní se cizí věci nikoli malé hodnoty…způsobí škodu nikoli malou…* . Tím není naplněna skutková podstata. Obdobné je to v případech § 257a, kdy je nutno prokázat pachateli úmysl. Nedbalostní kvalifikaci toto ustanovení vůbec nezná.

Znaky trestného činu – jeho skutkovou podstatu charakterizuje objekt a objektivní stránka trestného činu a dále subjekt a subjektivní stránka trestného činu.

Internet ale podle Smejkala [20] není subjektem práva, nemá právní subjektivitu, není hmotným předmětem ani čistě nehmotným statkem a není ani objektivní právní skutečností nezávislou na lidském chování. Je to informační a komunikační systém, který jako celek nemá majitele.

Subjekty z trestního hlediska jsou zde uživatelé, poskytovatelé připojení, vlastníci serverů, poskytovatelé služeb. **Objekty** jsou pak hmotné i nehmotné objekty, chování a důsledky chování. Je proto velmi problémové postupovat klasickým způsobem. Internet se proto považuje za přenosový kanál, umožňující poskytování a využívání služeb. Z hlediska práva je nutné řídit se dvěma základními principy:

1. Princip teritoriality – uplatňuje se právo té země, ve které je služba poskytována, popř. kde je sídlo poskytovatele, nebo kde jsou umístěny servery. Problémem je, že jednotlivá místa - země mohou být různá a stejně tak jsou různé i právní systémy těchto zemí.

2. Princip práva upravující druh činnosti – obchodní, občanský zákoník, autorský zákon a podobně. Opět vše komplikuje charakter internetu – jeho globální prostředí, bez prostorových hranic a anonymita.

3.4. Protiprávní jednání proti počítači

Tato problematika je dělena také na tzn. tradiční jednání, které se informační kriminality týká jen okrajově, a nová jednání.

Mezi tradiční jednání patří:

- **Krádež** – rozumí se zde odcizení počítače, notebooku, části nebo celku IT systému. Motivací pachatele je zde obohacení, nedochází ke zneužití dat apod. Bývá naplněna skutková podstata §247 TZ

- **Loupež** – obdobná činnost, za použití násilí, pohrůžky násilí nebo se zbraní podle §234 TZ

- **Průmyslová špionáž** – provedení obvykle pomocí hackingu, ale s cílem získat cenné data. Útok bývá prováděn nejen zvenčí, ale i zevnitř zaměstnanci firmy. Zde je aplikován § 257a TZ

Nová jednání:

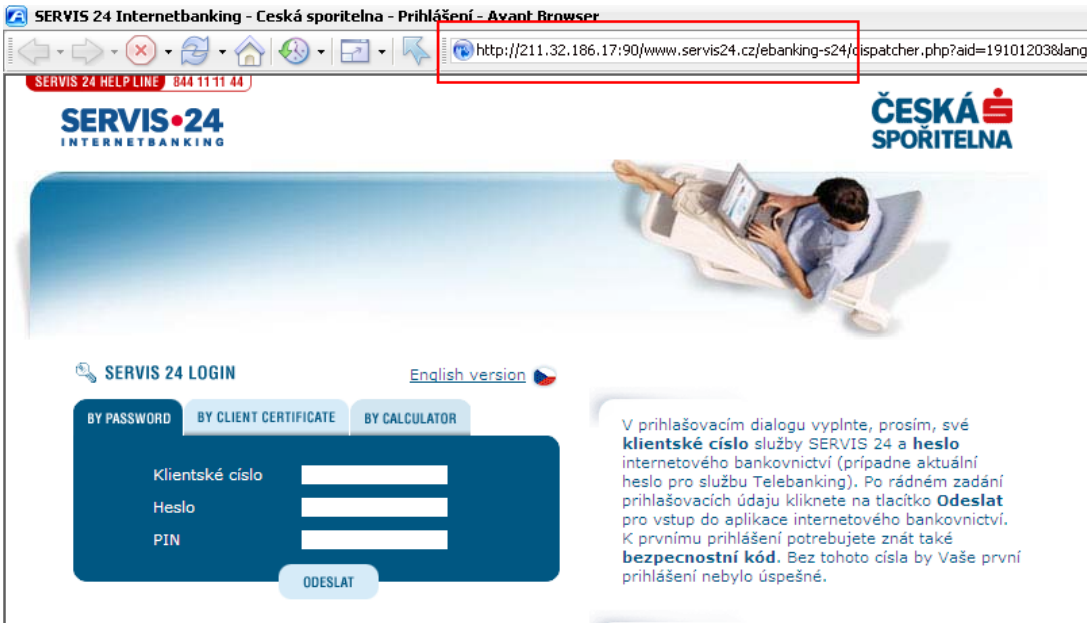
- **Hacking/cracking** – je druhou největší oblastí po porušování autorských práv. Dochází při něm k průniku do systému s cílem zneužít data ve svůj prospěch §178 TZ nebo způsobit jinému újmu §257a TZ. Jak už jsem popisoval výše, motivací hackerů bývá dobrodružství, snaha překonávat bariéry nebo jen zábava. Zpočátku svou činnost neprovádějí se „zlým úmyslem“, postupem času se ale většinou stávají crackery. To v případě, že své znalosti, získaná data nebo programy využívají pro svou potřebu resp. obohacení. Často bývají i zneužíváni. V druhém případě se z hackerů stávají uznávání odborníci na IT bezpečnost.

- **Carding** – zde se jedná o zneužívání platebních karet. A nejen jich. Z naší historie jsou známy případy tzn. nekonečných karet do telefonních automatů. Ke zneužívání platebních karet dochází nejen jejich krádeží. Zcizovaly se algoritmy, které dokázaly vygenerovat číslo kreditní karty. Zvláštním odvětvím je **phreaking** - tato metoda

spočívá v technice, kdy se pachatel vydává za zaměstnance banky a od poškozeného „vytáhne“ potřebné údaje.

- **Phishing** – navazuje na phreaking. Pachatelé vytvoří téměř identické falešné webové adresy a pomocí nich získávají od napálených klientů bank jejich čísla účtu, přístupové kódy a podobně. Předmětem zájmů jsou i jiné citlivé informace.

-



Obrázek 1. Falešné stránky České spořitelny

(zdroj http://blog.vyvojar.cz/photos/pbouda/picture227260.aspx)

Nejčastěji bývá útok prováděn zasláním e-mailů, které obsahují oficiálně vypadající formulář. Poté pachatelé jen čekají na jeho vyplnění a odeslání. Sofistikovanější formou odvozenou od phisingu je **pharming.** Ten spočívá v „otrávení“ záznamu v DNS (jeho změně) tak, že běžný uživatel ani nepozná, že jej systém přesměrovává na podvržený server. Hlavní metodou pharmingu a phishingu je **sociální inženýrství**. Jeho hlavním úkolem je získat si důvěryhodnost.

- **DoS** resp. **DDos útok** – jeho snahou je zahlcení serveru nebo sítě s cílem ochromit jeho provoz. DDoS útok bývá navíc prováděn souběžně z velkého množství počítačů - jsou označovány jako **botnety**. Ty byly předtím nakaženy virem, který

má cíl, čas a druh útoku zakódován. Spouštění je také možné stažením a spuštěním speciálního softwaru. Obrana před takovým útokem je velmi obtížná – znamená přenastavení routerů a firewallů.

Motivací pachatelů je zisk. V posledních letech byl tento typ vydírání i škody způsobeny DDoS útoky na vzestupu. Jsou dokonce známy případy, kdy jsou počítače jako botnety pronajímány.

3.5. Protiprávní jednání s využitím počítače

U těchto trestných činů je nejvíce patrný pokrok v oblasti IT a ICT techniky. Každý nový vynález či jiný pokrok je téměř okamžitě využit v protiprávních činnostech. Příkladem mohou být zlepšující se a výkonnější vypalovací mechaniky nebo barevné tiskárny, pomocí kterých je možno vyrábět nelegální kopie.

Také zde jsou trestné činy podle tradičního jednání a nového jednání. Tradičním jednáním se tady opět rozumí trestná činnost, která nástupem a možností využívání moderních IT technologií získala nový rozměr. Jedná se především o:

- **Podvody, zpronevěru a různé podvodné hry**. K naplnění skutkové podstaty trestného činu podvodu podle § 250 TZ dochází při provozování falešných e-shopů, jsou to také aukce, inzeráty a další podobné aktivity. Je zde maximálně využívána anonymita internetu. Zpronevěry podle § 248 se dopouští zaměstnanci bank nebo jiných finančních institucí. IT technologie a znalosti přístupových kódů jim značně ulehčují jejich činnost. Podvodné hry, sázky a „letadla“ postihuje ustanovení § 250c TZ.

- **Padělání a penězokazectví**. Pokročilá výpočetní technika v současné době velmi dobře nahradí práci rytců. A ve spojení se stále dokonalejší reprodukční technikou dokáží padělatelé doslova divy. Česká republika drží v Evropě v počtu padělaných bankovek neslavné druhé místo.

- **Šíření pornografie, Extremismus a Hoaxes.** Prostředí internetu se v této oblasti osvědčuje jako téměř dokonalý distribuční kanál. Paradoxně tomuto prospívá i zvyšující se propustnost sítí. Za Hoaxes je považováno šíření lživých a nepravdivých zpráv. Některé opravdu zdařilé a působivé hoaxes mohou naplňovat skutkovou podstatu trestného činu šíření poplašné zprávy § 199 TZ.

Novější jednání – jejich formy, techniky a způsoby nelze označit za klasické, jejich vznik byl podmíněn nástupem IT technologií.

- **Porušování autorských práv.** Je to absolutně nejvíc rozšířená oblast informační kriminality. Na porušování autorských práv je možno nahlížet jako na občanskoprávní delikt. Ale jen do té doby, než dojde naplnění skutkové podstaty trestného činu podle § 152, § 149 a § 150 TZ nebo § 32 zák č. 200/1990 Sb. o přestupcích. Ochrana autorských práv se v tomto smyslu vztahuje nejen na díla hudební a filmová, ale také na databáze a SW. U databází a programů se vžil název **Softwarové pirátství**. Z pohledu Autorského zákona se jedná o nelegální užití, ke kterému dochází:

1. Rozmnožováním (§ 13 Aut. Z)
2. Rozšiřováním (§ 14 Aut. Z) - rozšiřování originálu i rozmnoženiny
3. Pronájem originálu nebo rozmnoženiny (§ 15 Aut. Z)
4. Půjčováním díla (originálů i rozmnoženiny) (§ 16 Aut. Z)
5. Sdělováním díla veřejnosti (§ 18 Aut. Z)

Jak lze vidět, při porušování autorských práv dochází k více různorodým činnostem. Na každou činnost se soustředí daný „specialista“, dohromady pak tvoří funkční skupinu. Práce jednotlivých členů – specialistů spočívá pro příklad u filmového díla v získání originálu, odstranění ochrany, výroby titulků, další možné úpravy jako konverze do jiného formátu, doplnění další zvukovou stopou apod. až do distribuce.

V minulosti bylo softwarové pirátství záležitostí jednotlivců. S rozvojem IT technologií dochází k jejich sdružování do skupin, dochází k nástupu warez. K rozšiřování svých děl v rámci internetu byly a stále ještě jsou využívány P2P - *peer to peer* sítě. S rostoucími přenosovými rychlostmi a stále dokonalejšími kompresními formáty dochází ale stále více k využívání warez forum. Jsou to v podstatě webovské stránky, které jsou obvykle přístupné pouze s registrací, a které slouží k diskuzi nad nejrůznějšími problémy (V České republice jsou to například stánky www.war-forum.net, www.war4all.com). Nelegální obsah je distribuován formou odkazů na webovské servery, které slouží jako výměnné uložiště dat. Používání tohoto serveru je obvykle zpoplatněno.

Ve většině vyspělých zemích je tvorba a distribuce warezu považována za nelegální činnost. Proto je tato činnost provozována buď přímo nebo prostřednictvím (umístěním serverů, využití proxy serverů,..) zemí, kde je tato činnost ignorována, není postihována nebo není nelegální. Například u nás je podle § 30 Autorského zákona použití jiného díla než programu a databáze pro vlastní potřebu **legální i bez svolení autora**. To znamená, že je sice nelegální distribuce, ale stažení a užití díla pro vlastní potřebu v rozporu se zákonem není.

- **Spam** – rozesílání nevyžádaných informací, obvykle e-mailovou poštou. Se spamem se setkal každý, kdo má zřízenu e-mailovou schránku. Velké organizace a provozovatelé poštovních serverů se spamem bojují blokováním e-mailových adres spamerů.

- **Cyberšikana** – relativně nový „nešvar“. IT technika je využívána k obtěžování, pomluvě nebo jinému nátlaku na konkrétní osoby. Děje se tak umísťováním videí, nebo jiných nahrávek na internet, posíláním zesměšňujících nebo urážlivých SMS anebo pomlouváním na různých chatech. Rozsáhlejší a sofistikovanější útoky proti skupinám nebo obecně široké veřejnosti jsou označovány za **Kyberterorismus**.

- **Sniffing** – jedná se o neoprávněné monitorování a odposlouchávání komunikace. Zjištěná data, hesla a podobně bývají snadno zneužitelná. Sniffing není jen nelegální

činností, bývá obecně využíván správci sítí k analýze propustnosti sítí nebo při provádění auditů dané sítě.

3.6. Opatření v boji s informační kriminalitou

Pro boj s informační kriminalitou jsou nezbytnou podmínkou příslušné právní normy. Tyto normy by ale také měly, stejně jako normy v ostatních oblastech trestního práva, přihlížet ke stupni nebezpečnosti spáchaného trestného činu. Určitě by se mělo jinak přistupovat k pachateli, který sice způsobil škodu vydavatelské firmě tím, že dále distribuoval její hudbu nebo filmy, ale rozhodně tím nikoho neohrozil na životě. Jiným příkladem by bylo „nabourání“ se a „shození“ dispečerského řídícího stanoviště pražského metra, kdy by došlo k ohrožení mnoha životů.

Zcela zásadním problémem při boji s informační kriminalitou je již výše popisovaná teritorialita. Pokud se má dosáhnout nějakých výsledků, bude nutné, aby svět při vytváření právních norem týkajících se této problematiky alespoň v základních bodech postupoval jednotně.

Možné řešení současné situace proto rozděluji do tří základních oblastí:

- **Zvýšení informovanosti uživatelů** – Z historie víme, že prevence má nezastupitelnou úlohu v předcházení problémů. Pokud si tak výchovou a vzděláním dokážeme vychovat odpovědné uživatele, věřím, že časem dojde k výraznému zmenšení prostoru pro možnou informační kriminalitu. A to i proto, že snad dojde k úbytku případů, kdy docházelo k porušování zákonů z nevědomosti nebo podceňování možného postihu. Potencionální pachatelé by měli již dopředu vědět co je a co není trestným činem. Svoji úlohu má proto samozřejmě i represe. Musí být jasně daná „pravidla hry“ a případné tresty by měly být společensky akceptovatelné.

- **Zavedení bezpečnostních standardů** – Znamená to důsledné vytváření a zavádění pravidel pro informační bezpečnost. Když použiji analogii – pokud nechám na parkovišti otevřené vozidlo, nemohu se pak divit, že jej ráno už nenajdu.

- **Sjednocení základních právních norem** - Tady musím předpokládat největší úskalí celého snažení o posílení informační bezpečnosti. Problémem je, že celosvětový internet se neřídí žádnými celosvětovými pravidly. Snahy Evropské unie nebo jednotlivých zemí pak nemají požadovaný účinek.

Pokud se pokusím shrnout problematiku informační kriminality, je i pohled široké veřejnosti v podstatě jednotný. Společnost chápe informační kriminalitu jako zlo, proti kterému se musí bojovat. Značně diferenciovaný je ale pohled na ochranu autorských práv. Týká se to především hudebních děl, kde jsou jednotlivé vydavatelské společnosti mající v podstatě monopol na konkrétní dílo, chápany jako nemorální a ziskuchtivé. Ničemu ani nepřispívají jejich kartelové dohody o cenách, diskriminace trhu a lobování za trestní úpravy. Porušování autorského práva se právě díky digitalizaci a komunikačním kanálům stalo nerozšířenější na světě. A obecné řešení tohoto problému je ale zřejmě v nedohlednu.

Dá se říci, že vyspělé země se s nárůstem informační kriminality snaží vypořádávat. Vždy se ale snaží vycházet z již dosud platných norem a zabývají se hlavně otázkou informační bezpečnosti. Jeden ze strategických dokumentů v České republice *Státní informační a komunikační politika – e-Česko 2006* má jako prioritní cíle dostupnost a bezpečnost komunikačních služeb. Dále se pak zabývá uváděním v život používání elektronického podpisu. Z hlediska boje s informační kriminalitou se připravují úpravy resp. novelizace trestního zákonu.

V preventivní oblasti lze jen ocenit velkou práci odváděnou neziskovými organizacemi. Ty se snaží i velmi pružně reagovat na konkrétní problémy jako je tomu třeba u kyberšikany. Bohužel je jejich „úhel záběru“ omezen možností získání grantů na konkrétní úkoly.

4. Digitální stopy

V česky psané literatuře je problematika digitální stop snad nejlépe vysvětlená v článku V. Porady a R. Raka, Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách [6]. Z tohoto textu budu proto také v této kapitole především vycházet.

Jak je tedy uvedeno v [6], v běžném životě denně používáme velké množství techniky, od telefonů, resp. mobilních telefonů, digitálních záznamových zařízení (kamery, videokamery, diktafony), elektronických diářů až po počítače. A nejen jich. Prokazatelné stopy své činnosti zanechávají i jiné zařízení. Může se to týkat například platebních karet, palubních počítačů vozidel nebo zabezpečovacích a monitorovacích zařízení.

„Celá řada technologických zařízení, i když nejsou prostředkem nebo cílem trestného činu, obsahuje velké množství rozmanitých dat, která v průběhu vyšetřování jiného trestného činu, přestupku či zcela jiné aktivity mají v první fázi klasický charakter kriminalistické stopy a v konečné etapě v ideálním případě pak charakter soudního důkazu. Pomocí všech těchto stop je pak možné prověřovat vyšetřovací verze případu, sbírat důkazy proti pachateli nebo naopak potvrzovat alibi nevinných osob. Stopy se v procesu soudní obhajoby stávají přímými či nepřímými důkazy. Na datovém médiu mohou být záznamy o činnosti uživatele na počítači, v mobilním telefonu seznam posledních hovorů oběti trestného činu, na videozáznamu dohledového centra obchodního domu či banky zákazníci přítomní v inkriminované době, v palubním počítači automobilu identifikační čísla (VIN), která pachatel zapomněl při mechanické falzifikaci ostatních čísel na vozu změnit, nebo to nevěděl či neuměl; v telefonní centrále výpis všech uskutečněných hovorů, v systémech GPS souřadnice objektu (např. automobilu) v konkrétním čase atd.“ [6]

4.1. Definice digitální stopy

„Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. Tyto záznamy jsou z kriminalistického hlediska stopami. …

Ve smyslu výše definované počítačové nebo kybernetické kriminality nebo kriminality počítačově či kyberneticky související je pojem zařízení pracujících s daty mnohem širší než pouhý počítač.“ [6].

Snad nejčastější a v odborných kruzích nejuznávanější definicí je definice, která byla navržena v roce 1999 pracovní skupinou *SWGDE – Scientific Working Group on Digital Evidence* – skupinou odborníků a zástupců amerických úřadů zabývající se vyšetřováním. Ta vznikla roku 1998 z iniciativy FBI.

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“

Tato definice splňuje všechny předpoklady - je dostatečně obecná a použitelná pro celou oblast vyšetřování, které může být prováděno nejen státními orgány při zajišťování stop v souvislostí s trestnou činností, ale i forenzními nebo soukromými společnostmi při provádění například auditů. Digitální stopa nemusí být tedy nutně spojována s trestným činem. Digitální stopy se mohou používat jako podklady i v soukromém nebo veřejném sektoru pro další analýzy v oblasti zkvalitňování služeb, zlepšování pracovního procesu a podobně.

Podstata **kriminalistické stopy** je obecně popsána filozofickou teorií odrazu: *„Působí-li na sebe současně dva nebo více objektů, dochází ke vzájemnému předávání informací o jednotlivých objektech navzájem“*. Přitom je v podstatě lhostejné, jaký je charakter jednotlivých navzájem na sebe působících objektů [Porada, 2001]. V praxi to znamená, že za kriminalistickou stopu je považován odraz, který splňuje podmínky:

1. K odrazu resp. změně musí dojít v souvislosti s kriminalisticky důležitou událostí.

Ne všechny záznamy resp. informace jsou kriminalistickými stopami. V celkové množině jsou to ty, které nelegální činnost pomáhají dokumentovat a odhalovat. Ostatní mohou být využity při obecnějším šetření nebo auditu.

2. Odraz resp. změna musí existovat minimálně od vzniku do jeho zjištění.

   Důvodem je samozřejmě objektivnost. Za stopu nemohou být vydávány domněnky a dohady. Stopa musí existovat a musí být zajištěna.

3. Odraz resp. změna musí být vyhodnotitelná.

   Tato podmínka se vztahuje k analýze digitální stopy, na základě které se určí její relevance a její možná důkazní hodnota. Pokud nelze zjištěný odraz současnými prostředky vyhodnotit, není pro prováděné šetření použitelný. To klade velké nároky na odbornost a technické vybavení kriminalistického, znaleckého nebo forenzního pracoviště, které se daným vyhodnocováním takových stop zabývají.

4.2. Kategorizace digitálních stop

„Při zkoumání digitálních stop v první fázi nemusí být vždy zřejmé, zda digitální stopy odpovídají aktivitám kriminálního charakteru nebo zda mohou být využity pro forenzní šetření obecnějšího charakteru, či zda se jedná o stopy běžné, legitimní činnosti pachatele. Digitální stopy obecně se mění v kriminalistické, když je nalezena souvislost s trestnou činností pachatele. Záleží tedy na tom, co vyšetřujeme, co hledáme. V každém případě je nutné prověřovat každou relevantní stopu, potvrzovat nebo vyvracet pracovní vyšetřovací hypotézy.

Stopy v materiálním prostředí a ve vědomí lidí lze podle jejich využitelnosti pro různé druhy vyšetřování rozdělit do tří základních kategorií:

a) *Kriminalistické stopy*. Vztahují se k vyšetřování trestných činů a přestupků, specifikovaných zákonem. Pro potřeby kriminalistické (stejně tak ovšem i

forenzní) praxe je požadována vysoká kvalita, objektivita zajištěných stop. Kriminalistické stopy chápeme jako podmnožinu forenzních stop.

b) *Forenzní stopy*. Obecně jakékoliv stopy využitelné pro potřeby forenzního vyšetřování, včetně šetření orgánů činných v trestním řízení. Na rozdíl od klasického kriminalistického vyšetřování sem ale patří i vyšetřování charakteru forenzních auditů v civilní nebo komerční sféře. Výstupy vyšetřování jsou připravovány tak, aby svou kvalitou a formálním zpracováním obstály před soudními orgány. V praxi se setkáváme s případy, kdy na základě šetření interního auditu nebo nezávislé expertní (nestátní) instituce je podáno trestní oznámení. Zajištěné důkazy (stopy) by auditorskými orgány měly být předány státním orgánům činným v trestním řízení v dostatečné, standardně požadované kvalitě. Zajištění originálů některých digitálních stop je neopakovatelný proces, tj. dalším orgánům se nepodaří zajistit již jednou zajištěné stopy (vůbec nebo v požadované kvalitě tak, aby byly akceptovatelné).

c) Jinak využitelné stopy. Tento typ stop odráží všechny ostatní aktivity objektů a subjektů, které nespadají do dvou výše uvedených kategorií. Jsou to důsledky legitimních činností uživatele nebo objektivního působení vnějších sil a energií, které nemají logickou vazbu na forenzní stopy a které lze využít např. při nejrůznějších analýzách, zaměřených na zvyšování výkonu nebo zlepšování funkčnosti zařízení, ekonomičnosti provozu, dostupnosti služeb, stupně bezpečnosti apod. Kvalita a norma zpracování stop v tomto případě je obvykle poplatná účelu, ke kterému mají být výstupy použity. Často jsou to i interní materiály vnitřní kontroly, dodržování institucionálních pravidel atd. Svým charakterem a kvalitou tento druh stop nemusí (ale může) být akceptovatelný soudními orgány.“ [6]

Dalším možným členěním digitálních stop je jejich kategorizace podle jejich materiální povahy:

Hmotné stopy – podle teorie digitálních stop [6] fyzické objekty. Těmi se zde rozumí „*…technologické části, zařízení určené ke zpracování, uložení nebo k přenosu dat. V praxi to jsou pevné disky počítačů, různá paměťová média (diskety, CD a DVD disky, paměťové karty, datové pásky atd.). V širším smyslu slova to jsou celá zařízení*

(např. počítače, tiskárny, síťové prvky apod.), obsahující kromě digitálních stop i další informace, jako jsou výrobní čísla, daktyloskopické nebo mechanické či biologické stopy a další, které dokazují logický vztah fyzického zařízení (vlastnický, uživatelský, časový ...), jeho uživatele (pachatele) a trestného činu nebo jiné aktivity, která je předmětem zájmu vyšetřování (zkoumání, šetření, interního nebo externího auditu). Fyzické objekty bývají často předmětem obecně širšího kriminalistického zájmu, než jen zkoumání digitálních stop. Podle potřeby jsou využívány všechny běžné metody kriminalistického zkoumání."

Nehmotné stopy – těmi rozumíme digitální data. Mohou to být soubory, adresáře, databáze, obsahy pamětí, … Ty jsou obvykle ukládána nebo přenášena na hmotných/fyzických objektech. Mohou to ale být jen doprovodná nebo pomocná data, která jsou neustále měněna a aktualizována. Jejich životnost je tomto případě velmi omezená a jejich uchovávání tak může být vážný problém.

4.3. Zdroje digitálních stop

„Podle definice je digitální stopa jakákoliv informace s vypovídající hodnotou relevantní pro vyšetřování konkrétního činu nebo aktivity, uložená nebo přenášená v digitální podobě. Informace jako taková je nehmotná. V okamžiku jejího ukládání se zhmotňuje v prostředí paměťového média, které se technologického charakteru. Abychom mohli přenášenou informaci analyzovat, musíme ji nejprve technologicky zachytit a následně opět trvale nebo dočasně uložit na paměťové médium. ***Digitální stopa je hmotného, materiálního charakteru.*** *Digitální stopa vzniká působením člověka (obecně uživatele, vývojáře, administrátora apod., neboť pachatel trestného činu může mít jakoukoliv z právě uvedených rolí) na uživatelský nebo systémový SW, automaticky předem naprogramovaným jiným softwarem či fyzikálním působením (např. silné vnější magnetické pole dokáže zničit data na paměťovém médiu a přitom zanechá stopy tohoto působení, jež jsou rovněž digitální) nebo jinými technickými prostředky. Interakcí vzájemného působení objektů se v případě digitálních stop účastní*

objekty živé přírody (zejména člověk), objekty neživé přírody (např. nahodilé fyzikální úkazy) nebo artefakty uměle vytvořené člověkem, kam patří SW, technická zařízení a prostředky apod. Ve všech těchto případech se na odrážející objekt přenášejí charakteristiky vnitřní stavby působícího, odráženého objektu. Digitální stopa je stopou vnitřní stavby odráženého objektu. ...

***Digitální stopa** je ve své primární formě, tedy uložená nebo přenášená, až na určité, nepatrné výjimky, **mikrostopou.** K jejímu zviditelnění jsou nutná technologická zařízení nebo uživatelský, systémový a zejména forenzní software. K nejjednodušším, uživatelům blízkým, technologiím patří monitory nebo displeje zobrazující digitální informace do lidsky přijatelného formátu (písmo, obrazy, zvuk, videosekvence, vibrace atd.), které navíc umožňují převod digitálních dat pro uživatele na nativní paměťové médium – např. kancelářský papír, klasická fotografie. Takto transformované digitální informace (stopy) jsme schopni vnímat našimi smysly, zejména zrakem a sluchem, popř. hmatem (slepecké Braillovo písmo). Uživatelský SW (textové, grafické editory, tabulkové procesory) dokáže zobrazit běžné stopy, podobně jako systémový software, který je běžným uživatelům z hlediska vnímání a možností využití podstatným způsobem vzdálen. Specializovaný software forenzního charakteru dokáže navíc číst informace o smazaných souborech, rozbíjet hesla chránící přístup k zakódovaným informacím apod.* [6]

Z obecné teorie digitálních stop vyplývá jejich velká různorodost. A hlavně zdroje, ve kterých můžeme digitální stopy nacházet, mohou být nejrůznější – od IT, audio, video, telefonii až například po automobilový průmysl. Proto i V. Porada s R. Rakem v [6] používá zavedené logické třídění do tří základních skupin.

Zdroje digitálních stop jsou:

1. *Otevřené počítačové systémy* - Zde máme na mysli vše, co si představujeme pod pojmem počítač – PC stanice, notebook, server, atd. Zdrojem digitálních stop jsou zde ve většině případů data uložená na pevných discích.

2. *Komunikační systémy* – Sem patří klasické telefonní spoje, bezdrátové technologie, Internet a počítačové sítě. Předmětem zájmů bývají nejen přenášené informace, ale i

doprovodné údaje jako jsou místo resp. poloha uživatelů, datum a čas spojení a podobně.

3. *Zařízení s integrovaným čipem* – to mohou být platební karty, telefony, faxy, PDA, GPS navigační systémy, řídící jednotky vozidel, kamery a podobně.

Moderní technologie zažívají obrovský rozmach. Digitální stopy jsou tak téměř všudypřítomné a je jen na zkušenostech a znalostech toho, kdo je získává, zda dokáže využít všechny možnosti, které jsou mu k dispozici. To ale samozřejmě souvisí s permanentním sledováním technologického vývoje, udržováním technického zařízení na potřebné výši a stálým doplňováním znalostí. Stále se totiž můžeme setkávat s případy, kdy nejsou digitální stopy získávány a využívány v takovém rozsahu, který by byl pro daný účel potřebný. Je to problém nejen s nedostatkem specialistů schopných s digitálními stopami pracovat a jejich technickým vybavením, ale i s nevhodným právním prostředím. Vše spolu působí tak, že jsou tyto stopy přehlíženy, podceněny nebo nesprávně vyhodnocovány.

5. Detekce nezákonné činnosti

Problematiku detekce nezákonné činnosti můžeme v podstatě rozdělit na dvě provázané oblasti. Tou první oblastí je detekce nezákonné činnosti, která je úzce svázána s informační bezpečností, druhou je pak detekce digitálních stop nezákonnou činnost dokazující. Zde máme na mysli nejen detekci resp. získávání digitálních stop, ale i jejich vyhodnocení z hlediska relevantnosti a důkazní hodnoty.

5.1. Obecné předpoklady detekce – implementace informační bezpečnosti

„Informační bezpečnost je důležitou součástí řešení informačního systému organizace, a zejména jeho provozu. Má řadu rovin a náhledů: technologický, právní,

koncepční a lidský, který je zřejmě nejdůležitější. Lidský faktor je nejvíce chybující a nejproblematičtější, což někdy vede k tvrzení, že otázka informační bezpečnosti je otázkou lidí….

…Ideální by bylo při budování IS rovnou vyřešit (pokud možno trvale) jeho bezpečnost a celkovou informační bezpečnost organizace. Situace ale není tak jednoduchá. Samozřejmě, pokud se bude zavádět nový informační systém, mělo by součástí řešení být také řešení bezpečnosti tohoto systému, kterou by měl zaručit dodavatel systému, resp. systémový integrátor. Toto by mělo být součástí smluv, stejně jako při zavádění IS by velmi jasně měly být definovány bezpečnostní aspekty celého řešení, jako je testování IS při využití dat organizace, mlčenlivost o získaných znalostech o objektové bezpečnosti organizace atd. Dodavatel IS by měl smluvně ošetřit, že dodávaný systém odpovídá legislativě i v oblasti bezpečnosti. Například pokud bude IS obsahovat osobní a citlivé údaje, měl by zaručit příslušné nakládání s nimi dle zákona o ochraně osobních údajů apod. Obvykle je ale postup opačný, firma již nějakou dobu existuje, plní svoji funkci a má IS. Bezpečnost je řešena alespoň částečně (např. provádí se možná antivirová kontrola, je zaveden určitý způsob zálohování, provádí se autentizace hesly). Ale řada kroků je více méně náhodná, neprovádějí se systematicky, jedno oddělení spoléhá na druhé. Teprve při incidentu se zjistí, že vlastně nezálohoval nikdo. Obvykle se tedy důkladné a koncepční řešení bezpečnosti provádí již při existujícím IS. Navíc se bezpečnostní problémy často projeví až po nějaké době jeho provozu. Informační bezpečnost není jen bezpečnost IS, ale i prostředí, ve kterém je umístěn, chování lidí, kteří ho využívají, objektové bezpečnosti atd. Proto doporučuji tento postup: při budování IS co nejvíce dbát na bezpečnostní aspekty, smluvně je ošetřit. Při výběru IS a jeho komponent bezpečnostní hledisko brát jako jedno z klíčových. Po nějaké době fungování IS s ohledem na danou legislativu, bezpečnostní situaci atd. provést standardní kroky řešení bezpečnosti.“ [12]

V citovaném článku [12] jsou dále popisovány konkrétní kroky nutné při řešení informační bezpečnosti. Jsou jimi: studie informační bezpečnosti, riziková analýza, tvorba bezpečnostní politiky, bezpečnostní standardy, bezpečnostní projekt, implementace bezpečnosti a monitoring a audit.

Tyto a další kroky jsou také zahrnuty v mezinárodní normě ISO/IEC 27001:2005[1].

Problém informační bezpečnosti se ale netýká jen velkých firem, společností nebo orgánů státní a veřejné správy. Jim je často určitá úroveň ochrany nařizována i zákonem o ochraně osobních údajů č. 101/2000 Sb. nebo zákonem o utajovaných skutečnostech č.310/2002 Sb. a zákonem č365/2000 Sb. o informačních systémech veřejné správy. Týká se ale i jednotlivců, kteří by si sami měli osvojit základní pravidla informační bezpečnosti. Ty si mohou osvojit především zvýšením informovanosti o možných rizicích, vzděláním a také díky preventivně-informačním programům. Jednou z agentur EU mající velký přínos v této preventivní oblasti je ENISA.[2]

Podle společnosti Gartner jenom phishing v roce 2007 jen v USA údajně napáchal škody za 3,2 miliardy amerických dolarů. V roce předchozím to byly škody za 2,3 miliardy. Odhady škod jsou však velmi nepřesné a téměř každá společnost nebo agentura uvádí jiná čísla. Na čem se však shodnou je zvýšení počtu phishingových nebo spamových útoků z oblasti Číny.

Přitom ekonomické náklady na informační bezpečnost se pohybují kolem 10% z ceny informačního systému. Řešením nejen pro menší firmy je zde velmi oblíbený outsourcing IT. Hlavními výhodami outsourcingu je zde především to, že odpovědnost za problematiku nese jiný subjekt, odpadnou problémy v personální problematice včetně zvýšených mzdových nákladů nebo zastupitelnosti potřebných specialistů. Komplexně to v drtivé většině případů znamená nižší náklady na zajišťovanou činnost.

[1] Mezinárodní norma ISO/IEC 27001:2005 (ČSN ISO/IEC 27001:2006) definuje požadavky na zavedení systému řízení bezpečnosti informací. Na ni navazuje norma "ČSN ISO/IEC 17799:2006 Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací".

[2] ENISA – agentura, která vznikla nařízením Evropského parlamentu a Rady(ES) č. 460/2004 dne 10. března 2004. Evropská agentura pro bezpečnost sítí a informací. Její náplní je poradenství a pomoc Komisi a členským státům , shromažďování a analýza rizik , sledování vývoje norem a postupů v oblasti bezpečnosti informací.

5.2. Podmínky detekce

Z uváděných kroků používaných při implementaci informační bezpečnosti jsou k detekci nezákonné činnosti nejdůležitější monitoring a bezpečnostní audit. Z nich totiž mohou vyplynout informace o možných incidentech. Taková data jsou pak velmi cenným materiálem (digitální stopou), který může výraznou měrou přispět k odhalení útoku a jeho pachatele.

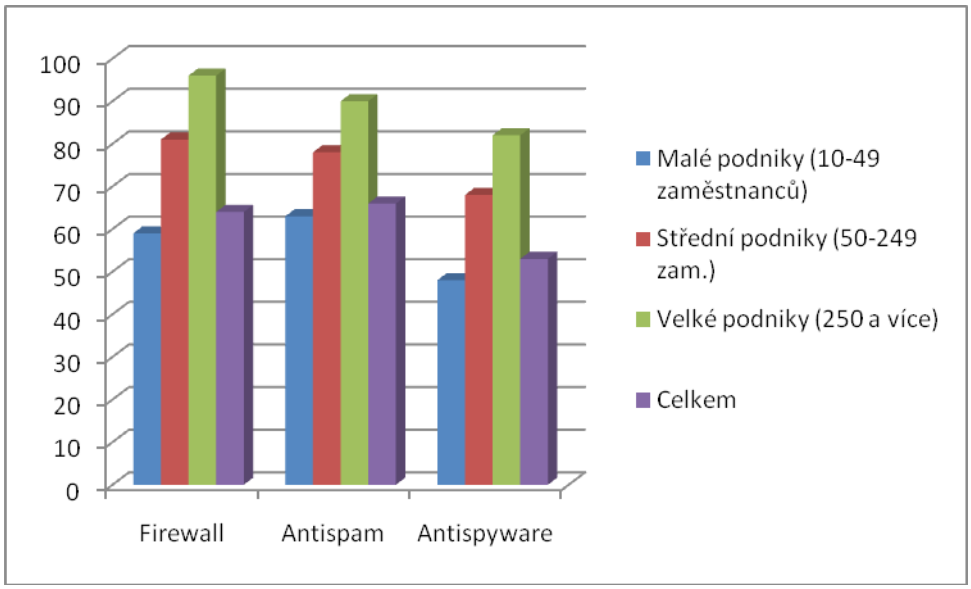
Velké společnosti svou informační bezpečnost orientují hlavně na samotné zajištění a udržení chodu firmy a zlepšování kvality poskytovaných služeb. Nicméně některé jejich systémy umožňují také využít zpracovávané informace i k detekci nezákonné činnosti. Typickým příkladem je používaní obdobné technologie, která je současně používána vládními agenturami některých států při boji proti terorismu. Zde máme na mysli systém vyhodnocování kvality poskytovaných služeb používaných v call - centrech. Jejich komerční monitorovací systémy jsou v současné době na takové úrovni, že běžně dokáží analyzovat v průměru kolem 60 tis. hovorů denně. Používané Voice Processing Systémy provádějí analýzy na vysoké trojí úrovni – z nahrávky je nejprve filtrován lidský hlas a dále jsou z proudu řeči určované emoce. Detekce klíčových slov je zde samozřejmostí.

Základní opatření pro zvýšení úrovně informační bezpečnosti a zjištění možného útoku (zde budeme hovořit především o počítačových systémech) jsou však mnohem jednodušší. Je jím používání antivirových programů, firewallů a antispywarových programů. Bohužel i přes relativně nízkou cenu takového zabezpečení je toto řešení stále podceňováno. Přitom podle [13] v roce 2008 byl v USA každý sedmý počítač vážně napaden virem, jehož odstranění vyšlo přibližně na 2,9 miliardy dolarů. Podobně byl každý čtrnáctý počítač napaden spywarem, náklady na jeho odstranění byly 3,6 miliardy dolarů.

Ze zde uvedených statistik dále vyplývá zamyšlení nad způsobeným přímým finančním dopadem – výdaji použitých na opravy. Odhad ukazuje, že každý sedmý uživatel (tzn. 26 milionů lidí) zaplatil $110 a každý čtrnáctý uživatel (tzn. asi 13

milionů lidí) zaplatil $275. Z toho lze zprůměrovat náklady, které vychází $35 na osobu. Průměrné ceny antivirových programů jsou přitom kolem $40.

Podle Českého statistického úřadu [15] používalo zabezpečení sítí a počítačů pomocí vhodných nástrojů v České republice v roce 2007 jen omezený počet podniků s připojením k internetu. Staticky procentuálně jsou znázorněny graficky na Obrázku 2.



Obrázek 2. Zabezpečení IT používané podniky v roce 2007

5.3. Detekce a analýza digitálních stop

Druhou problematikou související s detekcí nezákonné činnosti uvedenou v prvním odstavci v kapitole 5. je detekce digitálních stop. Informační bezpečnost můžeme chápat jako preventivní opatření, jejímž záměrem je informační kriminalitě předcházet a zamezovat ji. Detekce digitálních stop je pak spojována s opatřením represivním – souvisí s odhalováním, vyšetřováním a potrestáním této trestné činnosti. Zde je potřeba relevantní stopy zajišťovat, analyzovat a zpracovat. Aby byla získána digitální stopa akceptována s určitou důkazní hodnotou před soudními orgány, musí být zajištěna přiměřeným a legálním způsobem platným v dané zemi.

S tímto úzce souvisí standarty [9] navržené SWGDE[3] a IOCE[4], které byly odbornou veřejností přijaty.

Jejími základními principy pro zajišťování digitálních stop jsou:

1. Pro zajištění digitálních stop a jejich přípustnost je nutné vytvořit a dodržovat účinný systém zabezpečování jakosti. Standartní operační postupy (SOP) musí být dokumentovány a doložitelné. Jde o to, aby všechny subjekty, které zajistí, pořídí nebo zkoumají digitální stopu, zachovaly náležitosti SOP dokumentu.

2. Používané postupy musí být všeobecně uznávané v daném oboru.

3. Použité technické postupy musí být přesně zaznamenány.

   Použité postupy by měly být vhodně volené vzhledem k jejich účelnosti. Měl by být přesně zaznamenán postup zajištění stopy po jednotlivých krocích, včetně použitého hardwaru a softwaru.

4. Měl by být použit hardware a software vhodný a účinný nejen pro zajištěním stop tak, aby nevylučoval možné přezkumné řízení nebo jiné analýzy.

5. Všechny činnosti vztahující se k zajištění, skladování, vyhodnocení nebo převodu digitálních důkazů musí být zaznamenány v písemné formě a musí být k dispozici pro eventuální přezkoumání a svědectví.

6. Každá akce, která by mohla vést ke změně, poškození nebo zničení jakéhokoli aspektu původní digitální stopy, musí být dokladována a provedena kvalifikovanými osobami.

Popsané principy jsou důležité hlavně proto, že se snaží sjednotit postupy a činnosti při získávání, vyhodnocování a archivování digitálních stop obecně. Digitální stopa má svou důkazní hodnotu pouze tehdy, pokud lze prokázat nejen legitimitu jejího nabytí, ale i autentičnost a spolehlivost. K tomu všemu je také zapotřebí řádně

[3] Scientific Working Group on Digital Evidence - Vědecká pracovní skupina pro digitální stopy (SWGDE) byla založena v únoru 1998 na základě společného úsilí ředitele Federal Crime Laboratory.

[4] International Organization on Digital Evidence - organizace pro zajištění počítačových důkazů

vyškolený personál a odpovídající vybavení, software a postupy, které společně zajistí tyto atributy.

V této souvislosti jsou v [9] definovány další pojmy, které se při získávání, analýze a archivaci digitálních stop používají:

Datové objekty – Informace, data, databáze .

Fyzické objekty – Předměty, které obsahují datové objekty. (Paměti, pevné disky, CD, DVD, a podobně)

Originál digitální stopy - Jsou to datové nebo fyzické objekty zajištěné pro potřeby zkoumání resp. analýzy. Právě především k tomuto originálu se vztahují principy SWGDE. Z tohoto originálu se vytvářejí pracovní kopie a duplikáty stop, se kterými pracují experti nebo znalci. Originál ani jeho informační obsah nesmí být při vytváření kopie resp. duplikátu změněn. Postup musí být zaznamenaný tak, aby jej bylo možno za dodržení stejných podmínek opakovat.

Duplikát digitální stopy – Je to přesná reprodukce datového resp. datových objektů, která je provedena z originálního fyzického objektu v poměru 1:1. Obvykle se provádí i na stejný typ fyzického objektu. Výhodou duplikátu je přesný otisk dat, plnohodnotná a pohodlná práce a eventuální možnost vytvoření dalších duplikátů pro potřebu znalců. Nevýhodou může být velký objem dat, přičemž využitelná část pro potřeby vyšetřování může být minimální.

Kopie digitální stopy – Obdobně jako u duplikátu je to přesná reprodukce datových objektů na fyzický objekt. Ten obvykle bývá jiného typu a z datových objektů je reprodukována jen jejich část. Část, která je podstatná pro další vyšetřování. Hlavní výhodou je výrazně menší objem dat. Přínosem je i možnost použití u systémů, které není možné reprodukovat v poměru 1:1 (disková pole nebo jiná speciální uložiště dat). To může být zásadním problémem u větších nebo rozsáhlejších systémů. Nevýhodou bývá porušení vazeb a tím horší možnosti zkoumání. V některých případech nemusí kopie digitální stopy jako důkaz dostačovat a je potřeba ji doplnit i originálem.

5.4. Získávání dat

Detekce dat, jejich získání, zajištění a analýza zvláště u informační kriminality je často jedním z nejdůležitějších úkonů, jakým lze důkazní materiál získat. Jak ale roste zapojování informačních technologií do běžného života, roste i význam možnosti získání relevantních digitálních stop nebo jen podpůrných informací nezbytných k vyšetřování trestné činnosti.

Orgány činné v trestním řízení mohou nejčastěji zajistit potřebné stopy tradičními metodami, jako jsou:

- Ohledání místa činu
- Osobní nebo domovní prohlídkou, prohlídkou jiných prostor
- Vydáním nebo odnětím věci
- Kontrolním nákupem (ve spolupráci s ČOI)

Nověji se pak digitální stopy mohou zajišťovat monitorováním daného informačního nebo komunikačního systému. Oba způsoby jsou právně upraveny zákonem č. 141/1961 Sb. o o trestním řízení soudním (trestní řád).

5.4.1. Detekce digitálních stop pomocí monitorování IS/KS

Detekci digitálních stop v různé formě provádí mnoho státních i soukromých subjektů za účelem předcházení napadení informačního systému, ale také za účelem odhalení útoku nebo přímo ke zjištění pachatele takového napadení.

V případě soukromých subjektů je toto prováděno z důvodu ochrany svého soukromého vlastnictví, osobních dat, obchodních dat apod. Výčet důvodů by byl rozsáhlý, hloubka a kvalita takové detekce je různá, někdy i za hranicemi zákonů ČR (např. různé *šmírování* zaměstnanců).

V případě státních orgánů je situace zcela odlišná, protože každý státní orgán může pracovat pouze v rámci svých kompetencí na základě příslušných zákonů ČR. Přestoupení těchto kompetencí pracovníky státních orgánů je nejenom přestoupení pracovního řádu dané instituce, ale mohlo by vést i komu, že získané informace nedodržením zákonného postupu jejich získání by byly pro využití při soudním řízení nepřípustné.

Státní orgány, které mají pravomoc provádět detekci a analýzu digitálních stop jsou:

1. Policie ČR v případě vyšetřování trestné činnosti
2. Inspekce policie v případě vyšetřování trestné činnosti policistů
3. Armáda ČR v případě předcházení ohrožení bezpečnosti ČR
4. BIS v případě předcházení a odhalování ohrožení vnitřní bezpečnosti a stability ČR

Všechny tyto instituce mají své technické prostředky k detekci a analýze digitálních stop. Jako příklad můžeme uvést útvary policie – Kriminalistický ústav a Útvar zvláštních činností, které se zabývají touto oblastí.

Vzhledem k tomu, že při detekci digitálních stop pro účely trestního řízení dochází k zásahům do práv a svobod občanů ČR, není možné, aby výše uvedené státní instituce pracovaly bez kontroly a bez využití jiných zákonů, než těch, které je zřizují.

V případě trestního řízení, kdy Policie ČR (zřízená zákonem o Polici ČR č. 273/2008 Sb, a na základě tohoto zákona provádí také vyšetřování trestné činnosti) chce využít detekci digitálních stop, musí si útvary policie vyžádat příslušné povolení u zodpovědného orgánu. Takovými orgány jsou:

a) příslušné **státní zastupitelství**, které vydává povolení podle trestního zákona 141/1961 Sb. Nejlepším příklad takového povolení je použití § 158d, odst. 2, který se týká sledování.

b) příslušný **soud**, který vydává povolení také podle trestního zákona 141/1961 Sb, ale v případech, kdy dochází k zásahům do soukromí nebo je vyšetřována zvlášť závažná trestná činnost. Zde uvádím jako příklad § 88a, týkající se poskytování informací od soukromých subjektů. Tyto soukromé subjekty (provider, operátor apod.) mají povinnost na základě zákona č.127/2005 Sb. o elektronických komunikacích vytvářet databáze v rozsahu vyhlášky č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě způsobu jejich předávání orgánům oprávněných k jejich využití. Tyto údaje jsou bezpochyby digitálními stopami a jejich využití je v dnešní době při vyšetřování trestné činnosti zcela běžné a mají také velmi vysokou důkazní hodnotu.

Zákon o elektronických komunikacích byl přijat v roce 2005 na základě aplikace pravidel EU a obecně se snažil vyhovovat standartizaci ETSI.[5] Bohužel už od jeho schválení jsou vedeny snahy o jeho novelizaci. Vyplývají z něj důležité skutečnosti, které mají mimo jiné usnadňovat detekci nezákonné činnosti a získávat potřebné důkazní prostředky. Nově jsou zaváděny především povinnosti provozovatelů sítí, které mají tuto činnost výrazně posílit.

[5] European Telecommunications Standards Institute- nezisková organizace, jejíž posláním je tvorba telekomunikačních norem cílených převážně na evropský region. Na její činnosti se podílí více než 900 organizací z 55 zemí. Byla založena v roce 1988 a jejími typickými členy jsou organizace věnující se administraci sítí, síťoví operátoři, výrobci IT produktů, poskytovatelé IT služeb, výzkumné organizace a také uživatelské organizace. Svou působností odpovídá organizaci ITU.

Jedná se především tyto povinnosti:

1. Používat normy a specifikace, jejichž seznam je uveřejňován v Úředním věstníku EU, pokud není zveřejněn, normy přijaté evropskými organizacemi pro normalizaci (§ 62 odst. 1 a 2 ZEK) i neveřejné sítě (Pro poskytování služeb, určování technických rozhraní a síťových funkcí v míře nezbytně nutné pro zabezpečení interoperability služeb a k rozšíření možností výběru pro uživatele).

2. Zajistit technicky a organizačně bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob v souladu se zvláštním právním předpisem, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob při poskytování této služby;

   zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací) vnitřní technicko-organizační předpis (§ 88 odst. 1 ZEK).

3. Zajistit důvěrnost zpráv a s nimi spojených provozních údajů. Zejména nepřipustí odposlech, ukládání nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez jejich souhlasu, pokud zákon nestanoví jinak. (TZ) (§ 89 odst. 1 ZEK)

4. Zajistit zpracovávání a ukládání provozních údajů, včetně příslušných lokalizačních údajů, vztahujících se k uživateli nebo účastníku;

   povinnost je smazat nebo učinit anonymními, jakmile již nejsou potřebné pro přenos zprávy (§ 90 odst. 2 ZEK).

5. odposlech a záznam zpráv - povinnost zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv (§ 97 odst. 1 ZEK).

6. povinnost uchovávat provozní údaje a na požádání je poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu (§ 97 odst. 3 ZEK) podrobnosti stanoví prováděcí předpis.

Povinnost uchovávat a za určitých okolností i předávat některé údaje měli operátoři už dříve. Novela, která do českého práva promítá nároky jedné z evropských směrnic, však jejich povinnosti rozšiřuje. Podobně jako telefonní hovory bude dokumentována i počítačová komunikace, data budou archivována půl roku[6]. Na rozdíl od většiny vyspělých zemí má však Policie České republiky, BIS[7] a VZ[8] povinnost tyto data platit. Ceník je stanoven zvláštní vyhláškou č.486/2005 Sb. Přesné údaje resp. výši úhrad se zjistit nepodařilo, nicméně za rok 2005 měla Policie ČR zaplatit kolem 300 miliónů korun a BIS přibližně 18 miliónů korun.

Z výše uvedeného je patrné, že útvary činné v trestním řízení získávají přístup k digitálním stopám pouze na základě zákona. Vlastní získávání těchto stop je ale různé a lze je obecně rozdělit na několik úrovní:

1. získání dat v rozsahu příslušného povolení od soukromého či státního subjektu přímo na základě zákonů ČR (telekomunikační data od operátorů a poskytovatelů telekomunikačních služeb)

2. získání dat v rozsahu příslušného povolení od osoby spolupracující s policií nebo policií vyškolenou a nasazenou do kriminálního prostředí

3. získání dat v rozsahu příslušného povolení se zabavených nebo jiným způsobem zajištěných technických zařízení

4. získání dat v rozsahu příslušného povolení z vytvoření dálkového přístupu skrytým proniknutím do kriminálního prostředí

[6] Vyhláška č. 485/2005 Sb. - o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Vydána Ministerstvem informatiky ve spolupráci s Ministerstvem vnitra

[7] Bezpečnostní informační služba (BIS), je česká státní zpravodajská služba s vnitřním polem působnosti (civilní kontrarozvědka)

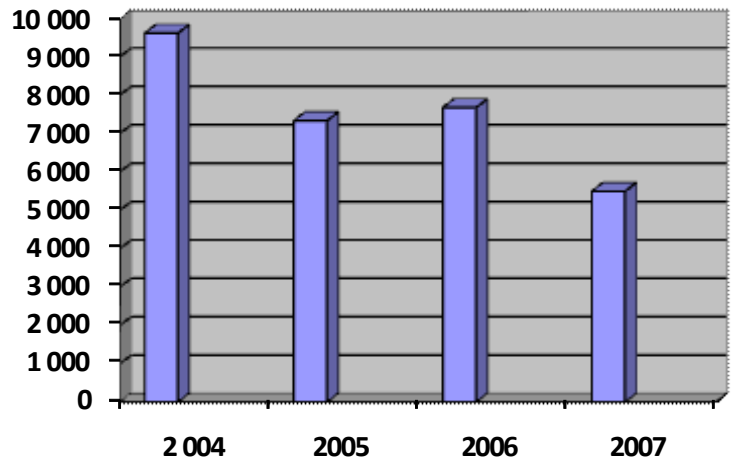
[8] Vojenské zpravodajství (zkr. VZ) je jednotná ozbrojená zpravodajská služba Armády České republiky. Zabezpečuje informace o možném vojenském ohrožení České republiky, o činnostech namířených proti obraně ČR a o činnostech ohrožujících utajované skutečnosti v oblasti obrany ČR. VZ vzniklo 1. ledna 2005 z Vojenského obranného zpravodajství a Vojenské zpravodajské služby. VZ působí jako rozvědná zpravodajská služba vně území republiky, ale své operace smí provádět i na území ČR.

Každé získání dat státním orgánem podléhá přísné kontrole. Například v případě odposlechu podle §88 zákona č. 141/1964 Sb, tedy získávání dat, které bezpochyby lze zařadit mezi digitální stopy, jsou to přímo poslanci parlamentu ČR. Bohužel nežijeme v ideální společnosti a i přes tuto přísnou kontrolu dochází k prozrazení postupů státních orgánů při vyšetřování trestné činnosti, čímž se stává to, že digitální stopa získaná složitým způsobem za využití technických prostředků je degradována a zpochybňována medií, nebo přímo osobou, která je za využití digitálních stop usvědčována.

Vývoj využívání telefonních odposlechů Policií České republiky v letech 2004 až 2007 je graficky znázorněn na Obrázku 3 a v Tabulce 1. Z něho vyplývá výrazný meziroční pokles 28% v období mezi roky 2006 a 2007 a pokles 43% za období 2004 až 2007 [14].

Rok	2 004	2005	2006	2007
Počet	9 610	7330	7672	5491

Tabulka 1. Počet odposlechů



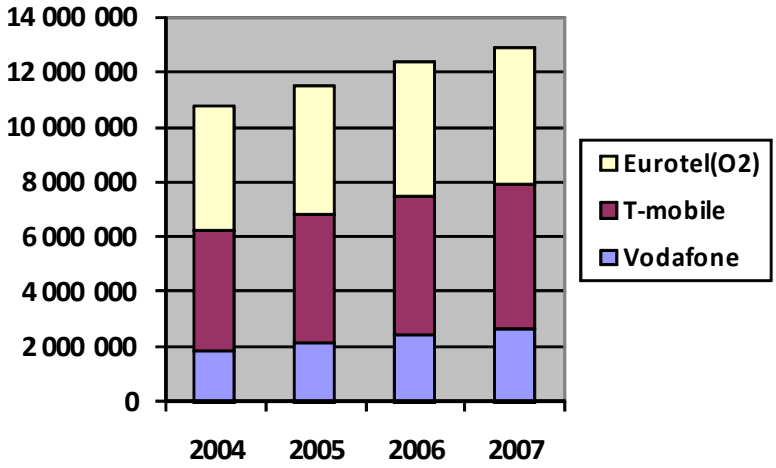
Obrázek 3. Grafické vyjádření počtu odposlechů v letech 2004 – 2007

Ze statistických údajů dále vyplývá, že v České republice byly v roce 2006 realizovány úkony dle § 88 t.ř. u 4386 osob, což je 0.04 % z celkového počtu obyvatel (použit údaj Českého statistického úřadu). V přepočtu na 10 000 obyvatel byly tedy použity úkony v průměru u 4 osob.

Přitom podle dalších níže uvedených statistik je zřejmý stále pokračující trend v nárůstu zákazníků jednotlivých operátorů (Tabulka 2 a Obrázek). Dále je nutno při hodnocení počtu odposlechů vzít do úvahy velký počet aktivních anonymních SIM karet, od kterého se už v ostatních zemích ustupuje (např. Německo, Španělsko, Itálie, Velká Británie, Švýcarsko, Slovinsko). Oproti tomu se v České republice v roce 2008 podíl tarifních zákazníků pohyboval od 46% u T-Mobile do 51,8% u Vodafone.

	2004	2005	2006	2007
Vodafone	1 831 116	2 140 000	2 413 000	2660000
T-mobile	4 359 980	4 634 165	5 049 000	5271000
Eurotel(O2)	4 591 471	4 676 000	4 864 000	4960000
Celkem	10784571	11452170	12328006	12893007

Tabulka 2. Počet zákazníků jednotlivých operátorů



Obrázek 4. Počet zákazníků jednotlivých operátorů

Další podobné problémy vyvstávají v oblasti IT. Je to způsobeno vzrůstajícím počtem připojení k internetu a využívání IT obecně. Tento nárůst nastává ve všech oblastech – veřejné správy, soukromých podnicích i domácnostech. Dochází tím k nárůstu možných komunikačních kanálů co do počtu, nárůstu možných druhů IT využívaného k páchání informační kriminality a také nárůstu možných typů a způsobů komunikace. Informační kriminalita tak může být páchána z nejrůznějších míst (práce, internetových kaváren, domácnosti a podobně).

Ve *Zprávě o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky* [17] v roce 2007 se také uvádí:

„*Rovněž došlo k rozdílnému výkladu manipulace s obsahem v internetu, a to ve smyslu zákona o elektronických komunikacích, kde jsou dány i povinnosti držení logových údajů a předávání těchto orgánům činným v trestním řízení. V některých ohledech vznikl rozdílný právní výklad, který poukazuje na možnost postupovat ve smyslu zákona o některých službách informační společnosti. Poskytovatel, který realizuje provoz např. e-mailového serveru a nezajišťuje připojení do internetu, není dle stanoviska Českého telekomunikačního úřadu vázán povinnostmi zákona o elektronické komunikaci a vztahuje se na něj pouze zákon o některých službách informační společnosti. Stanovisko Českého telekomunikačního úřadu hovoří o tom, že veškeré informace, jejichž držení a předávání stanoví zákon o elektronických komunikacích, je povinen uchovávat a předávat subjekt, který zajišťuje koncovému subjektu (který například provozuje poskytování elektronické pošty) konektivitu do internetu. Nastává tak patová situace zabraňující přístupu k některým údajům o proběhlé komunikaci v internetu. Daný stav je alarmující a je nutno přijmout opatření k jeho nápravě, nejlépe změnou zákona tak, aby nedošlo k ohrožení záměru přístupu oprávněných subjektů k logovým informacím.*“

Problémy nastávají i při páchaní trestné činnosti páchané prostřednictvím nebo s využitím internetové sítě. Českým specifikem je totiž připojení k internetu pomocí Wifi sítí, které je u nás masově rozšířeno nejen ve větších městech. Wifi připojení je

poskytováno nejrůznějšími providery a soukromými osobami používající často velmi odlišné technologie. Při vyšetřování trestné činnosti je pak i přes existenci zákona o elektronických komunikacích a z něho vyplývajících povinností, téměř nemožné od takového providera získat potřebné informace – digitální stopy. Těmi hlavními důvody zde bývá nedostatečné technické vybavení providera nebo možné odhaleni resp. prozrazení samotného vyšetřování a tím zmaření samotného úkonu.

V České republice mělo v listopadu 2008 připojení k internetu 32 procent domácností[16] a na jaře 2008 mělo přes 90% domácích počítačů v ČR možnost připojit se k Internetu. Nejrozšířenějším typem připojení v domácnostech bylo bezdrátové (36%), nejčastěji realizované technologií WiFi, následované pevnou telefonní linkou s ADSL (25%) a kabelovou televizí (23%). Připojení prostřednictvím mobilního telefonu vykázalo pouze 5% a kdysi nejvyužívanější technologie dial-up (vytáčené připojení) zanedbatelné 2%. Nejvíce počítačů bylo připojeno rychlostí 2 Mbit/s (20%) a 4 Mbit/s (19%), uživatelů s rychlostí do 1 Mbit/s bylo 36%. 14 % uživatelů internetu si není vědomo, jakou rychlost internetu používají.

Rychlost připojení v domácnostech byla poskytovateli internetu průběžně navyšována. V roce 2007 disponovalo rychlostí 2 Mbit/s a vyšší 36% uživatelů, v září 2008 se tento podíl zvýšil již na 51%.

5.4.2. Tradiční metody detekce digitálních stop

Ohledání místa činu – „*Místem činu je ta část prostoru, kde se uskutečnil děj, o kterém je možné podle jeho vnějších projevů předpokládat, že se jedná o proces protispolečenský, a u kterého je potřeba zjistit a zajistit takové znaky jednání, podle kterých by bylo možno věrohodně posoudit, zda se jedná o trestný čin.*

Ohledání místa činu je specifická kriminalistická metoda, kterou se na základě bezprostředního pozorování zkoumá, hodnotí a podchycuje materiální situace nebo jiný stav objektů, majících vztah k prověřované události, za účelem poznání a získání důkazů, jakož i dalších informací důležitých pro trestní řízení. „[21]

Domovní prohlídka a prohlídka jiných prostor - provádí se obdobně jako ohledání místa činu, na rozdíl od ní je zásahem do základních lidských práv a svobod. Velký důraz se také zde klade na pořízení dokumentace. Zkoumají se všechny skutečnosti, které mají souvislost s vyšetřovanou událostí. V případě informační kriminality se klade důraz především na IT techniku, digitální nosiče dat, záznamová media, apod.

Vydání nebo odnětí věci – „Kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat. Při vyzvání je třeba ho upozornit na to, že nevyhoví-li výzvě, může mu být věc odňata, jakož i na jiné následky nevyhovění.“[21]

5.5. Vyhotovení duplikátu digitální stopy

V případě monitorování IS resp. KS je výstupem obsahující digitální stopy obvykle datový objekt. Prakticky to jsou soubory – digitální data – audio, video nahrávky, soubory obsahující logovací data, výpisy dat a podobně. Ty jsou pak přenášeny a archivovány na fyzických objektech – CD, DVD, pevné disky, USB disky atd.

V případě tradičních metod jsou to většinou originály fyzických objektů:

- pevné disky konkrétního počítače, notebooku či jiného zařízení jako záznamového zařízení ukládajícího video signál z bezpečnostních kamer
- CD, DVD, USB disky a jiné
- PDA, mobilní telefony, …

– Jiné paměťová média, jednoúčelové zařízení (routery, palubní počítače vozidel,…)

U těchto originálů je nutné z důvodu zajištění autentičnosti a nedotknutelnosti dané digitální stopy (pro případ její možné změny-přepisu jinými daty) zajistit duplikát digitální stopy. Originál by totiž mohl být při analýze, archivaci nebo přepravě změněn, poškozen či jinak upraven a tím by byl pro trestní řízení jako důkaz nepřípustný.

Pokud se zaměříme na nejčastější vyhotovování duplikátů digitálních stop, jedná se nejvíce o takzvané otisky pevný disků. Existuje samozřejmě více možností a nástrojů, kterými lze požadovaného výsledku dosáhnout. Základním předpokladem použitelnosti je funkce kopírování **sector to sector** (sektor po sektoru) – tedy přesná reprodukce 1:1, nejen kopie dat. Používají se buď speciální HW zařízení, nebo je řešení softwarové.

5.5.1 Ninja versus EASEUS Disk Copy

Hardwarové zařízení **Ninja:121 IT & Forensic Cloning** je vyráběno a distribuováno japonskou firmou YEC Co, Ltd. (http://www.yec-usa.com) ve spolupráci americkou firmou STORAGEHEAVEN (www.storageheaven.com). Firmy se zabývají především vývojem, výrobou a prodejem zařízení sloužícím ke kopírování a klonování pevných disků, optických paměťových medií (CD, DVD) a páskových pamětí.

Mezi základní vlastnosti a funkce zařízení NINJA patří:

- Podpora pevných disků SATA / ATA / IDE 2,5 "- 1,8" - 1,0 "- 0,85"
- Přenosová rychlost až 4GB/min.
- Detekce hesla pevného disku

- Vytvoření kontrolního součtu MH5 Hash

- Funkce testování, klonování, kopírování, mazání

- Možnost „přeskakování“ chybných resp. vadných sektorů disku – tím je zajištěna práce i do určité míry vadnými disky

Obrázek 5. Ninja:121 IT & Forensic Cloning

(Zdroj :http://www.storageheaven.com)

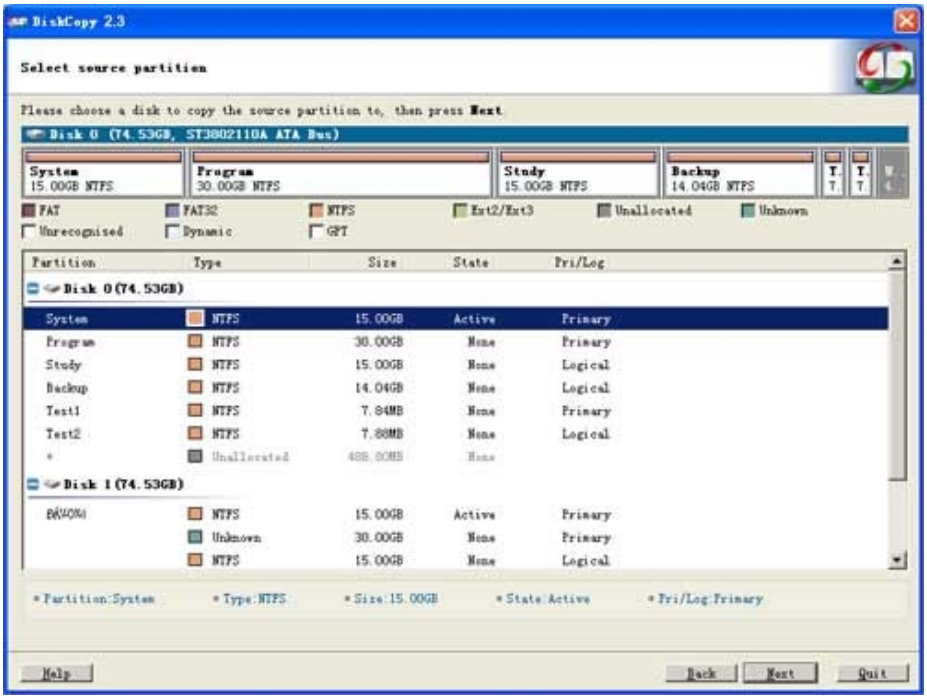
Software **EASEUS Disk Copy** verze 2.3 byl vyvinut čínskou firmy CHENGDU YIWO Tech Development Co., Ltd.(http://www.easeus.com) založenou v roce 2004. Hlavní činností firmy je vývoj a distribuce software pro profesionální zálohování a zabezpečení dat.

Mezi základní rysy SW EASEUS Disk Copy patří:

- Bootovaní z CD/DVD mechaniky, jádro převzaté z Linuxu

- Jednoduché a přehledné uživatelské prostředí

- Podpora pevných disků do velikosti 1TB



Obrázek 6. Uživatelské rozhraní programu Easeus Disk Copy

(zdroj: http://www.easeus.com/disk-copy/screenshot.htm)

5.5.2. Průběh testování, naměřené hodnoty

K testování byly dva různé pevné disky (originály digitální stopy):

- starší typ Maxtor, 40GB, 8MB cache, 7200 ot/min., IDE
- novější typ Western Digital 320GB, 16MB cache, 7200 ot/min. SATA II

Dále byly u SW EASEUS Disk Copy použity dvě rozdílně výkonné PC stanice:

1. PC **Lemonway** - procesor Duron 900MHz, mainboard VIA KT266, 256 MB RAM paměti, rozhraní pro připojení pevných disků IDE
2. PC **HP** – procesor Intel CoreDuo 2.6GHz, mainboard ASUS P5KC, 2GB RAM paměti, rozhraní SATA

Při vyhotovování duplikátů digitální stopy byl jako cílový pevný disk zvolen Western Digital 400GB, 16MB cache, 7200 ot/min, rozhraní SATA II. Tím jsou splněny základní podmínky pro vytváření duplikátu pevného disku – cílový pevný disk musí mít stejnou nebo vetší velikost proti disku cílovému. Byly vytvořeny stejné podmínky pro oba způsoby vyhotovování duplikátu – HW i SW, bylo také vyloučeno možné ovlivnění měření, které by mohlo nastat při použití jiného „pomalejšího“ pevného disku.

U měření - tvorby duplikátů pevného disku pomocí SW EASEUS byl navíc pro každé měření připojen cílový disk dvěma různými způsoby:

1. Cílový pevný disk připojen přímo přes IDE resp. SATA rozhraní u PC stanice **Lemonway** resp. **HP**
2. Cílový pevný disk připojen prostřednictvím dokovací stanice - rozhraní USB 2.0 (dále označen *)

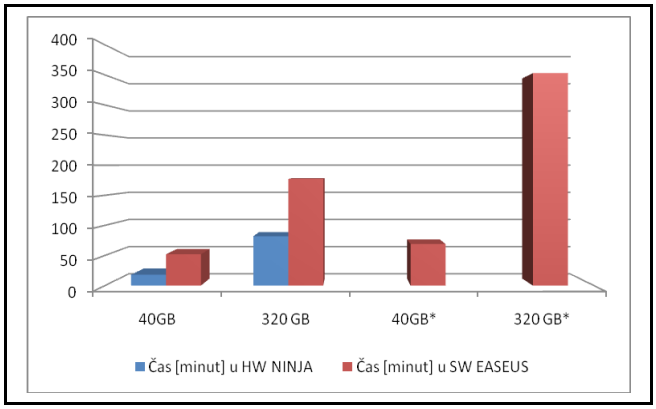
Naměřené hodnoty:

	40GB	320 GB
Čas [minut]	18	82
Přenos. rychlost [GB/min.]	2,15	3,6

Tabulka 3. Průměrné hodnoty dvou měření na HW NINJA

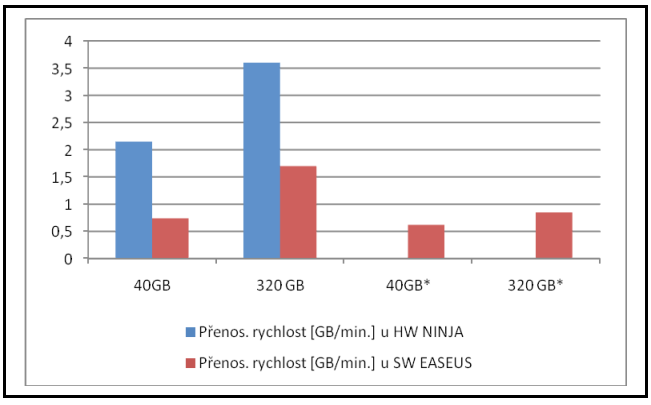
	PC Lemonway		PC HP	
	40GB	40GB*	320GB	320GB*
Čas [minut]	52	69	176	353
Přenos. rychlost [GB/min.]	0,74	0,62	1,7	0,85

Tabulka 4. Průměrné hodnoty dvou měření – SW EASEUS



Obrázek 7. Srovnání časové náročnosti

K porovnání byly vybrány dvě různé počítačové sestavy záměrně. Z předchozích praktických zkušeností byly značné rozdíly v časové náročnosti předpokládány. Také se tím potvrdila stejná závislost obou metod – přenosovou rychlost přímo ovlivňují nejen parametry samotného pevného disku (ot./min., velikost cache), ale u SW metody i použitý hardware celkově (velikost RAM, rychlost procesoru, sběrnice,..). To je také patrné z následujícího grafu.



Obrázek 8. Srovnání přenosových rychlostí

5.5.3. Vyhodnocení testování

Z naměřených hodnot je zřejmá naprostá převaha pořízení HW zařízení NINJA. Tedy pokud se zaměříme pouze na přenosovou rychlost, potažmo časovou náročnost. Ze subjektivního hlediska – hlediska operátora však mohu pochválit kvalitní výsledky, jednoduchost a spolehlivost obou zařízení. Obě zařízení mají navíc další funkce a možnosti, které ale nebyly předmětem testování. Jejich použití (testování disků, kopírování jednotlivých oddílů disků a další funkce) je využitelné až při další následné analýze pevných disků nebo při jejich komerčním využití.

Výhodou SW EASEUS Disk Copy je možnost vytváření duplikátů digitálních stop u pevných disků pracujících v některých typech RAID polích.

Hlavní rozdílnosti a omezení použitelnosti HW a SW metod:

- U HW zařízení je potřeba pevný disk ze zařízení (PC stanice, notebook,…) vyjmout.
- U SW metody lze EASEUS Disk Copy spustit (nabootovat) v dané zkoumané PC stanici resp. notebooku. Tím se zpřístupní všechny pevné disky i disky připojené v hardwarovém RAID poli. Omezením je nutnost spuštění bootovaní sekvence z CD/DVD mechaniky nebo USB (PC stanice nemusí mít optickou mechaniku nebo USB, nebo může být přístup k výběru bootovaní chráněn heslem). Digitální stopy se pak reprodukují na cílový disk připojený například prostřednictvím USB rozhraní.
- Pokud je nutné u práce s SW EASEUS Disk Copy vyjmout originální pevný disk (originál pevného disku není v PC, ale v jiném zařízení se zápisem dat na pevný disk, nebo z jiného výše popsaného důvodu), je možné vyrobit duplikát pevného disku jen po připojení k jinému PC nebo notebooku.

Z ekonomického hlediska je pak srovnání obou produktů složitější. Jako hlavním kritériem se mohou jevit jejich pořizovací náklady – SW EASEUS Disk Copy je totiž

distribuován jako freeware[9] i pro komerční využití. Na druhou stranu je k němu ve výše vyjmenovaných případech nutné pořídit podpůrný notebook nebo počítač a sadu propojovacích kabelů, redukcí pro připojení pevných disků.

	Ninja:121 IT	EASEUS Disk Copy
Pořizovací náklady	40 000 Kč	0 Kč
Kabely/redukce	7 000 Kč	2 000 Kč
Notebook	0 Kč	20 000 Kč
Celkem	47 000 Kč	22 000 Kč

Tabulka 5. Základní náklady na pořízení nezbytného vybavení

Dalšími náklady jsou mzdové náklady na práci technika nebo znalce. Při odhadu jsem vycházel z obecné hodinové sazby účtované soudními znalci v oboru IT. U HW zařízením NINJA je potřebná doba zaokrouhlena pro zjednodušení na 2 hodiny a u SW EASEUS na 6 hodin.

	HW NINJA	SW EASEUS
Práce technika/znalce	2 hodiny	6 hodin
1 hod. cca 2000,-Kč	4 000 Kč	12 000 Kč

Tabulka 6. Odhadované mzdové náklady

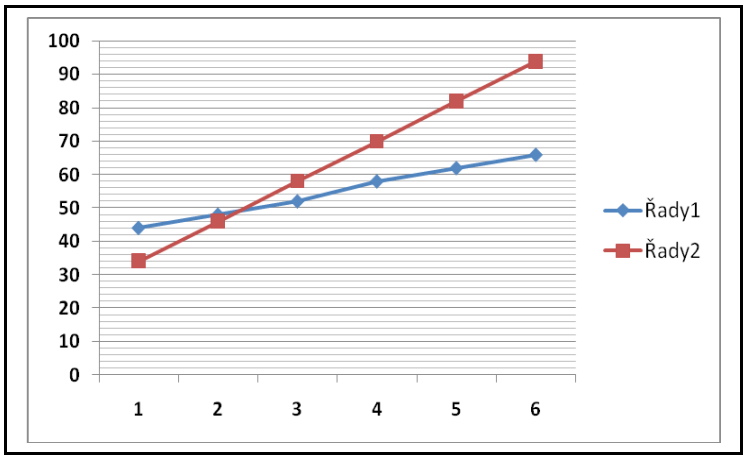
V další tabulce jsou srovnávány celkové náklady. Fixními náklady jsou náklady na pořízení HW nebo SW technologie, variabilními pro zjednodušení pouze mzdové náklady na práci technika resp. znalce. Celkové náklady jsou sledovány v závislosti na vzrůstajícím počtu duplikovaných disků. Opět je za základní jednotku, originál digitální stopy, zvolen měřený pevný disk o kapacitě 320GB.

[9] Freeware je software, který je distribuován bezplatně (či za symbolickou odměnu). Autor si u freeware ponechává autorská práva, například nedovoluje program upravovat nebo omezuje použití zdarma jen pro nekomerční či osobní potřebu

	320GB/NINJA [ks]	320GB/EASEUS [ks]
Vstupní náklady	40	22
Počet disků 320GB		
1	44	34
2	48	46
3	52	58
4	58	70
5	62	82
6	66	94

Tabulka 7. Srovnání fixních a variabilních nákladů

(náklady v tis. Kč)



Obrázek 9. Grafické vyjádření srovnání celkových nákladů

Z naznačených charakteristik je patrné, že od počtu tří pevných disků je ekonomicky výhodnějším řešením pořizování duplikátů pevných disků pomocí HW zařízení NINJA. Tato premisa však platí jen za určitých předpokladů. Mohou nastat případy, kdy se například:

- Sníží fixní náklady u SW metody používáním stávající IT techniky (notebooku, počítače)

- V praxi jsou běžné případy, kdy je nezbytné zpracovat – vyhotovit duplikáty několika pevných disků současně a navíc jsme limitováni určitým časem. V tom případě by pořízení většího množství HW zařízení NINJA bylo nevýhodné. Naopak náklady na vyrobení bootovatelného CD jsou zanedbatelné. A pokud je pak možné využít k duplikaci stávající počítače, je finanční úspora značná.

Proto by se měla před prvotními investicemi provést analýza, která by zhodnotila skutečnou potřebu, využitelnost a časovou vytíženost daného technologického řešení. Může se ale říci, že se vzrůstajícími kapacitami pevných disků bude výhoda rychlejšího HW zařízení růst také. Představa, že bychom duplikovali SW metodou 2TB disk SW metodou minimálně 21 hodin, je odstrašující. HW metodou bylo zapotřebí kolem 9 hodin.

Uvědomuji si, že uvedené náklady na mzdy a materiál vycházejí především z kvalifikovaného odhadu. Pro potřeby tohoto srovnání je ale považují za relevantní.

Je také samozřejmostí, že existuje více HW a SW řešení (Clonezzila, DiskDoubler,…) s různými možnostmi použitelnosti a rozdílných cenových relací. Přenosové rychlosti jsou však u všech obdobné. Zásadní nedostatky u ostatních produktů spatřuji v jejich omezeném využití a příliš složité následné analýze dat. Duplikáty pevných disků pořízených HW NINJA nebo SW EASEUS lze totiž přímo připojit do počítače, lze z nich spouštět systém a pracovat na nich jako na originální PC stanici. To ostatní zařízení ne vždy umožňují, analýza je pak výrazně složitější a musí k ní být použito zvláštní softwarové vybavení.

5.6. Analýza dat

S detekcí nezákonné činnosti úzce souvisí analýza získaných digitálních stop, která slouží k vyhodnocení relevantnosti a použitelnosti stop jako důkazního prostředku. Analýza je obvykle dalším navazujícím úkonem.

Vzhledem k tomu, že problematika informační kriminality zasahuje do všech oblastí života, je i problematika analýzy digitálních stop rozsáhlá. Z kriminalistického hlediska zasahuje téměř do všech oblastí (daktyloskopie, mechaniky, trasologie, IT, biologie,…). K vyhledávání nelegálních kopií filmů a hudebních děl jsou při raziích na tržnicích nasazováni i speciálně vycvičení psi.

Pokud jde o samotnou analýzu dat – tedy vyhodnocení datových objektů, provádí se nejen na specializovaných pracovištích Policie ČR (zastřešujícím pracovištěm je zde Kriminalistický ústav). Vyhodnocení mohou provádět také znalci nebo znalecké ústavy a v komerční sféře pak forenzní pracoviště.

U počítačových dat je využívána výpočetní technika, analyzují se převáženě nosiče dat. Právě k tomu jsou využívány duplikáty digitálních dat. Pokud jsou předmětem zkoumání pevné disky počítačů, je samotná metodika analýzy zaměřená na zjištění důkazních materiálů ke konkrétní trestné činnosti. U porušování autorských práv je to legálnost použitého software, případně přítomnost nelegálních kopií, emailová nebo jiná komunikace pachatelů a podobně. U trestných činů hospodářské povahy to bývají databáze s účetními daty a tak podobně.

Je potřeba si uvědomit, že rozsah analýzy je obrovský a neustále se vyvíjí. To souvisí se stálým vývojem nejen na poli IT. Důkladná analýza je proto náročná nejen časově a technologicky, ale klade i velké nároky na znalosti a specializaci konkrétních pracovišť zabývajících se touto problematikou. Hlavním nedostatkem u represivních složek je nekvalitní technické vybavení, značná absence příslušných odborníků a také nedostatek vyškolených a věci znalých státních zástupců a soudců. Represivní složky pak bývají za pachateli většinou o krok pozadu.

6. Závěr

V diplomové práci jsem se vás pokusil seznámit se zajímavým a moderním tématem, které bude náš život ovlivňovat z důvodu technického rozvoje čím dál častěji. Popsal jsem základní pojmy týkající se problematiky a vysvětlil jsem souvislosti mezi nimi. Z teoretické části práce týkající se informační kriminality vyplývá, že dané téma je široké a má svá specifika, které je nutné respektovat.

Dále jsem se pokusil specifikovat problematiku digitálních stop, její zvláštnosti a uplatnění při odhalování a vyšetřování trestné činnosti. Důraz kladu nejen na samotnou technickou stránku věci, ale část pozornosti byla věnována i právním aspektům detekce nezákonné činnosti a detekce digitálních stop. Zdůrazněna byla také oblast prevence – oblast informační bezpečnosti. Zde spatřuji stále velký potenciál, který by mohl problém informační kriminality pomoci řešit.

V praktické části jsem provedl a vyhodnotil dva odlišné způsoby pořizování duplikátů digitálních stop – pevných disků. Zkoumání nebylo zaměřeno jen na zhodnocení použitelnosti a funkčnosti, ale v úvahu bylo bráno finanční posouzení celé záležitosti. Rozhodnutí zda využívat HW zařízení nebo duplikáty pevných disků vyrábět pomocí SW metody záleží na předpokládaném objemu práce. HW Ninja je výhodnější používat pro svou rychlost při větším počtu duplikovaných disků, SW EASEUS Disk Copy pak v případech jeho občasného využití.

Literatura:

[1] CASEY, E. Digital Evidence and Computer Crime,1st edition Academic Press Elsevier: London, UK, 2000.

[2] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat, 1. vyd. Computer Press: Brno, 2004.

[3] HLAVÁČEK, J., a kol. Kriminalistická počítačová expertiza. Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality, 1. vyd. Praha: Policejní akademie, 1997, str. 51–65, ISBN 80-85981-50-5.

[4] PORADA, V. Teorie kriminalistických stop a identifikace. 1. vyd. Academia: Praha, 1987.

[5] PORADA, V. a kol. Kriminalistika, 1. vyd. Cerm: Praha, 2001.

[6] PORADA, V., RAK, R. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. In: Karlovarská právní revue 4/2006, str. 1-21.

[7] PROSISE, Ch., MANDIA, K. Počítačový útok. Detekce, obrana a okamžitá náprava. 1. vyd. Computer Press: Praha, 2002.

[8] SVETLÍK, M. Počítačová kriminalita (takticko-technické otázky). Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality. 1. vyd. Policejní akademie: Praha, 1997.

[9] Digital Evidence: Standards and Principles. Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE).[on-line], http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[10] Zákon č. 140/1961 Sb. Trestní zákon,[on-line] http://www.pravnipredpisy.cz/predpisy/ZAKONY/1961/140961/Sb_140961_------_.php

[11] Martin Formánek, Forenzní analýza digitálních nosičů dat pro počítače, BP ČVUT FEL 2008

[12] RNDr. Dagmar Brechlerová: Řešení informační bezpečnosti, IT SYSTEMS 4/2005 [on-line],http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm

[13] Viruses and Spyware: Expected Costs, 24 August 2008, [on-line], http://www.defendingthekingdom.com/archives/viruses-and-spyware-expected-costs

[14] Zpráva Policejního prezidia, Praha 26. června 2007, [on-line], web.mvcr.cz/archiv2008/dokument/2007/odposlechy/zprava.doc

[15] ČSÚ, Informační společnost v číslech 2008, [on-line], str 10, http://www.czso.cz/csu/redakce.nsf/i/c_podniky_is08/$File/is08_c.pdf

[16] Fakta na dosah, Tiskové zprávy, Michal Peca 26.9.2008,[on-line] http://www.factum.cz/tz319

[17] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2007, MVCR Praha 2008, [on-line], http://aplikace.mvcr.cz/archiv2008/dokument/2008/verejnyporadek/zprava08.pdf

[18] M.Matějka, Počítačová kriminalita, ComputerPress, Praha, 2002, 1. vydání, str. 8,9

[19] V. Paukertová, Elektronická informační kriminalita, UK Filozofická fakulta, Praha 2006

[20] V. Smejkal, Současný stav počítačové kriminality, jejího odhalování, vyšetřování a prevence proti ní, Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality. 1. vyd. Policejní akademie: Praha, 1997.

[21] Zákon č. 141/1961 Sb. Trestní řád (Zákon o trestním řízení soudním), [on-line], http://www.pravnipredpisy.cz/predpisy/ZAKONY/1961/141961/Sb_141961_------_.php