INSTITUT PRO KRIMINOLOGII A SOCIÁLNÍ PREVENCI

POČÍTAČOVÁ KRIMINALITA

Nástin problematiky

Kompendium názorů specialistů

Sestavil: RNDr. Stanislav Musil

Tento nástin nemá charakter oficiální publikace a je určen pouze pro interní studijní účely

Neprodejné

Praha 2000

ISBN 80-86008-80-0
© Institut pro kriminologii a sociální prevenci, 2000

Předmluva

Jedním z hlavních rysů současnosti je značný rozvoj informačních technologií a s tím spojené pronikání výpočetní techniky, nutně vybavené moderním softwarem, téměř do všech oblastí lidské činnosti, včetně každodenního života jednotlivců. Vývoj je tak rychlý, že nás nutí k soustavnému sledování nových informací, abychom předešli nežádoucím disproporcím mezi realitou a jejím poznáním. To platí i pro třídu negativních fenoménů, jdoucích ruku v ruce se zmíněným pokrokem, pro které se vžil souhrnný název *počítačová kriminalita.*

Do studie, pojaté jako stručný nástin aktuální problematiky související s tímto, jinak dosti neostrým pojmem, jsou zahrnuty některé nové projevy, implikované např. vznikem počítačových sítí (Internetu), realizací elektronického přenosu informací vůbec a nových možností studia osobnosti potenciálních pachatelů. Cílem sestavení tohoto materiálu je shrnutí poznatků a zkušeností, rozptýlených v nepřehledné paletě literárních pramenů. Neklademe si za cíl hodnotit či řešit nastíněné problémy, spíše jde o to, ukázat na závažnost, ale i složitost poznání daného jevu, upozornit na, do jisté míry ohraničené možnosti jeho zkoumání. V neposlední řadě pak též na otázky bezpečnostní informační politiky, boje s počítačovou kriminalitou, represe a prevence, v konkrétním i obecnějším pojetí.

Tento nástin byl sestaven z dostupných pramenů, seřazených v seznamu na konci textu. Odkazy na jednotlivé tituly jsou uvedeny v hranatých závorkách [..]. Omlouváme se za případnou neúplnost v citování poznatků a myšlenek jednotlivých specialistů, vynucenou omezeným rozsahem studie.

RNDr.Stanislav Musil

Obsah

strana

1. K vymezení pojmu počítačové kriminality

Čerpáno převážně z pramenů: [39], [102], [110], [111], [115], [136], [142], [188], [230].

1.1. Variabilita pojetí počítačové kriminality

Definovat ostřeji pojem počítačové kriminality není snadné. Nesnadnost vymezení počítačové kriminality je příčinou velké variability přístupů k vyjasnění a chápání tohoto pojmu. Počítačovou kriminalitu lze definovat nejobecněji např. jako každou nekalou činnost páchanou s pomocí počítačů. Pojem „nekalá činnost“ může být specifikována např. společenskou nebezpečností důsledků, které tato aktivita přináší. Což přichází v úvahu zejména v případech přestupků, trestných činů či obecně deliktů ve smyslu porušení platné zákonné úpravy. Takové vymezení je však jednak příliš široké, zahrnuje např. i banální machinace mzdové účetní, při kterých mění položky v počítači stejně jako by je měnila na jiném nosiči, jednak i úzké. Úzké v tom smyslu, že nepokrývá např. neautorizovanou distribuci softwarového vybavení počítače. Jedná se o produkty, k jejichž tvorbě je počítač sice nutný, avšak k jejich distribuci nikoliv, i když samozřejmě také použitelný.

Dalším možným přístupem je vymezení pojmu počítačové kriminality podle rozčlenění nekalých aktivit v souladu se studií [142]:

1) úmyslné útoky proti vlastnímu nosiči informace, případně proti datům v něm vloženým s úmyslem je zničit,

2) počítač jako prostředek obohacení formou

a) krádeže dat a programů,

b) krádeže strojového času,

c) nezákonné manipulace s počítačem, daty nebo programy.

Tato definice je poměrně funkční, i když nezahrnuje např. delikty nedbalostního charakteru, což se snaží napravit např. autor monografie [230] v definici jinak velmi podobné předchozímu vymezení. Jiným členěním je to, které přijala a ve svém materiálu publikuje Rada Evropy [115] ve formě

-minimálního seznamu aktivit:

1)počítačové podvody, včetně nedovolené manipulace 2)počítačová falzifikace, stíhaná podobně jako falzifikace tištěných dokumentů, 3)poškozování počítačových dat a programů, 4)počítačová sabotáž, včetně útoků proti hardwarovým prostředkům, 5)neoprávněný přístup (hacking, hackeři), 6)neoprávněný průnik, včetně neoprávněného používání komunikačních sítí počítačů a přístupu k datům jejich prostřednictvím, 7)neoprávněné kopírování autorsky chráněného programu, 8)neoprávněné kopírování topografie, včetně ochrany čipů;

-volitelného seznamu aktivit:

1)změna v datech nebo počítačových programech ve významu změn především bez finančního profitu, kdy však může dojít k dalekosáhlým následkům, např. při zpracování osobních dat apod., 2)počítačová špionáž, především zneužíváním průmyslového a obchodního tajemství, 3) neoprávněné užívání autorsky chráněného programu.

Význam této definice spočívá ve snaze o pokus adekvátního sjednocení legislativy evropských zemí ve vztahu k počítačové kriminalitě. Toto sjednocení je žádoucí, a to nejen v evropském, nýbrž i v celosvětovém měřítku, vzhledem k mezinárodnímu charakteru některých forem počítačové kriminality, které zejména v poslední době nabývají na intenzitě. Skutečnost, že některá trestná činnost v jednom státě by nebyla postižitelnou v zemi jiné při propojení počítačů např. telefonní sítí, by samozřejmě pachatele nežádoucím způsobem velmi motivovalo.

Další možné pojetí třídění aktivit podle [142]: 1)útok směřující ke zničení počítače nebo dat, 2)útok směřující ke zneužití dat, ať již ze zištných nebo nezištných důvodů, 3)porušení autorských práv jednak využitím software pro svou potřebu, jednak realizací nezákonné distribuce software, 4)zneužití strojového času.

Jde o třídění velmi praktické, které by zasluhovalo doplnit pouze v bodě 3) o zneužití software též pro služební účely.

**

Lapidárně, z pozic policejní represe, přistupuje k pojetí počítačové kriminality např. autor pojednání [39]. Podle něho je počítačová kriminalita, mnohdy i přes své nesporné prvky moderních technologií, jen jinou tváří různých standardních trestných činů. Co jiného než krádež je podvodné převedení peněz z cizího účtu na pachatelův nebo uveřejňování pedofilních obrázků na Internetu, které je obdobou různých pokoutně šířených tiskovin. Nejinak je tomu s aktivitami různých extremistických hnutí a skupin, například s neonacisty. Jde pouze o jinou formu, ale obsah je stejný. Obecně počítačová kriminalita představuje velkou množinu všech kriminálních aktivit, spojených s počítačem jako nástrojem, případně s počítačem jako cílem trestné činnosti. Protože svou šíří zasahuje řadu oblastí lidské činnosti a tedy i různé trestné činy od krádeží peněz po počítačové pirátství, nemůže proti počítačové kriminalitě existovat ani jednotný způsob boje. Jak vzdálené jsou si pedofilní aktivity na Internetu od prorážení obranných software různých databází! I z toho důvodu nelze říci, že je počítačová kriminalita jakýmsi ryze samostatným trestním světem. Jednotlivé trestné činy šetří a objasňují policisté zařazení na těch pracovištích, která je mají v popisu práce. Pornografii řeší mravnostní pracoviště, fiktivní převody nebo krádeže peněz hospodářská kriminálka, zaměřená na podvody, a počítačové pirátství jako útok na duševní vlastnictví také pracoviště hospodářské kriminality. Takovýto přístup k pojmu počítačové kriminality však není jakýmsi ignorováním moderního světa, ale odrazem toho, že není třeba přičítat věcem jiný význam než ve skutečnosti mají. Téměř každou formu počítačové kriminality lze totiž zařadit do již existujících kategorií. Z pohledu policejní represe je spíše nutné rozšiřovat kvalifikaci kriminalistů a zaměřit je na nové formy trestné činnosti, než vytvářet nové struktury, úzce profilované pro malou část kriminality. Jinak ovšem existují trestné činy, které nelze pojímat podle nějaké historické šablony. Například tzv. *hacking*, tedy překonávání ochranných softwarových prvků různých databází apod. Je to skutečně formálně i obsahově novum, kdy někdo pronikne systémem, do světové sítě (např. do Internetu) a pozměněním určitých dat poškodí tak informace poskytované sítí. Nebylo zatím obvyklé, aby se trestná

činnost uskutečňovala bez fyzické přítomnosti na místě činu. Pachatel může být doslova na druhém konci planety, a přesto svůj čin realizuje současně u nás. K tomu je samozřejmě potřeba velmi dobrého technického vybavení i značných intelektuálních schopností, především ale jistého kriminálního myšlení. Nepominutelnou stránkou počítačové kriminality a především softwarového pirátství jsou následné finanční důsledky. Velké softwarové firmy odhadují své škody jen na území naší republiky na mnoho miliard korun. Uvedenou částku lze považovat za polemickou, ale přesto je možné tvrdit, že finanční ztráty výrobců software u nás dosahují obrovských částek. Typickým příkladem je *INFOMAPA,* at' už Prahy nebo celé republiky. Společnost, která ji vymyslela, vytvořila a prodává, neustále se potýká s problémy ohledně minimálních příjmů z prodeje licencí. Přitom její produkt je velmi dokonalý, s nemalými finančními náklady vyvinutý a velmi žádaný. Má ho dnes téměř každý uživatel a tak by příslušná firma mohla být bez problémů na špičce softwarových firem. Není tomu tak proto, že většina uživatelů má tento software získaný nelegálně. V podstatě se dá říci, že i přes obrovskou kapacitu chytrých a operativně schopných tuzemských programátorů se málokdo pustí do podnikání v této oblasti, protože propast mezi očekávanými a skutečnými příjmy je nakonec tak veliká, že jí překonávají pouze softwaroví giganti se silným zahraničním kapitálovým zázemím. Za to jsou podle autora [39] odpovědni všichni ti, kteří bez jakéhokoli studu kradou počítačové programy a užívají je s přesvědčením, že je to správné, a pokud ne, tak je za to stejně nikdo nechytí. Čas však pokročil, dříve či později mnozí softwaroví piráti zjistí, že zákon platí i pro ně se všemi adekvátními důsledky.

**

Autor stati [110] rozšiřuje pojem počítačové kriminality na *kriminalitu informační*. Počítačová kriminalita je jistě výrazným jevem dnešní doby, ale zájem o informace, byt' byly zpracovávány, přenášeny a uchovávány jiným způsobem, je mnohem staršího data. Byli jsme jen zvyklí, a stále tak to i chápeme, tyto jevy nazývat jinými pojmy (vyzvídání, vyzrazování atd.), zejména podle způsobu uplatnění informací. To ostatně platí obecně dodnes. S postupně stále se rozšiřujícím zaváděním výpočetní techniky rostla a roste však míra jejího zneužívání a do jisté míry zastiňuje klasické formy práce s informacemi a jejich zneužívání. Z toho vyplývá, že bychom spíše měli hovořit o *informační kriminalitě,* kterou chápeme jako pojem širší než kriminalita počítačová. Zdá se to být rozumné v tom případě, když se na trestnou činnost díváme z hlediska informačního pojetí. Ale to v běžné, např. policejní praxi není obvyklé. Pro orgány činné v trestním řízení je určujícím hlediskem trestní zákon a jeho jednotlivá ustanovení. Je velmi pravděpodobné, že v budoucnu, kdy budou nejen převažovat, ale možná výlučně zůstanou k dispozici jen prostředky informační technologie, budeme hovořit pouze o kriminalitě počítačové. Přísně odborně vzato by tomu tak nyní být nemělo, ale vžitý termín jen tak jednoduše nezměníme. Zůstáváme tedy zatím u pojmu počítačová kriminalita ve významu deliktů páchaných v souvislosti s výpočetní technikou.

Autor studie [110] podává dále *obecnou charakteristiku počítačové kriminality* z pohledu policejní praxe. Podle něho jsou případy počítačové kriminality obvykle provázeny nedostatkem klasických důkazních materiálů. Týká se to zejména listinných důkazů, na jejichž místo nastupují záznamy informací na informačních nosičích, pokud se je ovšem podaří

získat. Také přenosy informací pomocí výpočetní techniky se ve většině případů provádějí bez potřebné dokumentace, pouze prostřednictvím elektromagnetických impulsů. Stanovení výše škody vzniklé trestnou činností je pak většinou velmi složité. Počítačová kriminalita může postihnout značnou šíři osobního i společenského života. Výpočetní technika je nasazena do řízení a správy státu, v armádě, policii, ekonomice, průmyslu i zemědělství, ve zdravotnictví a jinde. V počítačových systémech jednotlivých institucí se soustřeďují informace ze všech oblastí života společnosti i jednotlivce. Proto poškození funkce počítačových systémů, nejen celostátně budovaných, ale i lokálních, může vést k dezorganizaci v mnoha sférách lidské činnosti. Nezanedbatelné je také stále vzrůstající využívání soukromých osobních počítačů a jejich zapojení do počítačových sítí. Prostřednictvím počítačů je možné sledovat informace, vyhodnocovat získané informace, dotazovat se v mnohdy rozsáhlých informačních databázích, které mohou být navíc vzájemně propojeny. V současné době není žádnou zvláštností přenos informací mezi jednotlivými státy a mezi jednotlivými kontinenty. Vedle nesporného přínosu, který znamená zavádění výpočetní techniky pro společnost i jednotlivce, mohou počítače představovat určité potenciální i reálné nebezpečí. Potenciálními obětmi trestné činnosti páchané pomocí výpočetní techniky jsou všechny organizace a osoby, které počítače používají nebo jsou registrovány v počítačových sítích.

Podle [110] pro vlastní klasifikaci počítačové (informační) kriminality lze vyjít ze systémového pojetí jevů nebo názorněji z pozice pachatele a jeho cíle. Ten může mít zájem o předmět v této oblasti: (1) získat výpočetní technický prostředek, (2) získat obsah, tj. informace (data) na prostředku uložená, (3) získat obojí. Ve všech třech případech lze klasifikovat: způsob spáchání (jak pachatel chce dosáhnout svého cíle získat předmět, objekt zájmu), jaká byla nebo je jeho motivace (proč čin uskutečnil), eventuálně jaké důsledky mělo jeho jednání pro poškozeného. Cílem pachatele může být

-jednorázově prodat technické výpočetní prostředky, eventuálně zpeněžit získaná data,

-prodávat vícenásobně data a informace, získaného programové vybavení, či získaných informací a dat eventuálně využívat k páchání další trestné činnosti (např. vydírání, šíření poplašných zpráv, dezinformací apod.),

-neoprávněné využívání technických prostředků k vlastní komerční činnosti (mimo jiné i k návodům jiné trestné činnosti, provozování nepoctivých her ap.),

-předání získaných dat a informací jinému subjektu k jeho využití profesionálně nebo za úplatu (vyzvědačství apod.),

-jiné nespecifikované nebo komplexní užití.

K problematice počítačové kriminality pro potřeby specializované výuky autor [102] probírá otázky vhodné definice, zabývá se možnostmi trestního postihu podle stávající právní úpravy, dále pak problémy metod ochrany výpočetní techniky a prevence. Říká, že výpočetní technika a automatizovaný systém zpracování dat, stejně jako jiné materiální výsledky lidské činnosti vytvářejí podmínky i pro páchání trestné činnosti. V zásadě jde o objektivní faktory, které umožňují páchání trestné činnosti tím, že jsou buď prostředkem ke spáchání trestného činu nebo jsou předmětem útoku ze strany pachatele. Zdůrazňuje, že počítačová kriminalita je považována za nejnebezpečnější kriminální činnost vedle prodeje drog a prostituce, neboť

výpočetní techniky je využíváno k vydírání, krádežím, podvodům a dokonce i k páchání sexuálních deliktů. Úmyslná manipulace v automatizovaném systému zpracování dat může přivodit rozsáhlé katastrofy. I takové případy již byly zjištěny. Jednalo se o narušení řídících systémů v železniční a letecké dopravě. Základní příčinou využívání počítačů k trestné činnosti je především skutečnost, že výpočetní technika i automatizovaný systém zpracování informací jsou fenomény ovládající v současné době řadu oblastí společenského života. Výpočetní technika je využívána pro svou vysokou efektivnost při zpracovávání informací a pro schopnost zabezpečovat optimalizaci řídících procesů. Zvyšování významu výpočetní techniky ve společnosti je vysoce rozporuplným procesem. Na jedné straně se projevuje snaha o nejširší využívání výpočetní techniky, na straně druhé však vidíme, že celá řada oblastí, v nichž výpočetní technika zevšedněla, se stává zranitelnější z důvodu možných chyb ze strany obsluhujícího personálu, stejně jako z příčin jejího úmyslného poškozování či neoprávněných manipulací. Samostatný problém tvoří pak otázky přenosu dat, kdy vzájemné propojení počítačů dovoluje vytváření rozsáhlých automatizovaných systémů zpracování dat. Tyto systémy jsou vysoce účinné, nicméně je problematické zajistit jejich ochranu.

Při snaze o vymezení pojmu *počítačová kriminalita* autor [102] uvádí, že je možno vycházet z toho, že počítačová kriminalita představuje útoky na sběr, zpracování, přenos a uchovávání informací prostřednictvím výpočetní techniky. Počítačová kriminalita je v současnosti považována za trestnou činnost směřující k narušení především činnosti podniků, tedy podnikatelské činnosti jako takové, dále k ohrožení či narušení činnosti veřejnoprávních orgánů pracujících s výpočetní technikou. Každý podnikatel má zájem na ochraně vlastního podniku a především pak systému automatizovaného zpracování dat, neboť tento plní řídící i evidenční funkce. Současné tendence svědčí o snaze podnikatelů budovat vlastní systémy ochrany podniku. Ochrana výpočetní techniky patří mezi nejdůležitější formy ochrany podnikání. Pouze prostřednictvím kvalifikovaných odborníků lze vytvořit předpoklady pro kvalitní ochranu výpočetních systémů. Nelze však v této souvislosti pominout finanční náklady. Dříve se považovalo za dostatečné chránění počítače pancéřovými dveřmi. Dnes mnohdy náklady na ochranu počítačů dosahují částek mnohonásobně vyšších, než samotná cena počítače.

Podle [102] lze útoky proti výpočetní technice v zásadě rozdělit podle určitých společenských znaků právní povahy do tří skupin

-na úmyslná jednání páchaná s cílem zničit nebo poškodit výpočetní techniku, nosiče informací, programy, informace a spojovací techniku,

-na úmyslná jednání, při nichž výpočetní technika slouží jako prostředek k páchání trestné činnosti, zejména majetkové povahy,

-na nedbalostní jednání, při nichž dochází ke zničeni či zneužití výpočetní techniky a jejího vybavení, programy a informacemi, spojovací technikou.

Do první skupiny lze zařadit úmyslné útoky proti výpočetní technice s cílem ji poškodit nebo zničit. Může se jednat o vysoce kvalifikované útoky pachatelů, kteří jsou odborníky na výpočetní techniku či klasické destruktivní útoky. Druhá skupina je tvořena

případy tzv. *počítačové špionáže*, kdy pachatel usiluje o získání přístupu k informacím a nosičům informací s cílem zneužít informace vůči jejich původnímu vlastníku či držiteli. Patří sem i krádeže počítačového času, kdy pachatel využívá nákladné výpočetní techniky i programového vybavení jiného subjektu např. na základě napojení se na počítačovou síť. Do této skupiny jsou zařazována i jednání směřující k manipulaci s programy a informacemi pro získání majetkového prospěchu (vydírání, plánování organizované trestné činnosti). Sem by autor [102] pravděpodobně musel zařadit i přímo neuvedené delikty páchané v souvislosti s porušováním autorských práv tvůrců počítačových programů. Třetí skupina zahrnuje jednání, která lze spáchat z nedbalosti, přičemž věcně odpovídají jednáním popsaným v předcházejících dvou skupinách.

**

U dřívějších klasických informačních systémů (bez uplatňování výpočetní techniky) se jednalo hlavně o získání a zneužití informací. O nosiče dat v podstatě zájem nebyl. I proto by bylo možné hovořit o informační kriminalitě. Praxe však ukazuje na mnohočetnost faktorů charakteristik trestné činnosti v této oblasti, kdy pachatel nemívá jen jeden z výše uvedených cílů. Situace bude ještě komplikovanější v souvislosti s dalším rozvíjením a rozšiřováním informačních technologií. Proto také nelze mnohdy jednoduše klasifikovat kriminální jevy z této oblasti podle kategorií trestných činů daných trestním zákonem.

Je možno shrnout, že uvedené definice či přístupy sice přispívají k pochopení pojmu počítačové kriminality, ale žádná z nich nás v plné míře neuspokojí, zejména potud, pokud si uvědomíme, že tento fenomén má též svou dynamiku a bude se vyvíjet asi tak rychle, jak rychlý je pokrok v rozvoji počítačové techniky vůbec.

1.2. Počítačová kriminalita jako „fuzzy" pojem

Počítačová kriminalita je v současnosti značně odlišná od doby začátků masového rozvoje aplikací počítačů, kdy např. v oblasti tvorby programů docházelo mezi subjekty více méně k přátelské výměně nástavbových programových produktů bez jakýchkoliv aspektů komerčního typu.

S firemní profesionalizací výroby programových produktů, zejména pak programů se speciálním zaměřením, rozšířením masové dostupnosti personální výpočetní techniky, tvorbou a provozováním databází a počítačových sítí, včetně Internetu, vznikla rozsáhlá škála možností trestné činnosti. Současně s tím byl nastolen problém prevence a jejího institucionálního zabezpečení v místním i nadnárodním pojetí. Jako příklad uveďme zřízení *České protipirátské unie,* jejíž pole působnosti nebylo samozřejmě determinováno pouze rámcem počítačové kriminality. Na tomto příkladu lze vytušit obsahový posun původního významu počítačové kriminality jako takové.

Víme, že problém vymezení počítačové kriminality v současnosti není doposud vyčerpávajícím způsobem řešen, což vede mnohdy k jistým pragmatickým či jinak obecně méně uspokojivým definicím. V souladu s užší specializací autorů lze v některých případech vytušit vývojové tendence k odklonu od širokého pojmu počítačové kriminality ve prospěch jednotlivých dílčích problémových okruhů. To vše s akcentem na podstatu problému a méně již na formu, tedy na to, že daná činnost byla páchána počítačem. Mimo jiné i proto, že počítače se staly naprosto běžným prostředkem ve většině oborů lidské činnosti. Počítačové podvody, falzifikace, poškozování dat a programů, počítačové sabotáže, neoprávněné přístupy k datům, neoprávněný průnik do sítí, porušování autorských práv tvůrců a distributorů programů, neoprávněná kopírování produktů, počítačová špionáž, malverzace financí pomocí počítačů, neoprávněná užívání hardware, software, prevence počítačové kriminality, včetně vhodných legislativních úprav atp. jako základní problémové okruhy jsou do značné míry samostatnými specializacemi. Překrývají se též mnohdy s jinými fenomény kriminality (s hospodářskou kriminalitou, kriminalitou bílých límečků, organizovaným zločinem atp.), k jejichž páchání nejsou počítače nezbytně nutné. Kromě tendencí ke specializaci autorů na ostře vymezené problémy, vyskytují se též opačná extenzívní pojetí, přesahující rámec klasické počítačové kriminality ve smyslu výstižnějšího pojmu *kriminality informační* - viz např. [188].Odtud je vidět, že počítačovou kriminalitu nelze trvale vymezit jako ostře ohraničený pojem. Abychom předem vyloučili jeho nevhodnou restrikci či přesah, pojmeme jej dynamicky jako tzv. „fuzzy“ konstrukt ve smyslu otevřeného, jinak neostře vnímaného typu kriminality.

1.3. Stěžejní problémové okruhy počítačové kriminality

Počítačová kriminalita má řadu výrazných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů počítačové kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, trestný čin v oblasti počítačové kriminality může být spáchán v několika tisícinách vteřiny a pachatel ani nemusí být přímo na místě činu. Další významnou charakteristikou pro počítačovou kriminalitu jsou v jejím důsledku značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů. Počítačovou kriminalitu také provází určitá diskrétnost trestné činnosti. Pachatel počítačové kriminality musí být zpravidla vyzbrojen hlubšími znalostmi předmětnými i technickými z oblasti informačních technologií a počítačů zejména. Z uvedeného vyplývá, proč počítačová kriminalita bývá pro svou povahu někdy označována též jako kriminalita „bílých límečků“.

K vyjasnění pojmu a postavení počítačové kriminality lze přistoupit též z pozic problémových okruhů tohoto fenoménu a z problematiky jeho výzkumu. Účinnost takového přístupu vyplyne až později z podrobnějšího rozboru možností řešení jednotlivých otázek.

Problematika, kterou se budeme zabývat v této studii, je na základě zkušeností z literárních pramenů dána následujícími problémovými okruhy:

1. Vymezení pojmu počítačové kriminality.
2. Problémy výzkumu počítačové kriminality.
3. Útoky proti počítačům a programovým systémům.
4. Útoky směřující ke zneužití počítačů, dat a jiných informací.
5. Zneužívání strojového času, latence a modelování problémů počítačové kriminality.
6. Počítačová bezpečnost.
7. Porušování autorských práv.
8. Boj s počítačovou kriminalitou.
9. Prevence a represe z pohledu počítačové kriminality.
10. Osobnost pachatele počítačové kriminality.

Zde je třeba říci, že uvedené problémové okruhy, podobně jako pojem počítačové kriminality sám, nelze zcela ostře vymezit. Zjevně se například vzájemně prolíná prevence a represe s bojem proti počítačové kriminalitě. Tímto rozčleněním si ovšem neklademe za cíl pokrýt vyčerpávajícím způsobem celou tematiku počítačové kriminality. Jde spíše o praktické členění podle vzorů a dostupnosti informačních zdrojů. Je zde ještě jeden moment, velmi významný pro orientaci našeho podání. Dokud převažovalo státní nebo jiné kolektivní vlastnictví, ochranou informací se zabýval převážně státní aparát. Po změně vlastnických poměrů, kdy převažuje soukromé vlastnictví, informace se staly mnohem výrazněji zbožím, tedy prodejním i koupěschopným artiklem. Jejich ochrana je proto podstatně významnější než tomu bylo doposud. Tedy i jejich zneužití má relativně hlubší dopad, alespoň pokud se vlastníků týká. Z toho důvodu jsme těmto momentům věnovali zvýšenou pozornost.

S počítačovou kriminalitou souvisí i ochrana informací a dat v informačních systémech. Jak uvádí autor [111] v režimu převládajícího soukromého vlastnictví bude ochrana informací, tj. prevence před jejich únikem nebo zneužitím více záležitostí vlastníka, majitele, než orgánů činných v trestním řízení. Policii zůstane především úloha odhalování a objasňování konkrétních trestných jevů a činů, tedy kriminality. Obecná prevence může být realizována v podobě doporučení, rad, vytváření podmínek k dodržování zákonů atd. Proto i uvnitř policejního aparátu je vžito používání pojmu počítačová kriminalita v obdobných dimenzích, tak jak jsme naznačili. Protože v současné době nemá pojem počítačové kriminality žádný oficiálně definovaný obsah, je rozumné ponechat jejímu rámci určitou dynamickou vůli ve výše naznačeném smyslu.

2. Problematika přístupu k výzkumu počítačové kriminality

Čerpáno převážně z pramenů: [134], [136], [137], [138], [142].

2.1. Smysl výzkumu, jeho předmět a cíl

Určité formy počítačové kriminality mohou bezesporu představovat společensky velmi nebezpečnou činnost. To samo o sobě předurčuje fenomén počítačové kriminality ke koncentraci pozornosti orgánů činných v trestním řízení na tento jev. V předchozím jsme se zmínili o jeho barvitosti a šíři. Motivaci k jeho výzkumu podnítila kromě výše uvedených faktorů též jistá nepřehlednost terénu souvisejícího s touto tematikou, která se mimo jiné odráží i v rozsáhlých literárních zdrojích. Na základě našich věcných, informačních a personálních možností lze stanovit předmět a cíl výzkumu takto:

Z krátkodobého hlediska

-orientace v oblasti stávajícího vymezení pojmu počítačová kriminalita, s cílem upřesnit definici ve významu „fuzzy“ pojmu,

-orientace v literárních pramenech s cílem vytyčit základní problémové okruhy počítačové kriminality,

-zaměřit se na průběžné zpracování získaných informací s cílem podání studie jako podkladu k dalšímu výzkumu,

-nastínit další etapy postupu s cílem následného řešení nejdůležitějších problémů.

Z dlouhodobého pohledu

-na základě věcných a technických aspektů spjatých s obsahem a formou problematiky vybrat vhodné přístupy s cílem pochycení jednotlivých problémových okruhů,

-rozpracovat vybrané problémové okruhy s cílem shrnutí, utřídění a presentování stávajících i nových poznatků z oboru počítačové kriminality,

-aktualizovat poznatky s ohledem na vývoj společenských vztahů,

-průběžně každou etapu uzavřít zpracováním stručné studie s cílem výstupu nejdůležitějších poznatků a případných návrhů opatření.

2.2. Věcné aspekty spjaté s obsahem

V souladu s dostupnou literaturou lze nastínit následující logicky možné aspekty, které se do výzkumu promítají a které nutno brát v úvahu i v dalších etapách rozpracování:

1. Trestná činnost označovaná v literatuře jako klasická počítačová kriminalita.

Akceptování dostupných pramenů v literatuře, podle hledisek

-lokálních pro účelové využití ve výzkumu (útoky směřující ke zničení hardware nebo dat, útoky směřující ke zneužití dat formou jejich neoprávněného získání či změny, a to když útok je motivován zištně nebo nezištně, dále porušování autorských práv ať již využitím

software pro vlastní, či služební potřebu, nezákonná distribuce firemních programových produktů, zneužití strojového času atp.);

-nadnárodních, např. podle hledisek *Rady Evropy* ve snaze po sjednocení legislativy evropských zemí ve vztahu k počítačové kriminalitě (počítačové podvody, včetně nedovolené manipulace, počítačová falzifikace stíhaná podobně jako falzifikace tištěných dokumentů, poškozování dat a programů, počítačové sabotáže, včetně útoků proti hardwarovým prostředkům, neoprávněné přístupy, neoprávněné průniky, jako např. neoprávněné užívání komunikačních sítí počítačů a přístup k datům pomocí nich, neoprávněné kopírování autorsky chráněných programů, topografie, změna v datech nebo počítačových programech, problematika tzv. virů, počítačová špionáž, týkající se zpravidla otázek průmyslového a obchodního tajemství, neoprávněné užívání počítače, chráněných programů ap.).

2. Problematika hospodářské kriminality v průniku s počítačovou kriminalitou.

Rozvoj aplikací výpočetní techniky v ekonomické a finanční sféře, rozvoj finanční infrastruktury, vznik černého trhu, paralelní ekonomiky, konstituování strategických aliancí ke zvyšování mocenských účinků koncernů a celková globalizace života, otvírá možnosti vzniku a šíření specifické počítačové kriminality hospodářského charakteru.

Technicky vyspělé počítačové podvodníky v ekonomické sféře je obtížné vystopovat a dopadnout. Tito lidé představují novou formu individuální moci, která může mít dalekosáhlé škodlivé důsledky. Vlivem jejich hlubokých technických znalostí mohou překonávat i velmi důmyslné bezpečnostní bariéry ve smyslu preventivní ochrany systémů vůči počítačové kriminalitě. To je příklad zcela nového faktoru dokreslujícího barvitost současné počítačové kriminality, pokud jde o problematiku osobnosti pachatele.

3. Problematika organizovaného zločinu v průniku s počítačovou kriminalitou.

V současnosti organizovaný zločin jak vnitrostátního rozsahu, tak i v mezinárodním měřítku využívá často k páchání trestné činnosti prostředků nejmodernější techniky. Včetně zneužívání počítačů k široké škále deliktů, které spadají pod pojem počítačová kriminalita.

Specifickou složkou nové geopolitické situace je rozvoj celosvětových informačních a komunikačních systémů, které jsou propojeny s celosvětovými finančními a dopravními systémy, rozšiřují a doplňují je. Tím vzniká pro státy, zejména pro ty v postindustriálním stadiu vývoje, určité nebezpečí ohledně zneužití informačních toků mezinárodními zločineckými organizacemi.

Jak se jednotlivé podniky a společnosti stávají čím více závislými na propojených komunikačních a informačních systémech, tím více jsou zranitelnější. Existuje totiž ze strany organizovaného zločinu nebezpečí týkající se poškozování systémů pro místní, národní i světové finanční transakce, burzovní operace, kontroly letecké dopravy, správy výběru daní, sociálního zabezpečení, narušení komponentů vojenské, zpravodajské (špionážní) a policejní infrastruktury, atd. To jsou příklady problémových okruhů společensky velmi nebezpečné počítačové kriminality.

4. Právní aspekty počítačové kriminality.

Právní aspekty, legislativní úpravy, zákony, speciálně orientované právní normy nižší síly, včetně stanovení sankcí za delikty spadající do rámce počítačové kriminality lze považovat za atributy speciální prevence.

K obecným problémovým okruhům lze počítat rozbor faktorů

-ovlivňujících vymezení právních aspektů *de lege lata*, s možností jejich realizace pro potřeby výzkumu počítačové kriminality např. též s pomocí ASPI, automatizovaného systému právních informací,

-pro hlediska právních aspektů *de lege ferenda*.

Ze speciálních problémů lze jmenovat *softwarový audit*, respektive jeho právní aspekty. Tento relativně nový institut je realizován převážně u velkých firem, které jsou ochotny vynaložit určité finanční prostředky na hloubkovou kontrolu legálnosti jejich programového vybavení a přijetí dalších preventivních opatření proti zneužívání software.

5. Prevence počítačové kriminality

Kromě prevence počítačové kriminality na základě právních aspektů existuje ještě problematika ochrany pomocí prostředků

-hardware, např. formou speciálních úprav technických karet počítačů proti neoprávněnému průniku do počítače,

-software, např. pomocí nejrůznějších zámků, hesel, deklarací, případně jiných prostředků zamezujících neoprávněné otevření programů, souborů nebo jejich částí,

-preventivní výchovy zúčastněných osob, programátorů, operátorů, či uživatelů v nejširším měřítku.

Do teorie prevence počítačové kriminality lze zahrnout též

-zpracování koncepce počítačové bezpečnosti,

-aplikace zásad počítačové bezpečnosti s ohledem na specifika příslušného pracoviště,

-hodnotící interpretace preventivních opatření vůči opatřením represním.

2.3. Technické aspekty spjaté s formou

Podle výchozí orientace v dostupných pramenech lze nastínit tyto logicky možné základní aspekty spjaté s formou přístupu k dané problematice:

1. Využití stávajících literárních pramenů a navázání na předchozí výzkum realizovaný v IKSP.

Použitelnost tohoto přístupu skýtá asi nejširší možný informační záběr. Jen v databázi IKSP se nachází více než 80 odkazů k uvažované tematice. Daný kompilační záběr by bylo třeba podřídit vhodným *vymezením pojmu* počítačové kriminality, které u různých autorů není vždy zcela shodné.

2. Využití informací z internetové sítě.

Tento přístup by s ohledem na námi akceptované pojetí počítačové kriminality představoval další možný zdroj informací, též i nadnárodního charakteru. Pokud by byla zjištěna menší dostupnost pramenů v plném znění, využití by bylo nutno redukovat na pouhý rešeršní aspekt.

3. Využití informací z osobních kontaktů s jinými (např.policejními) pracovišti.

Vzhledem k tomu, že vyhledávání, stíhání a vyšetřování počítačové kriminality je především vysoce profesionální činností policejních složek, aspekty plynoucí z tohoto přístupu by představovaly další závažné konkretizační možnosti. Ovšem v závislosti na ochotě spolupráce odpovídajících složek vnitra, příp. jiných pracovišť, jako např. agentur pro ochranu software atp.

4. Využití informací z vlastních zdrojů, např. realizací dotazníkových akcí, studiem trestních spisů ap.

Realizace dotazníkových akcí k problematice počítačové kriminality, které se doposud uskutečnily v podmínkách IKSP byly založeny na zjišťování skutečností a názorů odpovědných a výkonných pracovníků vytypovaných lokálních počítačových sítí. Akce se setkala mnohdy s neochotou vypovídat ze strany majitelů lokálních sítí, takže návratnost byla necelých 25%. Operovat s vyčerpávající generalizací získaných výsledků by se podle vyjádření samotného autora akce „podobalo čirému šarlatánství“ [142]. Vzhledem k omezeným možnostem dosažení representativnosti takových akcí, jakož i k jejich velké časové náročnosti a pracnosti, bylo by nutné je koncipovat poněkud jinak, abychom v našich podmínkách docílili ekonomicky adekvátního přínosu.

5. Využití hromadných statistických údajů z dostupných databází.

Vzhledem ke stávajícím způsobům registrace kriminality a struktuře kriminálních statistik v našem resortu, nemůžeme bezprostředně z příslušných databází získat kvalifikovaný souborný pohled na stav, vývoj, trendy, případně na další charakteristiky počítačové kriminality. Lze předpokládat, že tento přístup by byl asi nejméně použitelný.

2.4. Komplexní zabezpečení výzkumu

Zabezpečení stávajícího výzkumu, včetně jeho předpokládaného pokračování nutno realizovat v systémovém pojetí komplexním přístupem, tj. provázáním práce podle dostupných hledisek věcných, informačních, metodických, technických a interpretačních. Zde uvedeme jen nejdůležitější předem vytypované zásady tohoto přístupu.

Zabezpečení podle věcných aspektů, stručně *věcné zabezpečení*, spočívá ve vymezení problémových okruhů na základě orientace v dostupných pramenech, případně při kontaktech s jinými pracovišti. Je tedy velmi úzce vázáno na dostupnost adekvátních informačních zdrojů, tedy na zabezpečení informační. Speciálně přitom budou i nadále akcentována právní hlediska počítačové kriminality.

Informační zabezpečení je dáno v podstatě výše vyjmenovanými aspekty spjatými s formou pochycení počítačové kriminality v podmínkách IKSP. Předpokládáme postupné rozvinutí od nejširšího místního informačního záběru až po specifickou problematiku podle orientace v možnostech spolupráce s jinými pracovišti. V případě dostupnosti dat, je třeba přistoupit k jejich systemizaci, vytřídění, případně k dalšímu předběžnému zpracování, např. formou sestavení časových řad apod.

Metodické zabezpečení jako nejnáročnější etapu zpracování nutno vázat na optimalizační postupy výběru informací textového, případně i numerického charakteru. Předpokládáme, že bude i nadále postupováno převážně sekvenčním způsobem, tj. každý další krok zpracování se bude orientovat bezprostředně podle předchozích poznatků heuristicky, tj. bez předem stanovených hypotéz. Pokud budou k dispozici statistická data, bude tímto způsobem rozhodnuto o případné nástavbové analýze. Ta by se realizovala v podstatě metodami *kriminologické statistiky* [138], např. aplikacemi modelů latence kriminality, trendů, prognóz, účinnosti prevence aj. Verifikační přístup bude uplatněn jen tehdy, když data, resp. výsledky nástavbových analýz umožní vyslovit pracovní hypotézy. Tyto hypotézy by byly pak verifikovány exaktními přístupy testování, a to i v případech malých statistických souborů, kdy lze nasadit testy specificky transformované.

K technickému zabezpečení bylo doposud využito běžné dostupné techniky IKSP. Softwarové vybavení výpočetní techniky nebude nutno zatím v dalších etapách rozšiřovat. K případné nástavbové analýze budou použity speciální programy podle vybraných modelů kriminologické statistiky, sestavené ve stávajících firemních systémech EXCEL, STATGRAPHIC, a GW-systému.

Interpretační zabezpečení by v případě tohoto výzkumu mělo vyústit k formulaci doporučení

-pro orientaci postupu v dalších etapách,

-aktualizaci stávajících poznatků,

eventuálně pro formulaci závěrů

-pro orgány činné v trestním řízení či pro legislativní praxi.

Při komplexním zabezpečení výzkumu počítačové kriminality lze doporučit respektování obecných zásad aplikace speciálních přístupů, alespoň v minimálním rozsahu popsaném ve studii [138]. Zejména je třeba přihlížet k určitým zvláštnostem charakteristickým právě pro aplikace speciálních metod, pokud tyto hodláme adekvátně uplatnit. Tyto zvláštnosti, spjaté s předmětnou disciplinou - kriminologií, jsou podmíněny řadou faktorů, z nichž vyjímáme

-*složitost předmětu kriminologie,* který zahrnuje objektivní i subjektivní aspekty, počítačovou kriminalitu jako hromadný i jedinečný jev, kriminalitu vůbec jako fenomén implikovaný danými objektivními společenskými podmínkami i kriminalitu ve světle specifických vlastností osobnosti pachatele;

-*odlehlost* principů kriminologie a pomocných disciplín poskytujících speciální přístupy, zvláště pak sociologie, psychologie, matematiky a matematické statistiky;

-*rozdílnost* ve stavu počítačové kriminality skutečné a registrované, tj. kriminality objektivně existující a na druhé straně kriminality podchycené ve statistikách;

-*obtížnost* odhalování latentních struktur počítačové kriminality;

-*diference* v přístupech k měření kriminality v různých resortech zabývajících se registrací kriminality;

-*nesnadnost* naplnění cílů kriminologie, které nelze zploštit pouze na kriminografickou stránku poznávacího procesu, ale v tomto případě spíše orientovat k využití získaných poznatků pro prevenci počítačové kriminality.

Metody kriminologické statistiky a jejich aplikace, používané při řešení konkrétních problémů kriminologických výzkumů, a tedy i výzkumu počítačové kriminality lze považovat

-za jeden z možných metodických prostředků popisu skutečnosti, např. tzv. kriminografie;

-za prostředek vysvětlení, explikace na základě empirických poznatků;

-za způsob indukce, generalizace určitých poznatků z jistého omezeného souboru na soubor větší;

-za prostředek anticipace, tj. předvídání jevů;

-za formu dedukce, tj. vyvozování dalších (specifických) logických závěrů z daných (obecnějších) pravd;

-za nástroj verifikace poznatků, jejich konfrontace se skutečností, např. ověřováním (testováním) hypotéz.

2.5. Smysl a možnosti použití speciálních metod při výzkumu

Aplikací speciálních metod při řešení praktických úloh dochází obecně k transformaci výchozích (empirických) dat na výsledné sestavy údajů. Očekáváme, že tyto výsledky budou mít pro nás větší význam z hlediska dalšího využití než data výchozí. V takových případech říkáme, že jde o *smysluplné aplikace* zvolených přístupů či analýz. Mnohdy je až zarážející, jak málo je věnováno pozornosti stabilitě výsledků v závislosti na zvolených přístupech. Protože problémy stability výsledků výzkumů přesahují rámec tohoto přehledu, odkazujeme zájemce na monografii [138]. *Kriminologická statistika* inklinuje k vymezení podmínek zmíněné smysluplné aplikace více či méně speciálních metod při řešení konkrétních problémů kriminologie. V tom tkví její význam a cíl jako statistiky aplikované.

Připomeňme, že použití statistických metod v kriminologii je podmíněno existencí a studiem těch stránek kriminality, které mají *hromadný charakter*. Ten se v podstatě posuzuje podle proměnlivých znaků dostatečně velkého počtu jedinců (prvků), jež mají některé vlastnosti shodné, společné. *Dostatečně velký počet* bývá případ od případu různý, avšak vždy takový, kdy se uvažovaná vlastnost spolehlivě projeví. I když při výzkumu počítačové kriminality předpokládáme zatím jen sporadické využití hromadných statistických dat, nutno

mít na zřeteli, že statistické metody skýtají užitek zejména tehdy, jdou-li jejich aplikace ruku v ruce s věcnou analýzou, vycházejí z ní a doplňují ji exaktními závěry, plynoucími též z kvantitativní povahy věci. V tomto smyslu lze aplikace statistických metod v kriminologii považovat za pomocný prostředek, který umožní realizovat studium příslušného jevu v celé šíři jeho podstaty, tj. po stránce kvalitativní i kvantitativní. Nelze universálně předpokládat, že předmětně orientovaný pracovník, který využívá v praxi statistických přístupů spíše jen jako doplňkového prostředku hlubšího poznání, bude zmíněným metodám věnovat tolik energie a času, aby pronikl k jejich matematické podstatě. Na druhé straně by však měl být obeznámen s jejich existencí a možnostmi aplikace, aby dovedl odpovědně rozhodovat o jejich konkrétním uplatnění v problematice, kterou se zabývá, a porozuměl dobře i výsledkům, které tyto postupy poskytují. Takový pracovník by se měl orientovat nikoliv k obsahově i rozsahem náročnému matematickému popisu přístupů, nýbrž informativně k možnostem a smyslu jejich uplatnění.

S ohledem na uvedené skutečnosti nutno též plánovat personální pokrytí výzkumné akce. Personální zabezpečení musí být také plánováno s přihlédnutím k celkovému pojetí výzkumu počítačové kriminality a možnostem řešícího pracoviště. Protože obojí se může v průběhu sekvenčního přístupu k problematice měnit, nutno vždy počítat i s dynamikou personálního pokrytí. Obecně se jeví jako únosné následující obsazení:

vedoucí úkolu pro vyjasnění základních pojmů a metodiky, výběr problémových okruhů, koordinaci a zastřešení výzkumu a zabezpečení výstupů,

právník pro analýzu právních aspektů počítačové kriminality se zaměřením na otázky generálně-preventivních účinků legislativních úprav,

technicky orientovaný pracovník pro obecnou problematiku prevence počítačové kriminality v oblasti hardware i software,

předmětný pracovník se zaměřením na styčnou oblast s hospodářskou kriminalitou a organizovaným zločinem.

3. Útoky proti počítačům a programovým systémům

Sestaveno převážně z pramenů: [9], [10], [24], [77], [110], [128], [129], [138], [179], [199], [247], [249], [250], [251].

3.1. Výpočetní technika a vývoj počítačové kriminality

Počítače, jejich příslušenství, včetně programů jsou předmětem vlastnických a závazkových vztahů, jednak oprávněných, ale i neoprávněných, tak jako je tomu u věcí movitých. Programové vybavení a data, která v naprosté většině bývají součástí počítačů, počítačových komplexů a počítačových sítí z těchto věcí činí předměty výjimečné a zvláštní - viz podrobněji [24]. Podle autora [24], počítačovou kriminalitu je v zásadě možné dělit na dvě hlavní oblasti, a to na útok proti počítači, nebo na útok, který byl připraven pomocí počítače.

Počítač je z vizuálního hlediska předně věc movitá. Jedná se zejména o jeho *hardwarové vybavení*, jeho příslušenství, obrazovku, klávesnici, myš, scanner, tiskárnu, telefonní modemy, faxmodemy atd., což má určitou hodnotu závislou na technické úrovni daného zařízení, jeho stáří a opotřebování. Pro sjednocení terminologie lze využít například pojmosloví podle *ČSN 36 9001*. Počítač je podle této technické normy stroj na zpracování dat provádějící samočinně posloupnosti různých matematických a logických operací. Aby tato technika byla funkční, musí být vybavena příslušnými programy.

Program-software má duální charakter, tedy nehmotný obsah, který je autorským dílem a musí být zaznamenán, fixován na tzv. nosiči dat, což je věc movitá. Z hlediska kategorizace autorských děl je podle našeho autorského zákona program co do principu ochrany srovnatelný s dílem literárním. Cena programu je vlastně součtem hodnot nehmotného obsahu, tedy autorského díla a hodnoty hmotného nosiče informací, na němž je program zaznamenán a předáván k dispozici uživateli. Hodnota nosiče v tomto případě je oproti hodnotě nehmotného obsahu zpravidla velmi malá, mnohdy zanedbatelná.

Další nedílnou a z hlediska zastupitelnosti či nahraditelnosti často nejcennější částí počítačového komplexu jsou *data, údaje, informace.* Informace o nějakém jevu je jistá veličina, která nám snižuje dosavadní neurčitost, neznalost o daném jevu. Podle citované normy informaci lze považovat za význam přisouzený datům. Jelikož informace je podstaty nehmotné, musí být, podobně jako program, uložena na nějakém hmotném nosiči nebo jeho prostřednictvím přenášena. Hmotným nositelem informace při jejím vnímání, tedy při přenosu od zdroje do našeho vědomí, je nějaká fyzikální veličina, obecně zvaná *signál.* Vzhledem k tomu, že každá informace má určitou vnitřní hodnotu, může být z ekonomických hledisek považována za zboží. Lze ji proto kupovat, prodávat, užívat, ale i zneužít. Lze ji získat legálně, ale i trestnou činností.

Práce s daty podle programu je charakteristickou činností počítače, přičemž podstatnou součástí hardware při tom využívanou je *nosič informací.* Pojmy počítač a nosič informací se

proto někdy mohou, ale také nemusí krýt. Lze si představit nosič informací bez počítače, ale opačně je tato představa nereálná. Nosič dat (datové médium) jako prostředek k záznamu dat může být snadno přenosný, což je dáno především pokrokem v miniaturizaci konstrukčních prvků (čipů, procesorů).

Z pohledu možného zneužití či jiných útoků proti nosiči dat bychom měli rozlišovat prázdný a naplněný nosič informací. Operační paměť počítače je po každém jeho vypnutí jako nosič informací prázdná. Naproti tomu pevný (hard) disk, disketa, CD-disk, optický disk, magnetická páska mění svůj nehmotný obsah pouze speciálním úkonem, nahráním, uložením, přepsáním, vymazáním, formátováním apod. Nosiče informací, podobně jako i jinou část hardware, lze samozřejmě poškodit vnějším zásahem a tím pozměnit či zničit i nehmotný obsah nosičem nesený. Z kriminalistické praxe jsou známy např. příklady úmyslného pozměňování či ničení informací na magnetických nosičích cíleným magnetickým polem, poškozování uživatele nasazováním speciálních programů, tzv.*virů*, pro vymazání spouštěcích programů, či zničení pevných disků i pro jiné znemožňování práce s počítačem. Podle autorky [77], 95 % všech počítačových zločinů, které byly odhaleny, byly odhaleny náhodou, nikoliv jako výsledek kontrolní činnosti. Pokud si uvědomíme současný stav bezpečnosti informačních technologií, od bezpečnostní politiky a analýzy rizik přes jednotlivé aspekty počítačové a komunikační bezpečnosti a stavu legislativy k podrobným popisům jednotlivých algoritmů, používaných v oblasti šifrování, při aplikaci digitálního podpisu ap., mohlo by se zdát, že počítačový zločin nemůže mít při aplikaci všech dostupných protiopatření prostor k realizaci. Opak je však pravdou. Dříve než se podíváme na historii počítačového zločinu, speciálně na vývoj počítačové kriminality ve světě za poslední čtyři desetiletí, několik slov k terminologickým otázkám.

**

Generace počítačů. Jak uvádí autor [179], v oblasti počítačové kriminality dosud není všeobecně známa a ustálena užívaná terminologie. Vyplývá to z překotného vývoje širokého spektra poznatků tohoto oboru. Počítačové systémy lze rozlišit podle použité technologie a vnitřní organizace na pět generací. První elektronický samočinný počítač na bázi elektronek byl spuštěn v roce 1945. Jde o první generaci počítačů. Program řídící činnost počítače byl tvořen elektrickým obvodem (byl součástí počítače) - nelze tedy mluvit o počítačovém programu v dnešním slova smyslu. Vznik druhé generace je podmíněn objevem nové technologie - tranzistoru. Architektura třetí generace je spojena s technologií integrovaných obvodů a přibližně od této chvíle je také možné mluvit o *„software“*, jak ho chápeme v dnešní době. Vývoj dalších generací byl produktem stupňování integrace elektronických obvodů, chipů a změnou architektury systémů. Programy v dnešním pojetí se objevily v 60. letech a již od 70. let se setkáváme s problémy jejich právní ochrany. Do jejich tvorby bylo totiž již od počátku nutné vložit značný tvůrčí potenciál i nemalé finanční náklady. V ranných stadiích rozvoje výpočetní techniky přesto ale byly tyto položky zanedbatelné ve srovnání s prostředky a cenou technické části těchto projektů - hardware. Mnohdy byl software dodáván jako součást hardware ve formě tzv. „bundlingu“, prodeji dvou nebo více než dvou výrobků v jednom cenovém balíku. Tím lze také snad částečně vysvětlit nevyjasněnost a nedostatečná

legislativní opatření v oblasti právní ochrany software oproti ochraně hardware. Což podle [179] do jisté míry ve světě přetrvává dodnes. Změnu přinesl prudký nárůst výroby personálních počítačů. Od roku 1976 tak mnohonásobně klesla cena hardware, přičemž výkon personálních počítačů se stal srovnatelným s výkonem někdejších střediskových počítačů. Jedním z důsledků bylo, že cena software již nebyla zanedbatelnou ve srovnání s cenou hardware, ba naopak začínala převažovat. Tím se změnila i strategie nákupu výpočetní techniky. Firmy napřed zjišťují své nároky na programové vybavení, vyberou vhodný software a teprve pak nakupují hardware, který umožní efektivní využití software v žádané kvalitě a požadované rychlosti odezvy. Existence velkého počtu izolovaných počítačů byla jedním z impulsů vedoucím k rozvoji počítačových sítí a k využití výpočetní techniky snad ve všech oblastech lidské činnosti a tím také k naléhavé potřebě právní regulace takto vznikajících právních vztahů. Další rozvoj výpočetní techniky je vázán na vývoj odpovídajícího software, který je v závěsu za vývojem hardware a tudíž vždy trochu opožděn, čímž neumožňuje vždy jeho plné využití. Výpočetní systémy tak často běží jen na část potenciálního výkonu, protože použitý software neumí využít pokročilé technologie.

Počítačová kriminalita v šedesátých a sedmdesátých letech. Jak uvádí [77], v průběhu posledních čtyřiceti let došlo k významnému růstu i kvalitativnímu vývoji počítačové kriminality, ve světě i u nás. Sběr údajů o zneužití počítačů zajišťoval v USA již od roku 1958 *Stanford Research Institute (SRI)*. V té době byly údaje rozděleny do čtyř kategorií na

-vandalismus, namířený proti počítačovému hardware,

-krádež majetku nebo informací,

-podvod uskutečněný pomocí počítače nebo krádež peněz,

-nepřípustné použití počítače nebo krádež a prodej počítačového času.

Zaznamenaná data nebyla významná až do roku 1968, kdy bylo podchyceno 13 případů. V roce 1977 dosáhl počet zaznamenaných případů již 85. Statistiku vedl *SRI* do roku 1978. V tomto období jsou alarmující příklady různých podvodů. V roce 1968 byl obviněn např. viceprezident brokerské firmy z děrování speciálních datových štítků, pomocí kterých převedl na svůj účet v průběhu 8 let 250 tisíc dolarů. V jiném případě modifikoval zaměstnanec brokerské firmy systém tak, že odesílal šeky s dividendami na svou domácí adresu. V novinách tehdejšího počítačového podzemí *Seed* se již objevuje článek, popisující technologii zničení počítače. Objevují se rovněž četné případy magnetického vymazávání a elektronického monitorování.

Počítačová kriminalita v osmdesátých letech. Kromě podvodů a fyzických škod dochází ke krádežím databází, šíření virů, infiltraci logických a časových bomb, k rozšiřování a využívání pirátského softwaru. Autorka [77] dále uvádí, že krádež softwaru nelegálním kopírováním se postupně stává nejobecnějším a nejdražším typem počítačového zločinu. V tomto desetiletí se rovněž odehrály dva zločiny, které dosáhly značné publicity a které vystihují počítačový zločin tohoto období. První byl podrobně popsán v knize *Kukaččí vejce*, vydané česky. Jde o skutečný příběh astronoma Clifford Stolla, pracujícího v Lawrence Berkeley Laboratory, a o jeho 10 měsíců probíhající monitorování průniků do různých počítačů náhodně zjištěného vetřelce, pojmenovaného Stollem *Willy Hacker*. Vetřelec se

pokusil o přístup do 450 počítačů, provozovaných americkou armádou nebo jejími dodavateli a byl úspěšný ve 30 případech. Z Willy Hackera se vyklubal počítačový profesionál ze západního Německa s údajným propojením na KGB. Jeho sledování si vyžádalo spolupráci více než 15 organizací včetně amerických a německých vládních úřadů a soukromých organizací. Případ internetového červa (typ síťového počítačového viru) je rovněž obecně známý. Autor červa, student R. T. Morris, využil bezpečnostní slabiny určitého síťového systému *Unix* a jeho program se nekontrolovaně rozšířil v síti do přibližně 6000 počítačů a způsobil jejich kolaps. Morris byl uznán vinným podle *Zákona proti počítačovému podvodu a zneužití* z roku 1986. Tehdy šlo o první usvědčení podle zmíněného zákona.

Počítačová kriminalita v devadesátých letech. Statistika amerického *Národního střediska pro údaje o počítačovém zločinu* ze začátku devadesátých let uvádí pronikání počítačové kriminality do 6 hlavních oblastí, jimiž jsou

-nedovolený vstup 2 %,
-krádež služeb 10 %,
-změna dat 12 %,
-škody způsobené na software 16 %,
-krádež informací nebo programů 16 %,
-krádež peněz 44 %.

Podle [77] devadesátá léta přinášejí s celosvětovým rozvojem Internetu i jeho zneužití k šíření pornografie, rasismu, propagaci výbušnin a drog, k prezentaci extremistů a kriminálních živlů. Mezi útočníky, jejichž cílem jsou informace uchovávané na počítačích, patří vedle profesionálních hackerů též zpravodajské služby, detektivní kanceláře, média, aktéři organizovaného zločinu i političtí extrémisté.

Situace v České republice. U nás se široce rozšířenou představou o sofistikovaných útocích dnešních potenciálních pachatelů příliš nekorespondují konkrétní zprávy v denním tisku, který jen celkem v omezeném měřítku informuje o případech páchaných v souvislosti s výpočetní technikou. Studie [77] uvádí některé konkrétní případy. Např. v roce 1998 u *Městského soudu* byla obžalována dvojice pachatelek, 24letá dcera a její matka, z podvodného vybrání celkové sumy 9 700 000 Kč. Do počítačového systému vstoupila a podvod spáchala jedna z pachatelek, v době činu úřednice *Komerční banky* tak, že se vydávala pomocí odpozorovaného hesla a fingovaných podpisů za svoji kolegyni, autorizovanou uživatelku systému. Zprávy podobného typu v denním tisku informují čas od času čtenáře o počítačové kriminalitě, která se zaměřuje převážně na naše finanční ústavy. Závažné škody způsobují ovšem i počítačoví piráti. Ročně připraví v České republice výrobce programů údajně o stovky milionů dolarů. To však za předpokladu, že by firmy příslušný objem produktů byly schopny realizovat na legálním trhu. Což není obecně pravděpodobné. Z tohoto hlediska se zdají být takovéto i další odhady škod poněkud nadsazené.

3.2. Trestněprávní aspekty útoků proti počítači

Podle [179] výpočetní technika zasahuje do stále většího počtu oblastí a svou dynamikou vývoje navozuje nové vztahy a problémy nebo mění jejich obsah. Jde o nový, dynamický fenomén ve společnosti, který se nutně odrazí v mnoha právních odvětvích. Znamená nejen očekávaný a uznávaný přínos, ale přináší s sebou i nové a ne vždy pozitivní jevy a skutečnosti. Pojmy jako počítačová kriminalita, softwarové pirátství, ohrožení informací a následně pak počítačová bezpečnost, autorská práva, ochrana dat, ochrana soukromí atd. se však již dostávají i do povědomí širší veřejnosti. Růst podílu výpočetní techniky na zpracování informací všeho druhu je neoddělitelnou součástí rozvoje společnosti a je třeba ho chápat nejen jako samozřejmý vývoj technický, ale i jako proces sociální.

Vztah práva a rozvoje výpočetní techniky není vztahem jednostranným. Tak jako je techniku možné považovat za prostředek zvyšování účinnosti a efektivnosti práva, je právo nepostradatelným prostředkem regulujícím rozvoj a možnosti využití techniky. Tento vztah platí pro softwarový průmysl, vzhledem k jeho charakteru, ve zvýšené míře. Nalezení kompromisu v otázkách ochrany práv autora, regulace a stimulování dalšího rozvoje tohoto průmyslu je nezastupitelnou úlohou legislativy, která by se dala zjednodušeně definovat jako kompromis mezi hrozbou inovacím na jedné straně a potřebou chránit investice do vývoje software na straně druhé. Autor pojednání [179] si všímá dále především otázek právní povahy software. Jeho úvahy lze však zobecnit i na obecné trestněprávní aspekty útoků proti výpočetní technice.

K vývoji této problematiky se dále ve studii [179] uvádí, že spory o charakter právní povahy software se vedou již přes 30 let a přesto není tato otázka dodnes plně dořešena jak v měřítku mezinárodním, tak vnitrostátním. Neutěšený stav v této oblasti je tak charakteristický ve větší či menší míře pro většinu právních řádů. A netýká se jen ochrany software. Jde o úpravy se zaměřením na výpočetní techniku, provoz nelegálních programů, činnost specializovaných pachatelů, operace s viry, manipulace s daty nebo trestná činnost jiného druhu, páchaná prostřednictvím výpočetní techniky. Jako např. úsilí zaměřené k neoprávněnému majetkovému prospěchu, vydírání, zneužití dat, krádeže strojového času, zneužívání počítačových sítí apod.

Počítačová kriminalita je jedna z velmi nebezpečných forem kriminálních deliktů a z hlediska nebezpečnosti pro společnost je srovnatelná např. s organizovaným zločinem. Počítače mnohdy pachatelům usnadňují či umožňují urychlit páchání trestné činnosti a výrazně snižují riziko jejich odhalení. Počítače jsou zneužívány ke klasické hospodářské trestné činnosti zejména tam, kde manipulace s daty by byla bez počítače složitá, zdlouhavá nebo přímo v reálném čase nemožná. Zde máme na mysli např. realizace hazardních finančních her, podvodných investičních záměrů apod. Další velkou třídou možností využití počítače v kriminálním prostředí je oblast padělání a zhotovování falešných papírů, dokladů, platebních instrumentů aj. Vše samozřejmě v náležité kvalitě a vysoké věrohodnosti, což zejména moderní textové a grafické editory umožňují poměrně snadno.

Jak uvádí autor studie [110], podle předmětu útoku pachatele lze říci, že pachatelův útok směřuje proti počítači buď jako hmotnému předmětu, nebo proti jeho cennému programovému vybavení a uloženým důležitým datům. Tato kriminalita představuje vlastně útoky proti technickým prostředkům informačního procesu, tj. sběru, přenosu, uchování, zpracování a distribuci dat (informací), což je uskutečňováno prostřednictvím výpočetní techniky. Pachatel sleduje především obohacení vlastní nebo třetí osoby. Může se jednat o přímý útok nebo útok ve svých důsledcích anebo útoky s různou motivací zaměřené proti fungování výpočetní techniky a k neoprávněnému nakládání s ní. Tato oblast kriminality je charakterizována podle směru útoku pachatele dvojím způsobem. Pachatel směřuje svůj útok proti počítači jako hmotnému předmětu s úmyslem jej odcizit nebo poškodit. Skutková podstata tohoto jednání je vyjádřena v § 247 trestního zákona - krádež, a § 257 trestního zákona - poškozování cizí věci. Vzniklou hmotnou škodu touto trestnou činností lze celkem snadno vyčíslit, ve většině případů jde o náklady na pořízeni výpočetní techniky. V této kategorii počítačové kriminality by bylo vhodné rozlišit mezi pachatelem, který

-odcizí počítač či jeho komponenty s úmyslem za ně získat hmotný prospěch a kterému by stejně dobře posloužila ke stejnému účelu jiná hodnotná věc,

-počítač a jeho komponenty poškodí z pohnutky, která přímo s napadeným objektem nesouvisí,

a pachatelem,

-jehož prvotní pohnutka a jeho jednání cíleně směřuje k počítači (tj. odcizí počítač nebo jeho komponenty, protože přesně zná jejich finanční a užitnou hodnotu),

-který poškodí počítač z pomsty (majiteli, uživateli apod.).

Naznačená hranice v této oblasti mezi obecnou kriminalitou a kriminalitou počítačovou je velmi neostrá a mnohdy může dojít i k vzájemnému prolínání obou pojetí. Při statistickém zpracování údajů o trestné činnosti se u jednotlivých případů tato hranice vůbec nerozlišuje. V souvislosti s tím vyvstávají určité teoreticko-právní otázky vázané na pozadí počítačových technologií, o které nutno opřít též trestněprávní aspekty útoků proti počítačům. Například autoři článku [128] se zabývají dvěma základními problémovými situacemi, které vznikají ve spojení práva s počítačovými technologiemi. První z nich vzniká ze skutečnosti, že užití počítačových technologií působí obtíže, které zákonodárce nepředpokládal, druhá ze skutečnosti, že užití těchto technologií jako nástroje právníků mění jednak způsob, jakým pracují, jednak samu jejich profesi. V první části příspěvku se autoři zaměřují na dopad prudkého nárůstu významu informačních technologií na právní řád, a to jak nizozemský, tak evropský. Poukazují především na nepříznivé důsledky kopírování amerického přístupu k ochraně informačních technologií, zejména čipů, databází a software obecně. S ohledem na harmonizační směrnice evropských společenství se autoři obsáhleji věnují především otázce *legality reversního inženýrství*, nezbytného pro další rozvoj evropského softwarového průmyslu. Přihlížejí ke skutečnosti, že většina základních programových postupů pochází z oblasti mimoevropských, přesto však směrnice z roku 1991 rekonstrukce zdrojových programů z provozních překladů cizích autorů přímo zakazuje. V oblasti databází se autoři [128] zabývají v první řadě harmonizační tendencí projevující se v návrhu směrnice *Komise evropského společenství* z roku 1992, která směřuje k autorskoprávní ochraně databází jako

kolektivních děl. V souvislosti s ochranou dat je v příspěvku zdůrazněn zejména význam, který evropské země přikládají mezistátním tokům dat a ochraně osobních údajů při jejich zpracování počítačovými technologiemi. Zdůrazněna je skutečnost, že data nutno *považovat* za věci hmotné povahy protože jsou manipulovatelná technickými prostředky. I když fyzikálně vzato hmotná samozřejmě nejsou, v právním smyslu mohou být hmotným majetkem, podobně jako speciální formy energie, například elektřina. Skutečnost, že data je nutno považovat za zboží byla konstatována i v nizozemské judikatuře již v roce 1983. Navzdory tomu byla v novele nizozemského trestního zákona z roku 1993 data pojata jako specifická kategorie od ostatního zboží se lišící, což způsobilo nutnost komplikovaného a neopodstatněného doplňování stávajícího předpisu. Přitom je téměř polovina trestných činů v oblasti informačních technologií řazena do kategorie počítačového pirátství, tedy snadno postižitelná zákony na ochranu autorského práva. Dokonce i další rozsáhlé kategorie počítačových trestných činů spadají do již známých trestněprávních skutkových podstat, snad až na nedovolený vstup do informačních systémů. Pokud se právní informatiky týče, autoři [128] konstatují hojné používání počítačových technologií v administrativě, ovšem velmi nízké využívání systémů zpracování dat v běžné právnické praxi. Jedinou výhodou právnických databázových systémů je podle autorů vyhledávání podle slov či klíčových úseků, což však není zcela běžným způsobem právnického získávání informací, kde jsou klasické tištěné informační zdroje zatím běžně preferovány. Vytváření systémů, které by byly schopny řešit konkrétní právní otázky, speciálně pak otázky počítačové kriminality, brání především nedostatek empirického poznání v oboru, a dále pak pevné vědecké báze práva. Proto se i autoři ve výzkumných programech *Erasmovy university* zaměřili spíše na užiti počítačových technologií ve vytváření systémů schopných poskytnout aktuální informace a na moderní prostředky vědecké komunikace. Konečně ve zvláštní pasáži [129] se autoři věnují otázce počítačově automatizované legislativy, tzv. legislativy čtvrté generace, která podle jejich mínění opět snižuje soudce na úroveň sluhy zákonů a v otrockém pojetí vrhá vývoj práva zpět.

**

Jak uvádí autor přehledu [199], po roce 1989 vznikly u nás první právní předpisy vymezující nově demokratický právní řád a vycházející z *Listiny základních práv a svobod*. V rámci toho byly definovány meze svobodného podnikání v prostředí tržní ekonomiky. Následovala pak etapa nutného zpřesňování a zdokonalování právního systému, neboť rozhodně bylo a stále ještě je co vylepšovat. Součástí právního řádu je i poměrně specializované - leč stále se rozšiřující - tzv. *počítačové právo.* Je to souhrn právních předpisů souvisejících jakýmkoliv způsobem s počítači, jejich konstrukcí, výrobou, prodejem a využíváním, s vytvářením, distribucí a využíváním programového vybavení a se sběrem, zpracováním, přenosem a využitím dat na počítačích. Počítačové právo je v České republice kodifikováno v několika základních zákonech. Jsou to trestní zákon [247], zákon o dílech literárních, vědeckých a uměleckých (autorský zákon) [249], zákon o ochraně osobních údajů v informačních systémech [250], zákon o ochraně topografií polovodičových výrobků [251]. Právní předpisy týkající se počítačové problematiky u nás vznikly nebo byly rozhodujícím způsobem novelizovány po roce 1989. Dikce některých paragrafů není ještě zcela dokonalá,

nicméně zejména prostřednictvím trestního zákona lze poměrně uspokojivě postihnout většinu skutkových podstat trestných činů spáchaných v souvislosti s počítači.

Je úkolem vlád pečovat o bezpečnost informačních technologií? K této otázce autorka [77] vysvětluje přístup vlády USA. Snaha americké vlády zajistit národní bezpečnost odpovídala vždy mezinárodnímu postavení USA. Byly to proto vládní úřady, zejména úřady pod ministerstvem obrany, které v USA podporovaly a řídily pokrok v počítačové bezpečnosti již od počátků vývoje počítačů. Vysoce tajný *Národní bezpečnostní úřad (NSA)* byl ustaven již začátkem padesátých let. Jeho úkolem bylo zajišťovat hlavně komunikační bezpečnost se zřetelem na národní bezpečnost a dále vztahy mezi *Ministerstvem obrany USA* a civilními úřady, zabývajícími se počítačovou bezpečností, zejména *Národním úřadem pro normy a technologii*, a komunitou prodejců. V roce 1977 došlo také k vytvoření *Národního výboru pro komunikační bezpečnost*, jehož cílem bylo rozdělit odpovědnost za komunikační bezpečnost. *NSA* tak zůstala odpovědnost za ochranu klasifikovaných informací a informací vztahujících se k národní bezpečnosti a *Národní správě komunikací a informací*, podléhající *Ministerstvu obchodu USA*, odpovědnost za informace neklasifikované. Direktiva NSDD 145 z roku 1984 znovu rozšířila pravomoci *NSA*. Požadovala, aby federální úřady ustanovily politiku, postupy a praktiky zajišťující v počítačových systémech ochranu jak klasifikovaných, tak neklasifikovaných dat. Nové *Národní středisko pro počítačovou bezpečnost (NCSC)* spolu s *Radou COMSEC* pak bylo odpovědné za počítačovou bezpečnost v civilní vládní oblasti i v komerčním světě. K dalšímu přerozdělení odpovědností došlo znovu v roce 1987, kdy *Computer Security Act* definoval roli *NBS* (nově *NIST*) v ochraně citlivých informací a roli *NSA* omezil na její tradiční oblast, ochranu klasifikovaných informací. Stav informační bezpečnosti se nevyvíjel samozřejmě v jednotlivých státech zcela jednotně. Např. kalifornská legislativa požadovala již v sedmdesátých letech pro každé státní výpočetní středisko funkci pracovníka specializovaného na informační bezpečnost a *Ministerstvo financí USA* vyžadovalo pravidelnou kontrolu politiky na ochranu důvěrnosti. Jako reakce na skutečné události vznikly další iniciativy. Např. v souvislosti s výskytem internetového červa bylo např. ustaveno několik týmů, jejichž úkolem bylo reagovat na incidenty, jmenujme např. *CERT (The Computer Emergency Response Team), DDN SSC (The Defense Data Network Security Coordination Center) a CIAC (The Computer Incident Advisory Capability).* Odpovědnost americké vlády za počítačovou bezpečnost dokumentuje rovněž nařízení č. 200 *Národního výboru pro bezpečnost telekomunikací a informačních systémů (NTISSP)* z roku 1987, které požadovalo, aby federální úřady a jejich kontraktoři instalovali do roku 1992 u víceuživatelských systémů obsahujících klasifikované nebo neklasifikované, ale citlivé informace, volitelnou kontrolu přístupu a audit na vyšší úrovni tzv. *Oranžové knihy*.

Legislativa v USA v oblasti počítačové kriminality a bezpečnosti byla poměrně široce rozpracována již od počátků masového rozvoje výpočetní techniky. Pro možnost porovnání s vývojem úprav u nás uveďme podle [77] několik vybraných paragrafů úpravy *U.S.C*, které byly k dispozici v USA již v roce 1989. Jsou to paragrafy

-1029, zakazující podvodné činnosti ve spojení s použitím přístupových zařízení v mezistátním obchodě; zahrnující též počítačová hesla, telefonní přístupové kódy a kreditní karty,

-1030, který zakazuje vzdálený přístup s cílem defraudace v souvislosti s počítači federálního zájmu nebo vlastněnými federální vládou a dále zakazuje neautorizovaný přístup k počítači zaměstnancům společnosti,

-1343, zakazující používání mezistátních komunikačních systémů s cílem defraudace,

-2512, který zakazuje pořízení, distribuci, vlastnění a inzerci na průniková komunikační zařízení,

-2778, 2510, zakazující nelegální export software a dat, kontrolovaných *Ministerstvem obrany* a *Ministerstvem obchodu USA*,

-2701, který zakazuje nezákonný přístup k elektronicky uchovávaným informacím.

Připomeňme, říká autorka [77], že ani Evropa nebyla pozadu. Harmonizační snahy *Rady Evropy* vyústily v doporučení *Rady Evropy* o počítačovém zločinu z roku 1990. Vyjmenovává 8 povinných konkrétních typů zločinu, mezi nimiž je např. počítačový podvod nebo neoprávněný přístup, a 4 nepovinné, mezi něž patří např. změna počítačových dat nebo programů a neautorizované použití počítače. U nás ovšem výslovně počítačová ustanovení existují pouze v několika zákonech, a samostatný zákon o zneužití počítače naše právo nezná, potud [77].

3.3. Počítač jako předmět a prostředek trestné činnosti

Útoky proti software jsou považovány obecně za nebezpečnější než kriminalita týkající se hardware. Je jistě pravda, že např. zničení počítače je pro uživatele či provozovatele jistě závažným a zpravidla i finančně náročným problémem. Pokud se jedná skutečně jen o hardware, jde o škody napravitelné pořízením nové techniky. Je-li však přitom zničen nezálohovaný systém informací v počítači uložený, každý uzná, že škoda může být nenahraditelná. Počítač a jeho software, či informace v počítači uložené však nemusí být pouze předmětem (objektem) páchání trestné činnosti. Počítač bývá často též prostředkem takové činnosti. Doposud jsme tedy poznali, že aktivity, které lze charakterizovat jako trestnou činnost související s počítači, mohou být značně rozdílné, i co nebezpečnosti pro postižený subjekt. Lze je například rozdělit takto:

1)trestné činy ve vztahu k počítači, jeho příslušenství a jiným nosičům informací jako věcem movitým,

2)trestné činy ve vztahu k software, datům, uloženým informacím; počítač a jeho programové vybavení a data v něm jako cíl útoku, jako předmět trestného činu,

3)trestné činy při nichž je počítač prostředkem k jejich páchání,

4)útoky na nehmotný majetek, trestné činy ve vztahu k programu jako autorskému dílu.

Poslední dva typy útoků jsme obsahově zařadili do problémových okruhů popisovaných v dalších kapitolách.

3.4. Trestné činy ve vztahu k počítači jako věcem movitým

Pokud je předmětem nebo cílem počítač a jeho příslušenství jako věc movitá, skutková podstata je táž jako u trestných činů, spáchaných v souvislosti s jinými movitými věcmi. V daném případě může jít zejména o tyto trestné činy: §247 trest.zák.-krádež, §248 trest.zák.-zpronevěra, §250 trest.zák.-podvod, §251 a §252 trest.zák.-podílnictví, §254 trest.zák.-zatajení věci. Vlivem jisté výjimečnosti počítačů existují zvláštnosti, které činí problém skutkových podstat ještě poněkud složitější. Trestní zákon kromě uvedených ustanovení chránících jakýkoliv majetek obsahuje ještě speciální ustanovení postihující útoky na počítače jako nosiče informací. Jde o poškození a zneužití záznamu na nosiči informací podle §257a trest.zák.

Krádež podle §247 trest.zák. Odcizení počítače může být trestným činem podobně jako odcizení jiné movité věci. Specifičnost je zde dána faktem, že počítač většinou zahrnuje v sobě jednak *technické zařízení* včetně nosiče informací (hardware) a jednak *nehmotný obsah*, obecně zahrnující *programy* (software) a *data* (informace). Hodnota nehmotného obsahu může výrazně ovlivnit celkovou hodnotu odcizené věci. Ta může několikanásobně převýšit cenu samotného počítače. Celkovou výši škody nemusí zahrnovat původní úmysl pachatele, protože toho ve většině případů zajímá komerční cena samotného počítače, což by bylo z hlediska postihu nepodstatné. Podle platné zákonné úpravy se k okolnosti podmiňující použití vyšší trestní sazby může přihlédnout, jde-li o těžší následek, zaviní-li jej pachatel v tomto případě i z nedbalosti. A to i tehdy, když pachatel věděl, že může porušit nebo ohrozit zájem, ale z přiměřených důvodů spoléhal, že újmu v takové rozsahu nezpůsobí. Jinak ovšem vědomost o hodnotách skrytých v programech i datech je již dnes celkem všeobecná a lze ji předpokládat i u lidí odcizujících počítače.

Neoprávněné používání cizí věci podle §249 trest.zák. Podle platné zákonné úpravy bude potrestán ten, kdo se zmocní cizích věcí nikoliv malé hodnoty v úmyslu jich přechodně užívat nebo kdo na cizím majetku způsobí škodu nikoliv malou tím, že neoprávněně takových věcí, které mu byly svěřeny, přechodně užívá. Úpravu, jejíž podrobné znění je obsaženo v platném trestním zákoně, lze aplikovat i na případy zneužití počítačů. Pokud pachatel se zmocnil počítače a neoprávněně jej přechodně užívá nebo jej užívá v rozporu s dispozicí vlastníka, kterému tímto vznikla škoda, mohou nastat dva základní případy:

1)Na nosiči jsou informace a tyto pachatel neoprávněně užil. Jednání lze pak kvalifikovat podle ustanovení *§257a trest.zák.- poškození a zneužití záznamu na nosiči informací.*

2)Pachatel neoprávněně užívá počítač aniž by informace uložené na jeho nosiči neoprávněně užil, poškodil, učinil neupotřebitelnými, zasáhl do technického programového vybavení počítače. Tehdy může být jeho jednání kvalifikováno pouze podle §249 trest.zák.

Za škodu, případně prospěch lze v souvislosti s danou problematikou považovat
-mechanické nebo elektrické poškození,

-neoprávněné užívání počítače či počítačové sítě po určitou dobu, například též krádež strojového času,

-náklady vynaložené na preventivní kontrolu počítačového systému nebo programového vybavení poté, co bylo zjištěno neoprávněné vniknutí,

-náklady na obnovení zničených nebo poškozených dat a programů,

-podíly nákladů na provoz telefonní, či počítačové sítě v případech speciální modifikace nedovoleného užívání věci při *průniku do cizího počítače* prostřednictvím těchto sítí.

3.5. Trestné činy ve vztahu k datům, respektive k uloženým informacím

Jde o jednání pachatelů, které lze postihovat podle ustanovení *§257a trest.zák.- poškození a zneužití záznamu na nosiči informací.* Podle této úpravy bude potrestán ten, kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací

-a takových informací neoprávněně užije,

-nebo informace zničí, poškodí nebo učiní neupotřebitelnými,

-nebo učiní zásah do technického nebo programového vybavení počítače.

Pokud pachatel odcizí nosič informací (počítač), pak v takovém případě učiní informace pro oprávněného uživatele (např. vlastníka) neupotřebitelnými. V případě, že pachatel, který neoprávněně užívá počítač, smaže informace, byť částečně, jde o zničení či poškození informací. Pachatel může učinit informace neupotřebitelnými tím, že je zašifruje, např. zaheslováním počítače, systému, či souboru. Pro oprávněného uživatele (vlastníka), nezná-li příslušná hesla, mohou pak být příslušné informace nedostupné, i když data nadále na nosiči setrvávají.

Pokud někdo odcizí počítač (vypnutý) vybavený pouze operační pamětí, nemůže naplnit skutkovou podstatu trestného činu podle §257a trest.zák., neboť se nezmocnil žádných informací a tudíž jeho jednání se bude posuzovat podle §247 trest.zák. Většina počítačů je ale vybavena pevným diskem, na kterém jsou uloženy jednak programy, jednak data a jde tedy o odcizení počítače s nosičem naplněným informacemi. V takovém případě jde o spáchání trestného činu krádeže podle §247 trest.zák. v jednočinném souběhu s trestným činem podle §257a trest.zák., samozřejmě v závislosti na ceně naplněného nosiče informací.

Z ustanovení §257a trest.zák. vyplývá, že data či informace lze tedy neoprávněně užít, zničit, poškodit a nebo učinit neupotřebitelnými. Neoprávněné užití může mít souvislost s dalším nezákonným jednáním, postižitelným podle jiných ustanovení trestního zákona. Může jít například o vyzvědačství (§105 trest.zák.), ohrožení utajované skutečnosti (§106 trest.zák.), zneužívání informací v obchodním styku (§128 trest.zák.), nekalou soutěž (§149 trest.zák.) aj. Taková jednání lze ale postihnout v rámci jednočinného souběhu s trestným činem podle §257a trest.zák.

Z hlediska policejní praxe je největší objasněnost případů registrována v oblasti hospodářské kriminality jednoznačně u podvodů, viz např. [10]. Existují však trestné činy, které nejsou zdaleka tak početné, ale přináší je doba a z pohledu objasnění a prokázání jsou velmi složité. Do této kategorie zahrnujeme počítačovou kriminalitu, speciálně pak trestné činy poškození a zneužití záznamu na nosiči. Autor [10] uvádí tuto kasuistiku: Případ začal pro pracovníky brněnské hospodářské kriminálky tím, že ředitel jedné významné brněnské firmy, zabývající se prodejem a realizací počítačových sítí a informačních systémů podal trestní oznámení. Tato organizace totiž zjistila, že jí neznámý pachatel pomocí telefonní linky doslova vysál převážnou část databáze uložené v řídícím počítači, a to i přes veškerá ochranná opatření, včetně hesel. Ukradené informace měly pro firmu velkou cenu; šlo o připravované zakázky, rozpracovaná výběrová řízení, nabídky cen, seznamy obchodních partnerů a podobně. Celková škoda způsobená touto krádeží byla vyčíslena na 30 milionů korun. Kriminalisté ihned stanovili několik možných verzí případu, které byly za použití všech zákonných metod a prostředků postupně vylučovány. Po několika dnech se jim podařilo zjistit telefonní linku, z níž byla tato počítačová loupež uskutečněna a získali také několik nezvratných důkazů. Dovedly je až ke konkrétnímu pachateli, dvaačtyřicetiletému bývalému zaměstnanci poškozené firmy, který byl v té době zaměstnán u podniku, zabývajícím se obdobnou činností. Pachatel se po zatčení k činu přiznal. Spisový materiál byl předán vyšetřovateli s návrhem na zahájení trestního stíhání zmíněného počítačového „piráta“. Ne každý podobný případ však lze úspěšně objasnit.

Útoky proti programovému vybavení počítače a uloženým datům v pojetí studie [110] mohou nabývat několika forem. Od nejjednoduššího smazání programového vybavení až po zavedení viru do programového vybavení a následné ztráty programů a dat. Jak již bylo řečeno, skutková podstata tohoto jednání je vyjádřena v §257a trestního zákona - poškození a zneužití záznamu na nosiči informací. Vzniklou škodu touto trestnou činností lze však jen velmi obtížně vyčíslit. Finanční hodnotu informace lze vyjádřit nákladem vzniklým na její získání a pořízení nebo určitou hodnotou, kterou představuje pro vlastníka nebo uživatele. Rovněž následně vzniklá či hrozící škoda se může skládat z různých položek (nejen z dosud uvedených dvou). Např. také ze škody, která vznikla nebo hrozila vzniknout neuzavřením kontraktu, nemožností uskutečnit plnění závazků vůči druhé straně, vše následkem zničení nebo poškození dat. V těchto případech je vyčíslení vzniklé škody nebo hrozící škody velmi obtížné a může se mnohdy pohybovat na samé hranici spekulace. Vzhledem k neexistenci prakticky jakékoliv metodiky, každý experiment v této oblasti představuje základní kámen řešení daného problému. Při stanovení hodnoty dat pro vlastníka se soudní znalci pohybují v oblasti, která není dostatečně probádaná a zmapovaná.

Ke *změnám v programech, datech a technickém zařízení* [110] dodává, že pachatelé těchto trestných činů mění nejčastěji programy a data za pomoci jiných programů, virů nebo přímými zásahy programátora. Jedná se o tzv. *počítačovou defraudaci*, kvalifikovanou jako trestný čin poškozování cizí věci podle §257 trest.zákona. (hmotné vlastnictví) a §257a trest.zákona (duševní vlastnictví). V menší míře se pachatelé dopouštějí úprav v zapojení nebo v jiném technickém vybavení počítače nebo komunikačního prostředku. Pro stanovení

správného postupu vyšetřovatele při získávání informačních podkladů podmiňujících zahájení vyšetřování a současně i použití správné právní kvalifikace jednání pachatele je důležité zjistit, zda se pachatel rozhodl způsobit škodu, nebo získat prospěch, např. tím, že vymyslí způsob, jak prospěch získat, nebo zda svůj úmysl již uskuteční např. za pomoci zfalšovaných údajů v databázi apod.

Počítač i počítačová síť může být jednak *předmětem* trestného činu, jednak jeho *prostředkem*. Jako prostředek je počítač ideálním nástrojem k páchání celé řady trestných činů. Mnoho ustanovení paragrafů zvláštní části trestního zákona může do určité míry s počítačem a s jeho zneužitím k trestné činnosti souviset. Např. podle [24] §257a trest.zák. výhradně souvisí s počítačem, §152 a §178 mohou souviset s počítačem a §151 rovněž do jisté míry s počítačem souvisí, případně souviset může.

Pachatelé při průniku do databází mohou zneužívat též osobní údaje v nich obsažené. Proto adekvátní *ochrana osobních údajů v informačních systémech* je v současné době poměrně velmi aktuální. Zákon [250], o ochraně osobních údajů v informačních systémech upravuje zejména

-ochranu osobních údajů,

-povinnosti související s ochranou informací při provozování informačního systému, který nakládá s osobními údaji,

-odpovědnost provozovatele informačního systému a dalších fyzických a právnických osob, které se účastní provádění činností souvisejících s provozováním takového informačního systému.

Zákon [250] vymezuje některé pojmy, a to prakticky poprvé v českém právním systému. Jde zejména o termín *informace, informační systém, provozování informačního systému, zpracování informace, likvidace informace* aj. Klíčové ustanovení v §16 říká, že: *„Provozovat informační systém, který nakládá s informacemi, které vypovídají o osobnosti a soukromí dotčené osoby, jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech, lze pouze, stanoví-li tak zvláštní zákon, nebo se souhlasem žijící dotčené osoby, pokud je možné, aby tento projev vůle učinila. Jestliže nelze podmínku souhlasu splnit, lze s informacemi nakládat jen za předpokladu, že bude zachována lidská důstojnost, osobní čest, dobrá pověst a chráněno dobré jméno dotčené osoby.“*

Ustanovení §17 uvádí mimo jiné mezi povinnostmi provozovatele

-provozovat informační systém v souladu s účelem, pro který je systém zřízen;

-získávat informace rozsahem tomuto účelu přiměřené, zejména vystříhat se shromažďování nadbytečných údajů;

-ověřovat, zda informace, s nimiž informační systém nakládá, jsou přesné, a podle potřeby je aktualizovat;

-označit náležitým způsobem v informačním systému nepřesné nebo neověřené informace, neuchovávat nepravdivé informace,

-zamezit sdružování informací a informačních systémů sloužících k rozdílným účelům, pokud zvláštní zákon nestanoví jinak;

-získávat informace pro informační systémy náležitým způsobem;

-získávat informace pod krytím jiným účelem nebo jinou činností lze pouze, pokud tak stanoví zvláštní zákon;

-zajistit ochranu informací i celého systému před náhodným nebo neoprávněným zničením, náhodným poškozením, jakož i před neoprávněným přístupem nebo zpracováním;

-poskytnout jednou do roka bezplatně, nebo za přiměřenou úplatu kdykoli, každé dotčené osobě na požádání zprávu o informacích o ní uchovávaných v informačním systému, pokud zvláštní zákon nestanoví jinak.

Jak uvádí [199], tomuto poměrně novému zákonu nebyla zatím u nás věnována náležitá pozornost. Důvodů bylo několik. Neexistoval dohlédací orgán a kromě toho sankce za porušení byly až do poslední novelizace trestního zákona velmi mírné. V ustanovení §20 je uvedeno: *„V případě porušení povinnosti provozovatele uvedených v §17 vzniká oprávněné fyzické osobě vůči provozovateli nárok na:*

a)zdržení se takového jednání, odstranění závadného stavu, vydání bezdůvodného obohacení tomu subjektu, na jehož úkor bylo toto obohacení získáno, a poskytnutí zadostiučinění tomu, jehož porušení povinností poškodilo, na náklady provozovatele,

b)likvidaci informace,

c)doplnění informace, jedná-li se o informaci, která byla do informačního systému vložena se souhlasem dotčené osoby, nebo jestliže se jedná o zveřejněnou informaci,

d)zaplacení přiměřené peněžní úhrady, jestliže bylo porušeno její právo na zachováni lidské důstojnosti, osobní cti, dobré pověsti a na ochranu jejího jména pokud není postižitelná stávajícími občanskoprávními a obchodně-právními instituty,

e)zamezení přístupu k informacím v průběhu sporu, pokud orgán příslušný pro rozhodnutí sporu výjimečně nestanoví jinak; nárok se týká pouze sporem dotčených informací.“

Autor [199] považuje za důležité

-realizaci dalších potřebných právních úprav formou vydání prováděcích předpisů či zvláštního zákona, na něž se výše uvedený zákon vícekrát odvolává;

-zřízení příslušného inspekčního (dozorového) orgánu, který je zákonem předvídán a který by měl zajisté dostatek smysluplné práce.

3.6. Problematika virů

Napadení počítače virem je v současné době zřejmě nejčastější metodou útoku proti software, případně i hardware. Virem rozumíme určitý program, který má specifické vlastnosti velmi podobné jeho biologickému protějšku. Zde máme na mysli zejména jeho schopnost samokopírování do doposud nezamořeného nosiče a tedy i možnost postupného množení. Odtud pramení jeho označení. Počítačový virus není ovšem dílem přírody, nýbrž vědomé činnosti programátora, a to činnosti velmi kvalifikované. Jeho výtvor může zničit data, programové vybavení nebo i hardware. K infikování konkrétního počítače může dojít nejčastěji

-neúmyslně nedbalostí uživatele, který si přinese infikovaný program nebo data na disketě, z níž se pak vir přenese do počítače,

-propojením počítače na nějakou síť, např. prostřednictvím faxmodemové karty, napojením na internetovou síť atp.

Méně časté, i když nezanedbatelné svými následky jsou případy úmyslného zamoření počítačů v rámci určitého podniku, kdy pachatel se chce z nějakého důvodu pomstít zaměstnavateli. Jiné známé motivace spočívají v tom, že pachatel

-chce škodit za každou cenu, a to často i za cenu neúměrného rizika prozrazení a následného potrestání,

-je schopným programátorem, který se chce utvrdit v tom, že vir dokáže vytvořit a pak podlehne pokušení ho vyzkoušet v provozu,

-potřebuje léčit své komplexy a proslavit se jako tvůrce zvláště originálního viru a pustit ho např. jako trojského koně do světa, i když v takových případech jde většinou o slávu naprosto anonymní,

-je psychopatem, kdy např. si myslí, že prokáže lidstvu službu, když bude bojovat tímto způsobem s rozvojem výpočetní techniky a tím i s postupující globalizací světa, případně podle jeho mínění s nespravedlivým společenským řádem.

Ochrana proti virovým útokům je v podstatě založena na dvou aspektech, kdy uživatel

-je veden k úzkostlivé opatrnosti při práci s počítačem, zejména tam, kde dochází k velkému pohybu informací, dat, či distribuci programů ať již formou kopírování z disket či ze sítě, je si vědom nebezpečí virové nákazy a informuje v tomto smyslu své případné podřízené, či spolupracovníky,

-vládne prostředky antivirové ochrany, tedy systémy programů, které umožňují kontrolovat stav zamoření, případný výskyt virů identifikovat a následně zlikvidovat.

Nejlepší ochranou je pak kombinace obou aspektů se zavedením režimu soustavné antivirové profylaxe pomocí legálně pořízených antivirových systémů na všech svěřených počítačových nosičích.

Systémy antivirové ochrany jsou v současné době dovedeny k poměrné dokonalosti, která, ve spojení s aktualizací nově se vyskytujících případů, umožňuje proti virům účinně bojovat. Seznam virů v jedné z posledních verzí antivirové ochrany *F-Secure Antivirus* obsahuje více než 200 položek základních druhů virů, z nichž některé zahrnují i velký počet dalších odvozených virů, variant a mutací jdoucích do tisíců položek.

K nejběžnější destrukční činnosti pachatelů prostřednictvím virů. Podle studie [110], v souvislosti s útokem na programové vybavení a data počítače s možností jejich velmi pravděpodobné ztráty je zapotřebí pojímat nebezpečí destrukční činnosti počítačových virů vždy vážně. Počítačový virus je nenápadný malý program, který má při spuštění schopnost sám sebe rozmnožovat. Může

-napadat určité programy, zpravidla soubory s koncovkou COM, EXE, (ale není to pravidlem), tehdy je označován jako *souborový virus*,

-napadat určité oblasti disku (např. BOOT sektor), pak nese název *boot virus*,

-být rezidentně uložen v paměti počítače po celou dobu jeho chodu, jako tzv. *rezidentní virus*.

Při každém spuštění nakaženého programu (počítače nebo při každém použití diskety v disketové jednotce) nakazí virus další program, který je v jeho dosahu a který je dosud nenapaden. Virus uvnitř programů změní obsah a sled instrukcí, takže napadený program dělá něco jiného, než původně měl, i když se někdy tato skutečnost navenek neprojeví. Podle škodlivosti autor [110] dělí viry na tzv. „hodné“ a „zlé“. Zatímco „zlý“ virus se snaží uškodit uživateli za každou cenu, lhostejno, zda zničením hardwaru, nebo smazáním dat, „hodný“ virus obvykle provádí jen nějaký nevinný žertík. Problémem „hodných“ virů však zůstává jejich nekontrolovatelné množení, kdy zamořením počítačů mohou způsobit značné potíže. Z informačního hlediska jsou proto oba typy škodlivé. Daleko razantnější, a tím také společensky nebezpečnější, jsou logické útoky, kdy pachatel využije vlastností počítačového systému, zejména jeho slabin. Jedná se o tzv. logické bomby, kdy se programy aktivují za určitých podmínek, např. po určité době nebo po spuštění určitého souboru a poté vykonávají i svou vlastní „virovou“ činnost. Odpovědnost pracovníka, který zavirování způsobil z pohledu §257a trestního zákona, předpokládá úmyslné zavinění stavu, kdy dojde ke ztrátě dat. V případě, že se virovou nákazou počítače chce nějaká osoba např. pomstít, je nasnadě, že měla úmysl dosáhnout poškození dat, programového vybavení nebo zničení hardwaru počítače. Pokud ale pracovník přinesl do zaměstnání disketu s hrou, na níž byl virus, o němž nevěděl, a došlo k zavirování počítače se všemi negativními důsledky, je bezpochyby jeho jednání neúmyslné. Ale paradoxně tedy dle uvedeného zákonného ustanovení nepostižitelné, i když ve svých důsledcích stejně destrukčně působící jako při úmyslném zavirování počítače. Samozřejmě může dojít ke zničení dat a programového vybavení také vlastním fyzickým poškozením nebo zničením počítače či jeho paměťového média. Avšak užiti fyzického násilí v předchozích případech nebereme v úvahu.

Šíření počítačových virů v Internetu. Světoví experti varují před rostoucím rizikem počítačových virů v Internetu. Zástupce *Spolkového úřadu pro bezpečnost v informační technice* SRN poukázal na nové ohrožení tzv. *makroviry*, které mohou být nepozorovaně ukryty v textu dokumentů a elektronickou poštou v několika vteřinách rozšířeny do celého světa. Postačí, když uživatel počítače vyhledá a zobrazí určitý text a ukryté makroviry jsou schopny zahájit ničivou práci. Konkrétní „škodící funkce“ mohou být u každého viru jiné. Nebezpečí makrovirů, jejichž počet se měsíčně zvyšuje přibližně o 25 nových exemplářů, spočívá především v jejich nenápadnosti. Proti těmto virům se bojuje hůře než proti tzv. *boot-virům*, které se aktivují pouze při zahájení činnosti počítače se „zavirovanou“ disketou. Za obzvláštní nebezpečí lze považovat skutečnost, že makroviry je možno vytvářet s pomocí nejjednoduššího programovacího jazyka *Basic*, zatímco klasické viry, jichž je dnes známo asi 12000, mohou být vytvořeny jen zkušenými programátory. Podle technického ředitele *Evropského institutu pro počítačový výzkum* jen v SRN je dnes vynakládáno na preventivní opatření a odstranění následných škod mnoho finančních prostředků, odhadem asi více než 1 miliarda DEM. V budoucnosti se situace ještě zhorší, neboť v rámci balíku programů *Office97* je zpřístupněn velmi výkonný makrojazyk, který rozšiřování makrovirů ještě dále usnadní. V této souvislosti je možno vytknout výrobci programů, firmě *Microsoft*, že tvorba obranných

mechanismů v tomto softwaru je zpožděna, což může ulehčit útoky zavlečených makrovirů. Internet není jen transportní médium pro útočné počítačové viry. Tato síť také dosud zcela legálně slouží výměně odpovídajících programů mezi konstruktéry virů. Profesor informatiky na hamburské univerzitě označil za příčiny tohoto nepříznivého vývoje příliš ukvapený transfer nových informačních technologií. Nové datově-technické produkty musí být nejdříve velmi intenzivně přezkoušeny z hledisek bezpečnostních aspektů a následovně optimalizovány ještě před rozšířením do světa.

**

Viry a červi, shrnutí aktuálních poznatků. Velmi přehledně pojednává o virech z hlediska počítačové bezpečnosti a informačního soukromí autor studie [9]. Poznamenejme, že i zde však vznikají určité potíže s definicemi. Počítačové viry se objevily poprvé v 80. letech. Tehdy prováděl Fred Cohen pokusy na počítačích s operačním systémem *Unix* pro jeho doktorskou práci a poprvé použil termín, který se od té doby vžil. V té době o virech toho nebylo mnoho známo, někteří odborníci (například Peter Norton) dokonce tvrdili, že takové programy principiálně nemohou existovat. Kusé zprávy o virech se tu a tam objevovaly v nedělních přílohách novin. Situace se změnila až po nástupu osobních počítačů *IBM PC*. Ty totiž přinesly jednoduchý operační systém, binární kompatibilitu programů a hlavně masovou výměnu dat a programů mezi uživateli. To všechno jsou faktory, bez nichž by počítačové viry nemohly pracovat. Obecně je možno říci, že virus je program, který je schopen přidat (modifikovanou) kopii sebe sama k jiným programům. Z této jednoduché (a ne úplně přesné) definice vyplývá i princip, jakým počítačové viry fungují. Aby mohly viry pracovat, musí se „napojit“ na nějaký kód, který je v počítači realizován a který je zároveň sdílen mezi různými počítači. Pro svět personálních počítačů z této definice vyplývají i možnosti konstrukce různých typů počítačových virů, zejména

-virů, které napadají programy uložené v souborech (aplikační programy),

-virů, které napadají systémovou oblast disku,

-makrovirů, jako relativně nového fenoménu.

Z uvedené definice vyplývá i to, že vir nemusí obsahovat žádnou složku, která by způsobila destrukční činnost, i když samo šíření viru může být škodlivé. Naopak, ne všechny programy, které destrukční činnost obsahují, jsou počítačovými viry.

Jak uvádí [9], prvním virem, který byl vytvořen pro IBM PC, byl boot vir *Brain* v roce 1985. Prvním virem, který se objevil u nás, byl v roce 1988 vir *Vienna*, následován o rok později viry *Cascade a Dark Avenge.* Tehdejší viry byly velice jednoduché. Až s postupem doby se objevovaly i mnohem komplikovanější struktury, které souvisely zejména s „bojem“ autorů virů proti úspěšným antivirovým programům. Objevily se například

-paměťově rezidentní viry s technikami *„stealth“* proti jejich detekci,

-polymorfní viry, které jsou v každé své kopii jinak kódované, takže není možno vybrat jednoduchý vyhledávací řetězec,

-multipartitní viry, které napadají jak soubory, tak systémovou oblast disku apod.,

-speciální viry, které se vyskytly zejména v poslední době, používající techniky přímo namířené proti heuristické analýze.

Nejdůležitějším faktorem, který nelze přehlédnout, je však četnost existujících virů. Jestliže v roce 1988 existovalo kolem deseti různých druhů virů, na konci roku 1996 jich již bylo více než deset tisíc. Každoročně tento počet překotně narůstá. Ne všechny jsou samozřejmě původní. Velká většina je jen modifikovanou variantou jiného viru, a ne všechny se volně šíří mezi uživateli, řada z nich toho není mimochodem vůbec schopna, protože obsahují spoustu chyb. Podle autora [9], volně mezi uživateli se šíří v současné době asi 500 druhů virů. Jejich seznam, na jehož vytváření se podílejí odborníci z celého světa, je pravidelně publikován na Internetu.

K *současnému stavu* virové problematiky u nás lze podle [9] říci, že s nástupem nových operačních systémů typu *Windows 95* a *Windows NT* dochází i ke změnám ve struktuře virů. Klasické souborové viry jsou částečně na ústupu, což je dáno i tím, že programy narůstají na objemu a proto se daleko méně distribuují či „vyměňují" na disketách. Také výskyt *boot* virů poněkud poklesl. O to větší nebezpečí mohou znamenat *makroviry*, které našly zejména v aplikaci *MS-Word* ideální prostředí pro svoje působení. Makroviry využívají toho, že moderní aplikace jsou mocným nástrojem a ve svých „datových" souborech neuschovávají pouze čistá data, ale i nástroje na jejich další zpracování. Příkladem mohou být makra v *MS-Wordu*. Tato makra jsou bohužel uložena ve stejném dokumentu jako text a řada z nich může být vyvolána automaticky, např. se spuštěním Wordu, s otevřením dokumentu a podobně. Další mohou být automaticky spjaty s položkami menu, s ikonami na pracovní liště či s libovolnou klávesou. Existuje jednoduchý způsob, jak makro zkopírovat z dokumentu do globální šablony, odkud pak vir může být aktivován při každém následujícím použití MS-Wordu. Makra jsou psána v jazyce *WordBasic* či nověji přímo ve *VBA* (Office 97). Tyto jazyky jsou velmi mocné a přitom poměrně jednoduché. Navíc díky elektronické poště si řada uživatelů vyměňuje dokumenty velmi intenzivně, a proto v posledním roce makroviry zaznamenaly neuvěřitelný nárůst výskytu. Zvyšuje se i počet nových druhů, přírůstky v posledních měsících se měří na stovky a jejich počet již přesáhl 700. Mimo jiné je to způsobeno i samotným MS-Wordem, protože za určitých podmínek může dojít k poškození maker, přičemž vir zůstává nadále funkční. U nás je situace zatím poměrně klidná, protože lokalizace MS-Wordu na české prostředí byla natolik důkladná, že většina makrovirů v prostředí českého Wordu nefunguje. Přesto se u nás první makroviry objevily již v roce 1995 a v posledních několika měsících se vyskytly masově některé makroviry, které jsou schopny se šířit i v lokalizované verzi, jako např. vir *CAP* nebo *Bertik*. Bohužel, s nástupem *Office 97* se situace pravděpodobně výrazně zhorší, protože lokalizace proběhla poněkud jiným způsobem. Lze tak i u nás v blízké budoucnosti čekat velkou vlnu makrovirů. MS-Word není jedinou aplikací, pro kterou existují makroviry, i když je jistě tou nejpostiženější. Makroviry existují i pro *MS-Excel, AmiPro, Lotus* aj. Svým rozšířením a způsobem využití a bohužel i svou podporou zůstane ale *MS-Word* prioritním cílem makrovirů i v budoucnu.

Pokud jde o *viry a červy na Internetu*, zmínili jsme se zatím o elektronické poště a Internetu v souvislosti s makroviry. Podle [9], při určité opatrnosti může být používání Internetu poměrně bezpečné. Novou verzi freewarového (zdarma legálně šířeného) programu není třeba hledat na místním systému *BBS*, kam ji mohl nahrát kdokoli a program samotný už

toho mohl mít hodně za sebou; na Internetu lze nalézt poslední verze programů pocházejících přímo od autorů. To samozřejmě nezaručuje, že se zde vir nemůže vyskytnout, ale riziko je mnohem nižší. Internet nabízí i značnou podporu ze strany antivirových firem. Jde o nejnovější informace o virech, aktualizace antivirových programů, vlastní produkty a podobně. Na druhé straně je možno na Internetu nalézt i velké množství virů, včetně zdrojových podob. Z minulosti je známo, že problémy mohou způsobit viry, zaslané do diskusních skupin či do šířených dokumentů s různými informacemi. Vlastní běh Internetu viry ovlivní jen těžko. Internet je totiž příliš rozmanitý, používá různé počítače s různými operačními systémy. Přesto již v minulosti k jednomu velkému útoku došlo; jde o nechvalně známý program *Roberta Morrise,* který v roce 1988 postihl asi 6000 počítačů. Byl to spíše *červ*, program který nenapadá jiné programy, ale využívá slabin sítě a šíří se z jednoho počítače na druhý. V souvislosti s Internetem se hovoří i o *celkové bezpečnosti* a využití nových technologií, jako např. *Java, ActiveX* a pod. Ani tady nehrozí masové vytváření virů, spíše ohrožení bezpečnosti formou *trojských koní*, tj. programů, které mají v sobě zabudovánu určitou maskovanou část, jež se aktivuje po splnění určité podmínky, např. k určitému kalendářnímu datu apod. K Internetu je tedy nutno přistupovat opatrně a měla by se dodržovat táž pravidla, jaká platí v běžném počítačovém provozu.

Výhledově vzato, jak uvádí [9], počítačové viry z našeho života bohužel v nejbližší době nezmizí. Nové viry se budou objevovat i nadále, nové operační systémy a technologie budou přinášet nové a nové problémy, kterým se budou muset antivirové firmy i uživatelé přizpůsobit. Zatím se však vždy našlo odpovídající řešení i v případech důmyslně rafinovaných virových deliktů, a tak tomu bude snad i v budoucnu.

Z hlediska *ochrany a bezpečnosti informačního soukromí* autor [9] na základě provozních zkušeností doporučuje

-zásadně nespouštět žádné programy s nejasným původem;

-diskety, používané v počítači zabezpečovat proti přepsání; originální diskety před instalací programu opatřit ochranou proti zápisu, zkopírovat a uložit na bezpečné místo;

-diskety zanechávat v jednotce jen po nezbytně nutnou dobu; po ukončení práce je okamžitě vyjímat, pokud na ně nebude dále zapisováno, opatřit je ochranou proti zápisu;

-zkusit přehodnotit postoj k nelegálně získanému programovému vybavení; jeho cesta od výrobce až na konkrétní počítač mohla být dosti svérázná a jeho použití je navíc nezákonné!!;

-vypnout zavádění systému z disketové jednotky, pokud to *Setup* příslušného počítače umožňuje;

-nikdy nepouštět k počítači cizí osoby, vhodné je používat prostředky pro řízený přístup k počítači,

-používat veškeré dostupné prostředky pro antivirovou prevenci, vhodně jim nastavit deklarace a pravidelně je aktualizovat;

-realizovat pravidelné antivirové profylaxe;

-pozorně sledovat chování počítače a včas reagovat na veškeré odchylky od normálního stavu, jako např. podivná hlášení, zvuky, chyby apod.;

-často a pravidelně zálohovat data, či jiné vlastní výtvory;

-v případě nejistoty při řešení problémů, vyhledat pomoc specialisty; často neodborný zásah způsobí větší škody, než samotný vir!

4. Útoky směřující ke zneužití počítačů, dat a jiných informací

Sestaveno převážně z pramenů: [23], [35], [38], [58], [62], [84], [97], [110], [116], [139], [155], [197], [199], [200], [201], [205], [206], [216], [226], [233], [250], [259].

4.1. Trestné činy při nichž je počítač prostředkem k jejich páchání

Do této skupiny bychom mohli zařadit počítačové finanční a investiční podvody, finanční hry, hry hazardního charakteru, kde se jedná o náročné požadavky na rychlé nebo přímo interaktivní zpracování vložených informací. Ať již formou vložených jednotlivých dat, nebo i celých datasystémů. Sem patří též defraudace ve finančních institucích, kde počítače podstatně snižují riziko odhalení.

Jak uvádí [110], nejsnadnější, ale také nejúčinnější způsob získaní finančních prostředků prostřednictvím počítačů je manipulace s daty. Může být zaměřena na různé oblasti lidské činnosti, např. na úpravu účetních dokladů, evidenčních údajů o skladovaném zboží apod. Činnost pachatele spočívá především v tom, že vymaže nebo přemaže údaje na magnetickém médiu, což nezanechává prakticky žádné stopy. Využívá se i skutečnosti, že pracovníci obvykle považují výsledky z počítače za správné. Mnohdy slyšíme: „...to počítač, my za nic nemůžeme...“, což ovšem zdaleka u zasvěcených nenachází pochopení. Bohužel však asi též na tomto faktoru závisí vysoká míra latence páchání trestné činnosti za současného využití neznalosti počítačové techniky u některých občanů.

Pachatelé této trestné činnosti mohou také měnit data úpravou dokladů, z nichž jsou data pořizována, nebo jejich úpravou přímo na médiu, na němž jsou uložena. Upravit data mohou také při výpočtu v počítači nebo na výstupní sestavě. Nejčastější formou podle [110] je změna vstupních dokladů, nebo pořízení jiných dat do počítače. Pachatel obvykle využívá situace, že pracovník, který na počítači data zpracovává, je může změnit před zpracováním, v průběhu zpracování, nebo po něm. Musí však také upravit ostatní informační soustavy, s nimiž jsou propojena logickými vazbami. Trestná činnost prostřednictvím počítačových prostředků, kvalifikovaná jako trestný čin podvodu podle §250 trest.zákona se vztahuje především k vnitřnímu kontrolnímu systému organizace, kterým je např. správné finanční účetnictví, fungování vnitropodnikové kontroly, včasná reakce na zjištěné nedostatky o možnostech zneužití apod. Tento typ kriminality se vyskytuje především ve finančních institucích, jakými jsou banky, spořitelny, pojišťovny apod. Převážně se jedná o podvody realizované formou neoprávněného převodu finančních prostředků na účet, který byl k tomu zvlášť založený. Pachateli jsou většinou vlastní zaměstnanci finančních institucí napadající počítačové systémy chráněné identifikací a autorizací. Jsou napadány automatizované i neautomatizované systémy, které jsou nedostatečně vybaveny pro rychlé zjištění trestné činnosti a jeho dostatečné zadokumentování. Odpovědní pracovníci organizace se obvykle domnívají, že v jejich organizaci byl zaveden bezpečný systém, přičemž se např. odhalí postrádání komplexní bezpečnostní ochrany. Zahraniční statistiky podle [110] také dokazují, že pravděpodobnost odhalení trestné činnosti spáchané zneužitím počítačových prostředků je

značně nízká. U tohoto druhu trestné činnosti nelze jen spoléhat na bezpečnostní ochranu počítačových systémů, ale je třeba zavést kvalitní personální práci podniku, vnitřní systém kontrol a celkovou bezpečnost managementu.

Ve stati [139] je uveden tento případ: *Na zcizený občanský průkaz bylo v pobočce jisté banky založeno konto neznámou osobou. Na toto konto bylo roku 1993 neoprávněně převedeno zhruba 1,2 mil. Kč z jiného konta. Poté neznámá osoba vybrala z daného konta 1,2 mil. Kč a další osoba následně provedla storno převodu, čímž vznikl debet ve výši 1,2 mil. Kč.* V případě vyšetřování zapůsobila pravděpodobně i náhoda a zrovna páska se záznamy konfigurace počítače, pomocí něhož byl spáchán trestný čin, byla poškozena a nebylo možné ji přečíst. Zmíněný trestný čin byl spáchán v prostředí počítače *ASI4OO* od společnosti IBM. Jeho operační systém *OSI400* byl již od samého počátku navržen jako operační systém, jehož součástí jsou bezpečnostní mechanismy. To bylo také možná příčinou až slepé důvěřivosti některých vedoucích pracovníků v tento systém. V dané bance chyběla jednoznačnost identifikace a autentizace uživatelů a správců - bezpečnost a průkaznost transakcí byla založena na velmi nespolehlivém prvku. Totiž na identifikaci prostřednictvím zadání jména a hesla, které bylo a je možné používat po určité časové období (týden, měsíc atd.). Tato bariéra byla překonána odposlechnutím hesel při přenosu po počítačové síti. Podle zjištěných skutečností provozovatel bankovního systému neprovedl v dostatečném rozsahu opatření, která by vyloučila nebo snížila na přijatelnou úroveň rizika plynoucí z používání informačního systému. V dané bance (nejenom v dotyčné pobočce) chyběla v době spáchání trestného činu mimo jiné bezpečnostní pravidla pro provoz bankovního systému, pravidla pro konfiguraci serverů (tj. řídících síťových počítačů, jakési centrály sítí) a bankovních aplikací, nebyly jasně odděleny pravomoci systémového a bezpečnostního administrátora, nebyl zajištěn a evidován přístup k počítačové síti. Na základě podkladů, které poskytl vnitřní audit banky, a na základě prvotního šetření vznesl vyšetřovatel proti pracovníkovi, pod jehož profilem (kód uživatele a heslo) bylo realizováno storno, obvinění. A to pro zpronevěru podle §248 odst.1, 4 trest. zák. a pro poškození a zneužití záznamu na nosiči informací podle §257a odst.1, 3 trest. zák. Během líčení u krajského soudu byla obhajobou všechna obvinění vyvrácena. Rozsudkem krajského soudu byl dotyčný zaměstnanec zbaven obvinění ve všech bodech obžaloby, což po odvolání státního zástupce potvrdil i Vrchní soud.

S rozvojem nabízených služeb, jako je například *homebanking* v souvislosti s elektronickým převodem peněz do kterékoliv části světa během několika okamžiků, zvyšuje se náročnost na bezpečnostní opatření proti zneužití. V případě spáchání trestného činu je ztíženo stíhání pachatele, protože ten se může nacházet v jiné zemi než poškozený a než bylo místo činu. Je zřejmé, že z pohledu jednotlivých států přitom sehrává negativní roli i doposud nejednotná legislativa.

Úmyslné infikace počítačovým virem patří rovněž k případům trestné činnosti, při níž je počítač nástrojem páchání těchto deliktů. Počítačů je rovněž využíváno v kriminálním prostředí k dosažení vysoké věrohodnosti při padělání a zhotovování falešných papírů, platebních instrumentů a jiných dokladů.

Užití počítače k páchání další trestné činnosti je podle [110] druhou oblastí základního rozdělení této formy počítačové kriminality. Zahrnuje kriminální jevy, při nichž je počítač nástrojem pachatele k páchání další trestné činnosti, která již není vázána na výpočetní techniku, programy nebo data. Typickým představitelem této oblasti je využití výpočetní techniky k modelování situací, které mohou nastat při páchání trestného činu. Jedná se však o činnost velmi náročnou, kterou v dobré kvalitě zvládá pouze odborník zabývající se problematikou modelování situací.

4.2. Zneužití informací podle typu újmy postiženého

Útoky směřující ke zneužití dat a dalších informací, ať jsou motivovány zištnými důvody či nikoliv, nutno řadit k formě počítačové kriminality, která zasluhuje mimořádné pozornosti s ohledem na její případné dalekosáhlé následky. Podle dostupných pramenů lze tyto útoky rozdělit podle různých hledisek, např. podle typu újmy postiženého, na

-zneužití personálních informací, které může způsobit újmy postižené osobnosti, morálního nebo i hmotného charakteru;

-zneužití informací obchodního a průmyslového charakteru s dopadem na prosperitu závodu, podniku, i vyšších organizačních jednotek, případně celých průmyslových odvětví; v dostupné literatuře [84] lze nalézt příklady problematiky tzv. průmyslové špionáže, ap.;

-machinace finančního charakteru, např. při převodech peněz, kdy dochází k finanční újmě jednotlivce či právnické osoby, peněžního ústavu ap.; v některých případech velkých bank může být újma zanedbatelná ve vztahu k obhospodařovaným finančním objemům, a tím i tíže objasnitelná; takové případy jsou známé např. z výzkumu tzv.kriminality bílých límečků [226], kdy programátor opakovaně převáděl na své konto zcela zanedbatelné částky vzniklé předpisovým zaokrouhlováním zpracovávaných položek, čímž způsobil do doby odhalení zaměstnavateli škodu, sice nevelkou, avšak naplňující skutkovou podstatu trestného činu;

-zneužití informací pro jiný než finanční profit, vydírání atp;

-útoky způsobující jiné další újmy.

V boji proti těmto útokům můžeme užít bohatšího výběru technických prostředků než při potírání útoků proti hardware, zejména pokud jde o omezování neoprávněného přístupu do počítače, sítí či systémů. Souhrnně tuto problematiku nazýváme *počítačovou bezpečností*. V našem nástinu ji věnujeme zvláštní kapitolu.

Trestněprávní aspekty zneužívání informací. Jak uvádí [110], v právních systémech bychom těžko našli některé z odvětví, kde by nebyla alespoň zmínka o ochraně informací nebo informačních systémů. Příslušná ustanovení nalezneme v občanském, obchodním, pracovním, správním právu a pochopitelně v právu trestním. Některé aspekty se objevují současně i v různých odvětvích. Např. osobní údaje jsou chráněny podle ustanovení občanského zákoníku (ochrana osobnosti) v zákoně o ochraně osobních údajů v informačních systémech, ale i v trestním zákoně apod. To je však v povědomí občanů málo známo a tím i

rozlišováno. Proto často dochází k jejich rozčarování, pokud se dovědí, že svůj problém musí řešit občanskoprávní cestou a nikoli trestněprávně. V této souvislosti lze se důkladněji poučit studiem příslušných pasáží publikace [116]. Kromě toho velmi užitečná jsou i pojednání [199], [200], týkající se problematiky počítačového práva. První případy trestných činů spáchaných pomocí výpočetní techniky se u nás vyskytly koncem sedmdesátých a v průběhu osmdesátých let. To ještě nebyly v masovém měřítku užívány osobní počítače, nýbrž hlavně samočinné počítače velké, sálové. Rozvoj a masové nasazování osobních počítačů a jejich postupné propojování do sítí v devadesátých letech vedlo postupně k pochopení skutečnosti, že éra počítačové kriminality začíná i u nás. Bohužel tuto skutečnost lze z pohledu počítačové kriminality ze stávajících databází jen velmi těžko kvantitativně podchytit. Konkrétně např. pro *poškození a zneužití záznamu na nosiči informací* podle §257a trest.zák. je v databázi Ministerstva spravedlnosti České republiky, speciálně v trestní statistice státních zastupitelství, za rok 1998 (1997;1996) registrováno pouze celkem 22 (15;6) trestných činů, stíhaných osob pak 14 (14;6); obžalovaných osob 6 (14;6), trestní stíhání bylo zastaveno v 8 (0;0) případech. V trestní statistice soudů dále figurují k danému trestnému činu pro rok 1998 (1997;1996) tyto údaje: *odsouzeno osob 0 (1-peněžitý trest; 1-peněžitý trest), zproštěno celkem 1 (0;0), zastaveno celkem 2 (1;0), amnestie 2 (0;0),* týkající se celé databáze pro Českou republiku. Průměrná délka soudního řízení téhož paragrafu v roce 1998 (1997;1996) byla u nás 269 (33;15) dní. Ani za rok 1999 nejsou údaje statisticky významně odlišné: stíháno 11 osob, žalováno 7, odsouzeno 2, skutky 6.

4.3. Internet a zvláštnosti spojené s jeho provozem

Dlouhodobé technické zaostávání v oblasti užívání počítačové techniky se po roce 1989 začalo rychle odstraňovat. Naše legislativa měla v tomto období určitou výhodu v porovnání s vyspělým světem. Mohli jsme se totiž poučit z praktických zkušeností v těchto zemích a přizpůsobit jejich řešení našim podmínkám.

Jak například uvádí autor studie [233], dnes stojíme před dalším relativně novým a nejen právním problémem - počítačovou sítí s názvem *Internet.* Internet nesmírně zjednodušuje globální komunikaci. V pohodlí domácího prostředí lze „listovat“ v nabídkách cestovních kanceláří, přečíst si denní tisk, zúčastnit se diskusí k určitému tématu, posílat dopisy svým známým kamkoliv na světě atp. To je jen krátký výčet možností, které poskytuje Internet. Internet má však i svou negativní stránku. V této počítačové síti se šíří i informace podněcující k rasové nenávisti, pornografie nejhrubšího typu, včetně dětské, porušují se autorská práva atd. Internet přinesl civilizaci konce 20.století informační revoluci. Jako prostředek komunikace nabízí několik variant služeb na principech vztahu *klient-server*, kdy uživatelé mohou např. přenášet soubory z jednoho stroje na druhý (prostředky *ftp*), nebo si otevřít určitou relaci na stroji, který je fyzicky vzdálený stovky kilometrů (*telnet*). Volnou analogií Internetu je telefonní síť, telefonem je v tomto případě počítač klienta a centrálou příslušný server.

WWW (World Wide Web) webovská technologie je založena na myšlence hypertextu, rozšiřovaného na hypermedia. Hypermediální dokumenty obsahují hyperlinky nejen na text, ale i na jakoukoliv jinou formu záznamové informace - zvuky, obrázky, filmy, viz např. [155]. Uživatel hypertextu nepotřebuje znát adresy, ale jen to, co hledá, např. název firmy, výrobku, tématu atp. Termínem *e-mail* rozumíme elektronickou poštu, která pomocí individuálně zvolených adres umožňuje komunikaci uživatelů Internetu mezi sebou. Může se jí přenášet nejen text, ale i obrazový materiál. Internet má tyto zvláštnosti:

1)Z pohledu práva je nejdůležitějším to, že Internet jako informačně-komunikační síť nikdo nevlastní. V důsledku toho zodpovědnost nemůže nést provozovatel jako v případě jiných hromadných informačních prostředků. Např. v televizi nebo tisku nese zodpovědnost za obsah informací provozovatel, resp. vydavatel příslušného hromadného informačního media.

2)Do Internetu se může dostat libovolný subjekt, který vlastní nebo obsluhuje počítač připojený na tuto síť. S tím mohou jít ruku v ruce právní problémy dotýkající se trestního práva, autorského práva, obchodního práva, ochrany dat ap.

3)Možnosti Internetu přesahují hranice jednotlivých států. Je proto žádoucí, aby právní úpravy *de lege ferenda* v této oblasti byly co nejvíce unifikovány. Zatím v Evropské unii neexistuje žádná speciální úprava týkající se Internetu. Nepřímo se dotýkají Internetu pouze např. směrnice [201].

Možnosti zneužití Internetu jsou poměrně široké, např. podle [259], v roce 1998 se italským policistům podařilo odhalit síť obchodníků s lidskými orgány, kteří inzerovali své „zboží“ na Internetu, a zatknout jednoho ze zprostředkovatelů. Vyšetřování tohoto případu probíhalo již od okamžiku, kdy nejmenovaný italský lékař policii oznámil, že pravděpodobně omylem dostal e-mail, v němž mu kdosi za 30 000 marek (v přepočtu necelých 600 000 korun) nabízel ledvinu.

Negativní postoje některých občanů vůči Internetu převládají podle [216] u starších lidí. Většina obyvatelstva neodsuzuje celosvětovou počítačovou internetovou síť, přestože si uvědomují, že jejím prostřednictvím lze šířit i pornografii, rasovou nenávist či násilí. Vnímají ho především jako téměř nevyčerpatelný zdroj informací. Podle průzkumu agentury *AMD* převládají negativní postoje vůči systému Internet především u starších občanů České republiky. Internetu nevěří, protože propaguje násilí a pornografii, 35 % lidí starších šedesáti let. Naopak u osmnácti až třicetiletých je to zhruba 20 %. Nedůvěra vůči Internetu roste s nižším stupněm vzdělání. Negativně se na nejrozšířenější počítačovou síť na světě dívá deset procent vysokoškoláků, u vyučených už je to 30 %. V poslední době se stále častěji ozývají hlasy volající po cenzuře internetovských stránek. Naposledy poté, co nizozemská policie odhalila síť, která šířila prostřednictvím Internetu dětskou pornografii do celého světa. Šetřením dětské pornografie se zabývá i policie v České republice. Jeden z českých uživatelů Internetu, vystupující pod pseudonymem *Larry Flynt*, umístil na stránky *XOOM* mimo jiné kolem třiceti dětských pornografických fotografií a odkazy na ně rozesílal na volně přístupné adresy. Právě dostupnost odkazů na pornografii bývá nejsilnější zbraní v cenzorském tažení. Ačkoliv je většina služeb placených, najdou se i neplacené. Na obranu Internetu se postavil

spisovatel, publicista šéfredaktor internetového listu *Neviditelný pes* Ondřej Neff. „Je zavrženíhodné, pokud se vina za šíření pornografie přisuzuje samotnému Internetu, jelikož je to otázka zločinu, nikoli informačních technologií. Prezentace jakéhokoli produktu na této celosvětové síti je otázkou osobní odpovědnosti jeho tvůrce," řekl Ondřej Neff.

Ve světové literatuře je v posledním období publikována řada článků, ve kterých se experti zamýšlejí nad nebezpečím zneužití počítačové sítě Internet k provádění trestné činnosti. Autoři se zabývají též možnostmi orgánů činných v trestním řízení tyto nelegální aktivity odhalovat a trestat. Jako velmi závažné riziko je uváděno využití Internetu k šíření zpráv, což umožňuje zločincům komunikovat bez jakékoliv možnosti kontroly ze strany státních institucí.

Internet nástrojem zločinů. Jak uvádí autor sdělení [206], nelze se divit, že ta část populace, která dává přednost nelegálním příjmům před prací, se dokáže velmi rychle adaptovat na nové podmínky a používat nejmodernější prostředky. Pro ni je totiž tato adaptace základem přežití. Staré triky jsou brzo neúčinné, a tak je nutné hledat nové. Jak se zdá, na Internetu je jich k dispozici celá škála. Proto se i Internet stal zajímavou alternativou pro různé skupiny i jednotlivce, kteří se zabývají nezákonnými aktivitami. Protože tvůrci legislativních norem (parlamenty, vlády apod.), stejně jako výkonné orgány (policie, soudy, vyšetřovatelé atd.) téměř všech zemí světa, nemohou technicky vzato být vždy v předstihu, mají tato individua volné pole působnosti. Díky svým komunikačním prostředkům a rychlosti je Internet pro některé formy zločinu ideálním nástrojem. Kolem Internetu a elektronických způsobů komunikace se tvoří navíc nové skupiny, které se zaměřují pouze na tzv. zločin „kybernetický".

Kybernetičtí policisté. Ve Spojených státech, které jsou techniky nejvyspělejší nejen v komerční sféře, se nyní policii daří odhalovat zločinecké aktivity spojené s Internetem. Vládní specialisté rozeznávají několik forem nezákonného využití Internetu. Některé zločiny se odehrávají přímo na síti a objektem jsou většinou podniková data, přístupové kódy, čísla kreditních karet apod. Další využívají Internet pouze pro komunikaci a výměnu dat nebo jako kontaktní prostředek pro zákazníky zajímající se o zboží.

Podezřelé informace. Internet a *WWW* především je velice silné informační médium. Těžko nalezneme mocnější nástroj pro šíření informací různé úrovně a velmi širokého zaměření, který navíc uživateli umožňuje volný pohyb a čtení informací v reálném čase. Ne vždy jsou takové informace ku prospěchu společnosti a není problém najít velmi atraktivní údaje (obsahově i formálně správné a didakticky dobře podané) o výrobě domácích výbušnin, odposlouchávacích zařízeních apod. Jako příklad lze uvést anarchistickou kuchařku, která obsahuje informace o otevírání zámků, defraudaci kreditních karet, ničení aut atd. *WWW* stránky nebo textové soubory s tímto obsahem jsou dostupné komukoli, kdo má o ně zájem. Podobně je tomu u informací o výrobě a užívání nejrůznějších druhů narkotik, omamných látek, jako např. LSD, amfetaminu atd. Zpřístupnění informací o ne zcela legálních aktivitách je asi nejčastějším „prohřeškem" na Internetu a je také nejsnadněji

postižitelným. Jinak je také nejméně nebezpečným, protože je na každém, jak se získanými informacemi naloží. Kromě toho je poměrně velká část těchto dokumentů přínosem pro informovanost v oblasti drogové problematiky, účinků, praxi teroristických skupin apod.

Prostituce na Internetu. Na *WWW* stránkách lze nalézt publikaci *The World Sex Guide*, ve které jsou uvedeny informace o prostituci ve více než 55 zemích světa. Tyto informace zahrnují údaje o legálnosti prostituce v jednotlivých státech, o místech, kde lze prostitutky najít a také rady, jak se vyhnout trestním postihům v případě nelegálnosti této nejstarší lidské činnosti. Podle údajů amerických úřadů se na Internet přesunuly také gangy, které se prostitucí zabývají. Využívají nového média k výměně informací mezi svými členy, ale i pro nabízení sexu zákazníkům a sjednávání schůzek. Také prodej a výměna prostitutek probíhá již částečně elektronickou poštou a na *WWW* stránkách. Díky téměř nemožné identifikaci adresáta příjemce elektronických zpráv, a ještě těžší možnosti zjistit, kdo si *WWW* stránky čte, je těžké obvinit z kuplířství osoby, které takto prostitutky nabízejí.

Aktuální kauzy. Americká *FTC (Federal Trade Commission)* se v současné době zabývá obviněním několika společností, které na *WWW* stránkách a v diskusních skupinách nabízely zboží. To však nikdy svým zákazníkům nezaslaly. V Austinu byly odhaleny falešné společnosti *Berry Associates a Scott Berry*, které používaly úspěšně Internet pro prodej kradeného zboží. Zakladatelé těchto společností vytvořili všechno tak, že obě firmy se tvářily a chovaly jako bezúhonné obchodní firmy.

Šifrovací techniky PGP (Pretty Good Privacy) umožňující vysokou úroveň ochrany dat přenášených po Internetu pomocí elektronické pošty, si k nelibosti především amerických úřadů všimli nejen manažeři informačních systémů v různých společnostech. *PGP* neušlo také pozornosti osob, které si potřebují vyměňovat informace nezákonného charakteru po celém světě. Úřady americké vlády se domnívají, že tímto způsobem spolu komunikují také teroristické organizace, operující na americké půdě. Protože pro rozkódování zpráv zabalených pomocí *PGP* je zapotřebí výkonná technika a soudní povolení, je v současné době velmi obtížné jednotlivé případy operativně identifikovat a rychle tak potvrdit případná podezření. Navíc, i kdyby se zprávy podařilo rozšifrovat, opět se dostáváme k problému identifikace toho, kdo se skrývá za e-mailovou adresou.

Prodej kradeného zboží. Pro černý trh je Internet opravdu ideálním prostředkem pro prodej nejrůznějšího zboží. Zejména v různých diskusních skupinách, zaměřených na inzerci prodeje zboží, se objevují nabídky zboží, které bylo později odhalené jako kradené. Podle mínění mnoha odborníků však není tento jev příliš častý, i když úřady o tom již nejsou tak pevně přesvědčeny. Ty totiž nemají reálnou možnost zjištění pravé identity inzerujících, kteří nepřijdou s kupujícím vůbec do styku. Na rozdíl od klasických inzerátů je prodej po Internetu mnohem rychlejší a flexibilnější. Také případná dodatečná komunikace mezi prodávajícím a kupujícím je pro zloděje bez nebezpečí, protože ani v tomto případě nemůže být snadno vystopován. Aktivity tohoto typu spadají pod zneužití tzv. *elektronického obchodu.* Tento institut (též i u nás označovaný jako *e-bussines),* pokud je poctivě provozován, může pro

běžného člověka být přínosem. Představuje možnost zakoupení věcí ve virtuálním obchodním domě, kde je grafickou formou nabízeno různé zboží od špendlíků až po počítače. V zemi zrodu, v USA, je vše postaveno na používání platebních karet jako VISA nebo AMERICAN EXPRESS. Jde o dobrý projekt - ten je však realizovatelný tehdy, využívá-li se Internetu masově. U nás zatím nedošlo k tak širokému využívání Internetu, jako např. v USA. Přesto však i zde hrozí nebezpečí určitého zneužití. Mohou vzniknout poměrně snadno virtuální obchody, kdy nabízené zboží bude pouze na obrazovce ale nikoli ve skladu nebo u obchodního partnera. Na druhé straně jistě budou existovat osoby, které se pokusí vystupovat pod neexistujícím jménem anebo si objednají zboží s úmyslem nezaplatit. Jak v prvním, tak ve druhém případě se jedná o trestný čin podvodu podle § 250 trestního zákona.

Klasický podvod. Další skupinou podvodníků jsou fingovaní prodejci. Po zaslání peněz na zakoupení inzerovaného zboží nedostane neopatrný uživatel nic. Úřady radí používat pro koupi zboží na inzerát třetí strany, která u sebe podrží peníze do doby, než kupující dostane, co si objednal. V současné době je již stíháno několik osob i falešných společností, jejichž podvodům podlehlo nemalé množství osob.

Typické elektronické zločiny. Popsané zločinecké aktivity jsou pouze odrazem jejich obrazu v neelektronickém světě. Mnohem zajímavější a pro úřady komplikovanější jsou podvody a nelegální aktivity, které se odehrávají pouze v kybernetickém prostředí Internetu. Pro vystopování těchto zločinů je zapotřebí odborníků, kteří jsou technicky na stejné výši jako pachatelé. Právě v této oblasti se vytváří nejnovější sorta zločinců, která je označována výrazy, jako je *cracker, hacker* apod. Úřady zde musí čelit nejen problému dostatečné vzdělanosti pronásledovatelů, ale také rozdílnému společenskému nahlížení na pachatele elektronických zločinců. Zatímco v případě klasické krádeže je obecně pachatel považován za zloděje hodného zavržení, v případě krádeže dat nebo průniku do podnikového systému je hacker především technickým „géniem“, který dokázal přelstít složité zabezpečovací systémy.

Ukradená data. Mnoho společností, které se houfně na Internet připojují, si svá data nechrání dostatečným způsobem. A jak je vidět z několika případů průniku na vládní servery, dostatečnou ochranu nemají ani data amerických vládních agentur. Technický vývoj jde tak rychle, že je velmi těžké zaručit stoprocentní ochranu dat. Na rozdíl od správců podnikových i vládních informačních systémů, mají hackeři dostatek času i chuti na zkoumání možných slabých míst ochranných valů. A zájem o podniková a vládní data nemusí mít jen osoby „na okraji splečnosti“. Útočníky mohou být i konkurenční firmy nebo i teroristické organizace či výzvědné služby ne zcela přátelských států. Poslední věta zní sice trochu fantasticky, a1e podle některých údajů jde o skutečnost, i když zatím pouze sporadicky se vyskytující, protože starší výzvědné způsoby jsou efektivnější a pro mnoho výzvědných služeb zůstává existence Internetu na pokraji zájmu, blíže k tomu viz [206].

Intrnetová „kasařina“. Existence elektronické měny se pomalu stává skutečností. Může být užitečným přínosem pro rychlé nákupy a výměnu peněz, bez ohledu na místo sídla společností, stejně jako fyzických osob. Ale také může být cílem útoku podobně jako klasická

banka. I její předchůdci, kreditní karty, přinášejí nejen komfort, ale také nebezpečí. Největší podíl nevelkých plateb prováděných přes Internet spadá právě na kreditní karty, které jsou zejména v USA suverénně nejpoužívanějším prostředkem plateb za služby i zboží (nepočítáme samozřejmě platby v hotovosti). A zabezpečení přenášených informací o číslech kreditních karet není zdaleka na takové úrovni, na jaké by mělo být. Proto bychom se před tím, než číslo své kreditní karty svěříme Internetu, měli ujistit, zda je přenos alespoň kódován pomocí speciálního přístupu (protokolu *SSL*), i když ani to není dostatečnou zárukou bezpečnosti. Právě současná nebezpečnost přenosu údajů o kreditních kartách brání většímu rozvoji komerčních aplikací a elektronického obchodování na Internetu.

Odhalování nezákonných aktivit není jednoduché. Zčásti díky technické zaostalosti úřadů určených k potírání zločinu, zčásti díky legislativním problémům. Nekalé aktivity v USA lze pomocí Internetu provádět, aniž bychom kdy na půdu amerického kontinentu vstoupili. „Kyberpolicisté“ používají pro odhalování zločinu na Internetu informátory. Mnoho míst, kde se aktivity tohoto druhu odehrávají, vyžadují autorizaci pomocí uživatelského informačního dialogu a hesla, které je zapotřebí nejprve získat. Sledováním aktivit zločineckých kruhů na Internetu se zbývá především organizace *NCSA (National Computer Security Association)*. Podle údajů *NCSA* je tato organizace v současné době nějak zapojena do sledování činnosti více než 370 organizací, kde existuje podezření o nezákonných aktivitách. Právě *NCSA* potvrdila, že narazila v poslední době na několik případů, kdy si gangy pomocí Internetu domlouvaly narušení podnikových informačních systémů.

Virtuální kriminalita a virtuální zákony. Strážci pořádku se budou muset s postupujícím technickým vývojem průběžně školit, aby byli schopni chránit zákony svých zemí v kybernetickém prostředí. Podle údajů několika výzkumných společností se podíl obchodu prováděného na Internetu bude rapidně zvyšovat, stejně jako zřejmě dojde k vytvoření opravdové a možná i jednotné elektronické měny. Čím větší množství peněz po Internetu poteče, tím více bude toto prostředí jistými živly využíváno k nelegálním aktivitám. A to zdaleka nejen klasickými způsoby a formami. Lze se domnívat, že se velmi brzo setkáme se specifickými počítačovými zločinci, kteří budou současnými právními řády těžko postižitelní a ještě těžší je bude vystopovat. Aktivity „kyber-policistů“ se v současné době až na jisté výjimky rozvíjejí hlavně v USA. Vlády a policie ostatních zemí zatím existenci Internetu jako nástroje zločinu víceméně ignorují, nebo si tohoto faktu prostě nejsou vědomy. Počítačový průmysl není na počítačové zločince dostatečně připraven. Pokud používáme počítač častěji a pokud jsme navíc připojeni na Internet a sledujeme současné dění, nelze si nevšimnout jednoho velice důležitého faktu. Počítačový průmysl totiž pracuje naprosto odlišně od ostatních oborů. Zřetelné je to zejména v oblasti software. Vytvořené produkty, a to i komerční, nejsou nikdy zcela spolehlivé. Téměř vždy obsahují nějaké chyby a slabá místa. To se projevuje především v aplikacích určených pro Internet, protože zde je technický pokrok obzvláště rychlý. Z toho důvodu následuje zpravidla produkt za produktem, dokonalejší verze za verzí. Nekalých aktivit přibývá. Počítačoví zločinci se odborně technicky zdokonalují, zneužívají každou mezeru v zákonech - viz [205]. Je proto třeba k virtuální realitě přistupovat virtuálně i v oblasti legislativy.

**

Internet jako „černá díra“. Autor [197] říká, že Internet jako konglomerát mnoha objektů velmi nejasně definovaných -a když už, tak sice technicky či programově, ale rozhodně ne místně, časově nebo obsahově- je jakousi černou dírou. Možnost umístit server kdekoliv na světě, vytváření zrcadlových serverů na mnoha dalších místech, existence časových konsekvencí vzhledem k reálnému času i času aktualizací nám neposkytuje jistotu, že ve všech okamžicích jsou na všech místech sítě stejné informace. A co je ještě podstatnější, nikdo nám neposkytne jistotu, že jakákoliv informace nacházející se v kyberprostoru Internetu je správná! Odpovědnost provozovatelů jednotlivých částí Internetu je pouze morální a ani oni dnes již nemohou tušit, co se všechno nachází na jednotlivých *WWW* stránkách nebo v jiných souborech, kdo s nimi mohl a jak manipulovat atd. Např. aféry se změněnými *WWW* stránkami se nevyhnuly ani našemu Ministerstvu obrany. Tedy –podobně jako u jednoho ze dvou známých automatizovaných právních informačních systémů- ani u Internetu nemáme jistotu, že informace, kterou dostáváme je správná. Navíc zde existuje nezměřitelná míra nejistoty při opačném procesu, tedy poskytování informací do Internetu. Nenajde se mnoho lidí, kteří by vyzváni neviditelnou osobou z černého tunelu vložili do vysunuté ruky svoji kreditní kartu; přitom je s podivem, že řada lidí tak klidně učiní na Internetu. Stejně zcestné je podle názoru autora [197] předpoklad obchodníků, že vydělají mnoho peněz, nabídnou-li svým zákazníkům tento způsob obchodování. A pokud jde o bankovnictví -banka, která je připojena na Internet, je připojena na desítky miliónů potenciálních nebo i skutečných hackerů. Autor [197] celkem přesvědčivě dokládá, že Internet je výhodný jen pro někoho, že je to dobrá hračka, ale zlý sluha. Pokud budeme chápat Internet jako určitou, výrazně interaktivní počítačovou hru, nebudeme zklamáni. U Internetu si nelze činit nároky takové, jaké požadujeme u profesionálních systémů, tj. požadavek na úplnost, správnost, včasnost, odpovědnost, zabezpečení atd. Ani jedno z těchto kriterií zde nenajdeme! Jeho obrovskou výhodou je však charakter komunikace - rychlost, masovost, operativnost. Další výhodou, ale dnes již mnohdy také nevýhodou je obrovské množství informací, které se v něm nachází. Autor [197] ve světle jeho, do jisté míry skeptického pohledu na Internet, použil tohoto přirovnání: *„Internet je obrovská hromada hnoje, v níž se nachází několik pravých a větší množství falešných diamantů“.* Dále říká: *„Mohu zde nalézti poklad, ale také po několikatýdenním přehazování hnoje zjistím, že jediným výsledkem je silné znečištění“.* Nedostatek funkční i obsahové spolehlivosti je to, co v očích autora [197] Internet zcela diskvalifikuje jakožto profesionální prostředek. Stále čteme optimistické prognózy o tom, kolik peněz proteče Internetem. Dnešní realita je ovšem zcela jiná. Internet je byznys, který vydělává peníze jen někomu. Zejména prodejcům všeho, co s Internetem souvisí (hardware, software); poskytovatelům *WWW* stránek a jiných reklamních aktivit; zprostředkovatelům, kteří jiným vysvětlují, jak vydělávat na Internetu; novinářům a publicistům, kteří plní Internetem stránky novin a časopisů. I když příjmy z takové činnosti mohou být v současné době lukrativní, lze vyslovit pochybnost o jejich dlouhodobé trvanlivosti.

Bomba z Internetu. Dokladem toho, že na Internetu se nešíří jenom pozitivní a prospěšné informace, je zpráva [23]. Na Internetu se vyskytuje i neskutečné množství balastu

a zla. Podle této zprávy bylo možno z Internetu získat více jak dvěstěstránkovou metodickou příručku *„Jak lze snadno a rychle vyrobit v domácích podmínkách nástražný výbušný systém“*. Metodika volně dostupná na Internetu dávala podrobné návody k výrobě výbušných směsí, jejich účinného plnění a iniciaci. Nebylo a není v silách nikoho zabránit šíření něčeho podobného. Nálož vyrobená podle nějakého podobného návodu přístupného v síti Internet nečekaně explodovala a způsobila těžká zranění čtyřem švédským gymnazistům. Ve Švédsku jsou zřejmě mezi studenty bomby vyráběné podle návodů vyčtených z Internetu módou. Došlo i k dalším vážným případům. Policejní pyrotechnici navíc několikrát zasahovali na výzvu rodičů a odvrátili tak hrozící nebezpečí. Je ale opravdu „vinen“ jen Internet? Rozhodně ne. Jeden argument za všechny: Kolik lidí v minulosti přišlo o prsty anebo oči při Silvestrovských radovánkách? Určitě motiv a zdroj svého činění nenašli na Internetu! Internet je pouze prostředkem k poskytování informací. A s těmi lze pracovat tak či onak.

Internet zahltí sám sebe? Stále se zvyšující počet uživatelů Internetu naplňuje autora [197] stejným pesimismem, jako pohled na pražskou automobilovou dopravu. Co jsou platná lepší auta a přísnější policisté, když průtočnost silničních magistrál je stále stejná. Internet je závislý na komunikacích, které nejsou nikde dokonalé, a to ani v zemích, o nichž si to myslíme. Např. telekomunikační společnosti v USA si stěžují, že jejich sítě nejsou připraveny na desítky a stovky minut trvajících internetových transakcí. U nás jsme v obzvláště frapantní situaci, protože naše spoje nezvládají mnohdy své základní funkce, natož dlouhodobou zátěž Internetem. Už dnes vyloudit rozumnou odezvu, pokud nemáte k dispozici pevnou linku, je značně obtížné. Situaci ještě komplikují nerozumní tvůrci *WWW* stránek, neboť co stránka, to záplava grafiky. Většinou zcela samoúčelné, ale bezvadně násobící dobu přenosu, často 10-krát až 100-krát! Někdy to vypadá skoro tak, že jde o jakousi tajnou úmluvu s Telecomem, aby přenosy trvaly co nejdéle. Vzniká tak nebezpečí, že se Internet zahltí sám sebou, pokud nebude nalezen zcela nový, řádově mnohonásobně kvalitnější a kapacitnější způsob přenosu informací po zeměkouli. Zatím lze Internetu používat rozumně, pokud respektujeme či si uvědomujeme určitá omezení. Přirovnáme-li jej k velké veřejné knihovně, vypadá to, jako bychom svezli knihy z mnoha knihoven na jedno místo a vybavili čtenáře rychlým rejstříkem. Ovšem na některou knihovnu bychom zapomněli, z jiné by odešel knihovník a nikdo by už neaktualizoval evidenci, některé knihy by zlomyslný čtenář přepsal jiným textem a nikdy bychom si nebyli jisti, komu jsme zaplatili čtenářský poplatek a zda nám přitom ještě nevykradl zbytek peněženky. Přirovnáme-li jej k poště, zdají se být výhody lepší. Internetový e-mail je rychlý, relativně levný a můžeme posílat i zcela neuchopitelné objekty. Jen si nemůžeme být zcela jisti odesílatelem, tím, že náš dopis někdo nepozměnil nebo si od něj neudělal kopii. Proti některým útokům se lze v rozumné míře bránit např. šifrováním. Autor [197] se však velmi brání myšlence uskutečňovat na Internetu takové transakce, které svým jednáním zakládají jakýkoliv právní vztah. Tady roste míra rizika nade všechny meze.

4.4. Internet a problematika některých právních institutů

Systém Internetu je od samého počátku postaven na principu skutečné svobody projevu, svobodné výměny informací a nemá žádná omezení, pokud jde o obsah *WWW* stránek. Co se zde objevuje, nikdo nereguluje. Čas od času se v různých zemích ozývají tendence směřující proti takové volnosti, ale ty většinou narážejí na velký protitlak uživatelů Internetu a nevládních organizací, které střeží svobodu projevu. Ona bezbřehá volnost by mohla být bez obav přijímaná, kdyby se ve světě nevyskytovali jedinci se sklonem k nekalé činnosti. To však nenastává, proto na Internetu nacházíme spoustu dat i obrazových sekvencí, jimiž je Internet zneužíván k aktivitám, které jsou ve většině zemí trestné.

Pomineme-li extremismus a různé sexuální úchylky, zbude ještě velká oblast týkající se duševního vlastnictví-*autorského práva*. V řadě zemí slaví počítačoví piráti úplné lukulské hody a patří sem i Česká republika. Nezměrný hlad po nelegálním software pokrývá stejně obrovská nabídka přičinlivých osob které se rozhodly přilepšit si nelegální činností. Těmto aktivitám neunikl ani Internet, který jako svrchované území svobody projevu přímo láká, aby se zde nabízel nelegální software a aby ohledně něho zavládla pomocí elektronické pošty i čilá obchodní korespondence. Pokud tak šíří svá díla výrobci či autoři software, není jim co vytýkat - je to rychlé a hlavně to funguje. Ale softwarové pirátství je činnost jednoznačně protizákonná. Softwarový pirát si na svém serveru, minimálně na cizím či jinak neanonymním, vytvoří *webovou* stránku, jejímž jediným smyslem je inzerce nelegálně získaného software. K tomu připojí svou elektronickou adresu (tu už anonymní) a nelegální obchod se může rozjet. Vše zdarma nebo za minimální poplatek. Pár zájemců na takovou stránku upozorní další a objem obchodu se rozrůstá. Pochopitelně, že při našich rychlostech přenosu dat nelze tímto způsobem získávat příliš velké celky. A tak lze udělat krok zpět na vývojové linii a CD-disky se zašlou na dobírku. To už je ale obvyklý postup, který ovšem skýtá možnost snadného dopadení s následným obviněním pro porušování autorského práva podle §152 trest.zákona. Jak uvádí autor [38], jiný přístup k nelegálním počítačovým programům probojovávají na Internetu novodobí „Jánošíci“, kteří na svých stránkách nabízejí množství odkazů na webové stránky s nelegálním softwarem. Obvykle nezapomenou co nejokatěji zdůraznit, že tím nepáchají trestnou činnost, ale pouze pomáhají lidem najít, co potřebují. Lze to přirovnat k poklidnému člověku, který na prahu svého domku ochotně každému kolemjdoucímu ukáže cestu ke kradeným věcem tamhle naproti za rohem. U jiných trestných činů než porušování autorského práva by se to dalo kvalifikovat jako napomáhání k trestnému činu. Tito lidé zřejmě legislativu donutí, aby se do zákona takové ustanovení doplnilo, viz [38]. Řadu softwarových programů lze též nahrát rovnou na hard disk počítače. Někteří pachatelé takhle nabízejí programy na tzv. *FTP* serverech, umožňujících velice rychlé stahování dat po Internetu. K tomu se přidává hit poslední doby - šíření hudebních nahrávek ve formátu MPEG3 *.MP3. Tato komprimační metoda umožňuje stlačit nahrávky na objem přijatelný pro přenos dat po Internetu. V důsledku toho se začal čile rozvíjet i obchod s těmito produkty a vznikli audio-softwaroví piráti. Bezúhonný člověk by se neměl pouštět do zmíněných aktivit, byť by byl sebevětším fandou výpočetní techniky a měl k tomu patřičné vybavení. Kdo koupí a užívá software v reálné prodejní ceně řádově 10 tisíc korun za pouhou

stokorunu, nemá podle [38] právo o sobě tvrdit, že patří mezi řádné občany a dodržuje zákon. Jak po stránce morální, tak i právní nutno tyto aktivity zavrhnout. I podle hledisek *de lege lata* by měly naplňovat skutkovou podstatu trestných činů. Internet je nutno vidět jako ideální fórum komunikace, včetně přenosů dat, ale nikoliv jako volný bazar nelegálně presentovaných počítačových programů.

Svoboda projevu nezahrnuje právo libovolného subjektu k naprosto volnému přístupu k hromadným informačním prostředkům. Právě Internet umožňuje, na rozdíl např. od tisku, rozhlasu, televize, uskutečnění a šíření projevu libovolnému subjektu. Projevy, které se uskuteční pomocí Internetu, jsou svým způsobem uplatněním ústavního práva na svobodu projevu. Ta je chráněná i v mezinárodních dokumentech, zejména pak v *Mezinárodním paktu o občanských a politických právech* a v *Dohodě o ochraně lidských práv a základních svobod.* Ve vztahu ke svobodě projevu má největší význam čl.19 *Mezinárodního paktu o občanských a politických právech* a čl.10 *Evropské dohody o lidských právech*. Odtud možno odvodit mimo jiné myšlenku, že svoboda projevu je jedním ze základních principů demokratické společnosti. Vedle myšlenek a projevů přijímaných příznivě, myšlenek považovaných za neškodné či takových, ke kterým se veřejnost chová lhostejně, se však mohou vyskytovat i takové projevy, které urážejí, šokují, či znepokojují. Problém určitého adekvátního omezení svobody projevu, jakožto základního demokratického principu vzniká s výskytem právě těchto negativních projevů. Protože svoboda projevu není jediným ústavně a mezinárodně garantovaným právem, je třeba ji vidět v kontextu jiných práv. Právě v souvislosti s Internetem vzniká otázka přiměřeného omezení svobody projevu. I když vzhledem ke složitosti přenosu informací, často ze zemí, kde autorům nehrozí žádný postih, nebude snadné se zhostit tohoto úkolu tak, aby nedošlo naopak k nežádoucí společenské újmě. V souvislosti s tím byla otevřena i otázka *cenzury* [97] , jako jinak zavrženíhodného konstruktu, v mnoha právních systémech přímo zakázaného. Tudy však pravděpodobně cesta právních úprav, adekvátních i z hlediska dalšího možného vývoje předmětné problematiky, nepovede.

Právo na ochranu soukromí. Internet jako nedostatečně chráněná síť přináší se zabezpečením práva na ochranu soukromí značné problémy. Ochrana soukromí je obecně považována za velmi důležitý princip v každé demokratické společnosti. Kontrola jednotlivce ze strany státu, případně územní samosprávy, musí být podřízena adekvátní právní úpravě. Nezanedbatelnou úlohu při ochraně soukromí by mělo sehrávat chránění zájmů jednotlivce před vnějšími komerčními zájmy a zásahy do soukromí. Jestliže pomocí počítače lze objednat zboží, má příslušný dodavatel možnost „přečíst“ chování potenciálního zákazníka a tomu přizpůsobit reklamu a nabídku. Je jen otázkou posunutí často neostré hranice, kdy takové chování lze považovat za vážnou újmu chráněných entit klienta. Uvedený příklad je však pouze jednou z možností narušování soukromí z komerčních důvodů. Jsou známy případy prodeje dat z databází centrálních orgánů, obsahujících adresy, data narození a jiné údaje občanů, která byla zneužita k nabídce zboží soukromými firmami. První případy byly zaznamenány i při shromažďování internetových adres. Podle [58] např. firma *Four11 Corporation* soustředila asi 4,6 milionu adres pro podobné účely. Právo na soukromí během své více než stoleté historie prodělalo několik vývojových stadií. Jde o právní institut, který

nemá v našem právu dlouhou tradici. Ochrana soukromí, speciálně její obsahové chápání se neustále vyvíjí. V prvním období se týkala především vztahů mezi osobami, fyzickými i právnickými. V dalším pak se právo na soukromí stalo především prostředkem právní ochrany jednotlivce proti zásahům státu do jeho soukromého života. Nyní je velmi potřebná i ochrana soukromí před zásahem jiných osob, což platí zvláště pro Internet. Bohužel technický pokrok tak chvátá, že v počítačové síti bude těžké garantovat tak klasickou ochranu soukromí, jakou je *ochrana listovního tajemství*. Zatímco toto právo je garantováno právními systémy celkem běžně, dokonce s rozšířením i na tajemství jiných dopravovaných zpráv a písemností, v počítačové síti Internet garantováno není. V tomto případě bude muset zákonodárce pouvažovat asi nad výjimkou. Přepravované informace jsou totiž v procesu jejich putování zaznamenávány na mnoha místech. Jejich případné kódování, aby se zabezpečila nedotknutelnost listovního tajemství, by zřejmě ztížilo komunikaci mezi uživateli.

Internet a trestní právo. Nový pojem *kriminalita v počítačové síti* vzniká ve spojitosti s trestnými činy páchanými většinou prostřednictvím neoprávněného přístupu do sítě, případně zneužitím elektronické pošty, webovských stránek apod. Jsou známy případy nelegálně distribuované dětské pornografie, šíření nelegálních informací, poplašných zpráv ap. V Itálii byly např. zabaveny stovky počítačů pomocí nichž byla uveřejněna nelegální data v síti Internet. Jiný příklad pochází z USA, kdy osmnáctiletý student Illinoiské university poslal e-mailem dopis, v němž vyhrožoval smrtí prezidentu B.Clintonovi a jeho manželce. I když zfalšoval adresu odesílatele, byl orgány vyšetřování dopaden, viz [233]. Naše platná úprava trestního zákona nezná zvláštní skutkové podstaty trestných činů v rámci Internetu. Podle našeho názoru a podle dosud uskutečněných činů v síti Internetu, je možné uvažovat o aplikacích ustanovení použitelných minimálně k postihu *schvalování trestného činu, hanobení národa, rasy a přesvědčení, podněcování k národnostní a rasové nenávisti, šíření poplašné zprávy, pomluvy, vydírání, podvodu, podpory a propagace hnutí směřujících k potlačování práv a svobod občanů.* Při postihu trestných činů v Internetu lze vidět určitou váhavost orgánů činných v trestním řízení, a to nejen u nás, ale i v zahraničí. Technická specifika počítačových sítí obecně ztěžují postih pachatelů, ale je třeba říci, že i při páchání „klasické“ trestné činnosti nenechává zločinec po sobě vždy čitelnou vizitku. Podobně je tomu i v síti Internet, kdy původce nekalé činnosti se snaží zpravidla o maximální anonymitu. Navzdory tomu by projevy v Internetu, které naplňují skutkovou podstatu určitých trestných činů, neměly zůstat nepovšimnuty orgány činnými v trestním řízení.

Zodpovědnost za činnost prostřednictvím Internetu. Uživatele sítě Internet lze rozdělit do dvou velkých skupin:

1)Uživatelé, kteří chtějí Internet využívat zcela legálně, neskrývají svou adresu a tudíž totožnost. Mohou tím být samozřejmě vystaveni určitým útokům na soukromí, avšak z jejich strany zpravidla nehrozí odveta či jiné zneužití sítě.

2)Uživatelé, kteří chtějí Internet využívat zcela legálně, skrývají však totožnost pod adresami pseudonymů, většinou z podobných důvodů jako ti držitelé telefonních stanic, kteří nechtějí zveřejnit své číslo v telefonních seznamech. Tito uživatelé jsou většinou méně

zranitelní případnými útoky na své soukromí, jinak o nich platí totéž, co bylo řečeno o předchozí skupině.

3)Uživatelé využívající vstupu do Internetu pro páchání protiprávní činnosti. Ti se snaží často i technicky zabránit odhalení místa odvysílání nekalých informací. Bohužel jsou zpravidla na poměrně vysokém stupni počítačové odbornosti, čehož zneužívají i pro mnohdy riskantní průniky, neoprávněné přístupy s překonáním určitých ochranných bariér atp., a samozřejmě k zamaskování své činnosti, aby ztížili případné odhalení.

Neexistence konkrétního vlastníka počítačové sítě Internet si vynucuje hledat jiný model zodpovědnosti za uskutečněné projevy, než tomu bylo doposud u známých hromadných informačních prostředků, jako např. v televizi či v tisku. V počítačové síti Internet existuje v podstatě jen jedna možnost - zodpovědnost ponesou uživatelé Internetu. Z takového modelu vycházejí také první soudní rozhodnutí v této oblasti, viz [233]. Určitá obava z případné odpovědnosti vznikla u firem, které realizují připojení na síť. Tyto firmy však zabezpečují pouze technickou stránku věci a nemohou proto zodpovídat za obsahové, jimi neovlivnitelné aspekty.

Elektronický obchod (e-bussines) předpokládá elektronickou komunikaci. Nejen mezi občanem a firmou, ale i mezi různými společnostmi navzájem. Je jasné, že taková komunikace vyžaduje jistá pravidla. Například závaznost jednání pro daný subjekt. To znamená, že nebude nutné, aby kolem podpisu figurovali různí právní zástupci a notáři. Stejně tak se po převzetí a přečtení obchodního dokumentu musí daná strana chovat podle pravidel a nikoliv, jak je u nás doposud zvykem, tvářit se nezávazně, jako by o nic nešlo. Podle [35], ve věku informačních technologií a elektronického obchodu se bude muset brát vážně vše, co nebude jasně odmítnuto. Předpokládá to konec her na schovávanou, nástup zralosti a odpovědnosti. Kdo nehodlá respektovat pravidla a nadále se bude chovat jako podvodník, bude muset následky svého jednání nést, ať už finanční újmou nebo v podobě odnětí svobody. Elektronický obchod naši legislativu staví před určité problémy vyžadující poměrně rychlé řešení. Ovšem na druhé straně všichni zainteresovaní by měli přispívat k vytvoření takového prostředí, které zabrání podvodníkům v jejich aktivitách. Nutnost co nejdokonalejší ochrany majetku v těchto případech je velmi potřebná. Represivní aparát musí přitom hrát velmi důležitou roli, avšak nikoliv prvořadou, neboť odsouzení občana by mělo být chápáno jako svým způsobem výjimečné řešení se všemi důsledky a funkcemi trestu. Autor [35] uvádí, že je nutno vytvořit jedinou *certifikační autoritu,* která bude vydávat jakési *elektronické občanské průkazy*. V podstatě jde o to, že certifikací bude dáno, že osoba, ať fyzická nebo právnická, skutečně existuje. Tím se odstraní výchozí možnost podvodného jednání, protože bude velmi jednoduše ověřitelné, že účastník obchodu nebo jednání není pouze fiktivní osobou. Předpokladem pro to bude vytvoření a schválení zákonu o elektronickém obchodu, jenž dá jasná pravidla hry a vymezí pojmy. Za trestné musí být následně prohlášeno prozrazení tajemství informace dopravované po Internetu, stejně jako je tomu u listovních a podobných zásilek. Bez toho nebude mít nikdo jistotu, že jeho zpráva nebude zneužita, například konkurencí.

**

Některé další možnosti zneužití Internetu. Podle německých kriminologů a kriminalistů budou v průběhu několika let členové zločineckých organizací, teroristé a finanční podvodníci využívat k dojednávání svých nelegálních aktivit počítačů, namísto dosud nezbytných telefonických hovorů či osobních schůzek. Tyto obavy jsou zcela oprávněné. Vysoce výkonné kódovací systémy umožňují již dnes realizovat v celosvětové počítačové síti Internet utajenou komunikaci mimo dosah jakékoliv kontroly. S pomocí kódů lze bezpečně odesílat jak zcela neškodná sdělení (milostné dopisy), tak i například návody na zkonstruování bomby. V Německu jsou prostřednictvím Internetu distribuovány v periodikách extremistických organizací i technické postupy pro zakódování sdělení. Vedoucí představitelé *Spolkového úřadu pro ochranu ústavy* (*BfV*) a *Spolkové zpravodajské služby* (*BND*) požadovali v minulosti na spolkové vládě přijetí opatření proti neregulovanému používání kryptografických metod. Podobně jako v záležitosti tzv. *velkého odposlechu* kolidují i v této problematice základní lidská práva s bezpečnostními zájmy státu. Vnitropolitický mluvčí frakce poslanců stran Unie ve Spolkovém sněmu požaduje přijetí „kryptozákona", který má zamezit tomu, aby si zločinci vyměňovali zakódovaná sdělení. Proti tomu stojí však domněnka, že požadovaný zákaz lze jen obtížně prosadit. Skeptičtí vůči státním zásahům v oblasti kryptografie jsou především spolupracovníci spolkového pověřence pro ochranu dat, i když nevylučují možnost poskytnout bezpečnostním složkám velmi omezený přístup ke kódovacím metodám. Předpokládaným možným způsobem je dosažení stavu, kdy klíče k dešifrování kódovaných textů by musel autor kódu uložit u nezávislého notáře. Bezpečnostním složkám by notáři směli dešifrovací klíče vydat jen při předložení soudního příkazu k telekomunikační kontrole. Spolupracovnice pověřence pro ochranu dat však upozornila na nejnovější kódovací techniky z USA. S využitím tzv. *steganografie* lze ukrýt informaci bez problémů i v obrazech. Nezúčastněné osoby si vůbec nevšimnou, že se může jednat o zakódovanou zprávu. Vidí například jen Monu Lisu.

Návrh multimediálního zákona. Německá spolková vláda schválila v roce 1996 návrh zákona, který má znemožnit využití celosvětové počítačové sítě Internet k propagaci nacismu a šíření pornografie. Návrhem „multimediálního zákona" (*Das Gesetz zur Regelung der Rahmenbedingungen für Information - und Kommunikationsdienste*) usiluje Německo o kontrolu Internetu, aniž by přitom došlo k omezování osobní svobody uživatelů. Deklaruje tím zásadu, že prostor poskytnutý informačními technologiemi se nesmí stát zónou, ve které neplatí zákony. Nikdo se nesmí domnívat, že se díky špičkové technologii dostane mimo působnost zákona. Návrh zákona byl též projednáván na úrovni vlád jednotlivých spolkových zemí SRN.

Názory špičkových představitelů německé justice na stíhání trestné činnosti páchané v Internetu. Spolkový generální státní zástupce vyšetřuje rozšiřování zakázaného vydání levicově-extremistického ilegálního dokumentu *Radical* prostřednictvím Internetu. Odborníci považují státní opatření proti výzvám k násilí, pravicově-extrémním heslům a pornografii v Internetu za téměř beznadějná. Nejvyšší německý představitel státní obžaloby je přesto rozhodnut převzít „určitou průkopnickou roli" v boji proti internetové kriminalitě. Spolkový ministr vnitra vidí v Internetu hrozbu pro právní stát a požaduje jeho tvrdší kontrolu. Ministr

spravedlnosti naopak považuje snahy o státní zasahování za zcela beznadějné. Podle spolkového generálního státního zástupce mají pravdu v podstatě oba. Státní zástupci nemohou v Internetu vyhledávat dokumenty s kriminálním obsahem. Ale současně státní instituce nemohou nečinně přihlížet s konstatováním, že záležitost je příliš složitá. Generální spolkové státní zastupitelství nyní hledá nové cesty při stíhání internetové kriminality. Přitom je tento úřad kompetentní jen pro stíhání deliktů souvisejících s ochranou státu. I tak se dostává do role určitého průkopníka vůči zemským státním zastupitelstvím. V síti Internetu putuje verze zakázaného časopisu *Radikal*, který obsahuje návrhy na sabotáže v železniční dopravě. Jedná se tedy o případ zjevně související s ochranou státu. Zástupci generálního spolkového státního zastupitelství se proto obrátili na poskytovatele připojení k Internetu (providery) a sdělili jim, že se pod jistou adresou nachází závadný obsah. Provideři byli zároveň upozorněni, že se vystavují nebezpečí stíhání za napomáhání trestnému činu, pokud i nadále přístup k této adrese umožní. Podle spolkového generálního státního zástupce je však v současnosti Internet pro všechny zúčastněné - politiky, právníky a provozovatele - novým dosud neprobádaným územím. Otázkou je, jak lze realizovat trestní stíhání, aniž by došlo k ohrožení jeho legálního chodu. V uvedené záležitosti nyní probíhá vyšetřovací řízení, mj. pro podezření z propagace teroristických sdružení a z navádění k trestným činům proti providerům, kteří neuzavřeli přístup k závadným stránkám, a také proti osobám, které do Internetu uvedly *Radikal* a dále ho distribuují. Provideři však zastávají stanovisko, že by se vůči nim mělo postupovat stejně jako proti *Telecomu*, který není vyšetřován, když někdo jeho prostřednictvím telefonuje návod k sabotáži. Podle spolkového generálního státního zástupce je zde však podstatný rozdíl. V Internetu se nejedná o individuální kontakt mezi dvěma osobami, nýbrž o jakousi veřejně přístupnou vývěskovou tabuli. Proto má provider také větší zodpovědnost než *Telecom*. Provideři namítají, že je zcela nemožné, aby kontrolovali vše, co je distribuováno v jejich sítích, nebo aby dokonce zkoumali zákonnost obsahu distribuovaného dokumentu. Podle spolkového generálního státního zástupce musí být splněny dvě základní podmínky podmiňující odpovědnost providera. Provider musí vědět, že umožňuje přístup ke kriminálním informacím a musí být telefonicky schopen tomuto přístupu zabránit. Spolkový generální státní zástupce SRN je dále přesvědčen, že v souladu se všeobecnými ustanoveními trestního zákoníku platí trestnost činu i v té zemi, ve které se projeví jeho účinek. To znamená, že ten, kdo například v USA zavede do sítě dokument s kriminálním obsahem, spáchá trestný čin i v Německu, pokud zde existuje přístup k uvedenému dokumentu. Pokud obviněný cizinec v budoucnosti přicestuje do Německa, vystavuje se zde nebezpečí trestního stíhání. Podle spolkového generálního státního zástupce nesmí pro Internet platit specifická národní pravidla. Je nutno dosáhnout mezinárodní shody v postupu proti páchání trestné činnosti v Internetu. Pokud se například převezme právní standard USA, muselo by se shovívavěji postupovat při posuzování společenské nebezpečnosti pravicově-extremistické propagandy. Otázkou potom bude pouze to, zda tento standard německou společnost neohrozí. V tomto smyslu není nutné pro Internet vytvářet speciální trestní právo. Je však třeba, aby obvyklé delikty byly stíhány (podle zvoleného právního standardu), i když jsou spáchány zveřejněním v Internetu. Hospodářský význam této mezinárodní sítě bude stále stoupat. Provideři a uživatelé budou stále více zainteresováni na odstranění existujícího balastu ze sítě. Zatím lze sázet do jisté míry na pozitivní projevy

mechanismu trhu. Pokud by však trh totálně zklamal, bylo by potřebné přijmout zvláštní zákony, které by definovaly konkrétní zodpovědnost zúčastněných. Samotný příjem informací s kriminálním obsahem nelze považovat za trestný. V souladu se stoletými zkušenostmi z boje proti trestné činnosti vyplývá, že zločinci jsou vždy o krok napřed před policií. Nelze pochybovat, že mafie bude zcela určitě využívat i Internetu. Sporný je problém svobodného přístupu ke kódovacím programům. Například ve Francii je zakázáno používání nepovolených kódovacích programů. Nelze ovšem jednoznačně říci, zda je to správná cesta. Žádná informační společnost však nemůže připustit rozšíření kódovacích systémů v rozsahu, který by znemožnil odhalování a vyšetřování trestné činnosti. V tomto směru bude třeba schválit přijetí právní normy, která zaváže výrobce kódovacích programů k předání klíče k dispozici orgánům činným v trestním řízení. Je zcela zřejmé, že ten, kdo vědomě vloží informaci s kriminálním obsahem do Internetu, podléhá trestním zákonům. Obecně je třeba vycházet z toho, že Internet není zcela bezprávní prostor. Spolkový generální státní zástupce vyvrací pochybnosti o tom, že nelze stíhat rozšiřování jednotlivých vydání *Radikalu* v Internetu.

Zákonná úprava použití kódovacích technik. Spolková vláda SRN zavádí urychleně přísné zákonné normy pro používání tzv. kódovacích technik. Autoři zprávy, která byla zpracována na objednávku *Státního výboru pro tajné zpravodajské metody a bezpečnost*, varují především bezpečnostní instituce, že extremisté a členové skupin organizovaného zločinu mohou mezi sebou komunikovat prostřednictvím zakódovaných telefonických nebo počítačových vzkazů. S cílem umožnit policistům kontroly telekomunikací navrhují bezpečnostní experti všeobecnou schvalovací povinnost pro všechny kódovací metody. V budoucnosti bude možno používat pouze ty metody, jejichž dekódovací klíče budou v případě potřeby přístupné státním orgánům. Používání neschválených systémů, které jsou dnes volně distribuovány například v Internetu, bude považováno za spáchání trestného činu a má být důvodem k rozsáhlému vyšetřování. Počítačoví odborníci však pochybují o tom, že i ta nejpřísnější pravidla povedou k úspěchu. V Internetu je totiž údajně možno posílat zdánlivě nevinné zprávy, aniž by někdo postřehl, že se jedná o zakódované informace.

Některé zajímavé postoje k právním aspektům Internetu jsou uvedeny v článku [197]. Autor se na fenomén Internetu dívá poněkud skepticky. Píše, že Internet je jen fikce, že jako takový právně neexistuje. Technicky je to soustava serverů, komunikací a k nim připojených počítačů, organizačně jsou to provozovatelé jednotlivých podsítí, zprostředkovatelé připojení, uživatelé apod. Ovšem nenajdeme žádnou právnickou ani fyzickou osobu, která by byla naším partnerem za Internet jakožto takový. Z toho vyplývá jeho neuchopitelnost a obtížnost „vejít se“ do obvyklého právního řádu, především co se závazkových vztahů týká. Můžeme sice najít odpovědnosti například provozovatelů jednotlivých serverů, ovšem i zde je tato odpovědnost při počtu stránek řádově desetitisíců velmi relativní. Ani za vytvoření a bezchybný průběh spojení *de facto* ani *de jure* nikdo neodpovídá, protože například jednoznačně identifikovat příčinu chyb mezi telefonním systémem, připojovacím místem a sítí je skoro nemožné. Proto autor [197] tvrdí, že Internet je cosi, co nepochybně existuje, ale jehož chování, struktura, odpovědnosti a jiné aspekty, které požadujeme u jednoznačně

identifikovatelného objektu, nejsou definovatelné. Z toho vznikají další problémy teoretického i praktického charakteru.

4.5. Neoprávněný průnik a přístup

Pronikání do počítačových systémů je podle [110] relativně samostatnou oblastí v útocích proti programovému vybavení a datům uloženým v informačních systémech. Aktéry jsou tzv. *„hackeři"* - *průnikáři*, kteří se snaží obejít zabezpečení informačního systému a neoprávněně do něj vniknout. Počátečním motivem takového průniku může být pouhá recese a touha dokázat, že hacker je „lepší" než použitý bezpečnostní systém. Velmi problematický je však postih takového průnikáře. Pouhý fakt, že nepovolaná osoba vnikla do systému, by byl obtížně kvalifikovaný jako trestný čin, k případné trestní postižitelnosti je důležité prokázání nějakého dalšího úmyslu. Pokud se však nezjistí a neprokáže, že informace byla použita anebo se její použití chystalo, je trestně právní postih průnikáře omezený. Je obecně známo, že mnozí průnikáři provozují svou činnost jako „koníčka", že proniknutí do systému berou jako určitou intelektuální výzvu, to vše bez hmotných nebo jiných ambicí. Podstatně jiná je situace, kdy se průnikář při průniku do zajímavé databáze rozhodne, že získané informace nějak, nejspíše za určitou protihodnotu, použije. Velkou společenskou nebezpečnost skrývá v sobě získání neveřejných nebo tajných informací, navíc pak jejich konkrétní zneužití. Nebezpečnost takového jednání je podle [110] zřejmě úměrná úmyslu a kvalitě získané informace, např. informace charakteru státního tajemství. Prakticky každá instituce by velice neochotně zveřejnila skutečnost, že došlo k průniku do jejího databázového systému. To se ve většině případů úspěšně utajuje, např. z obavy o ztrátu prestiže, vzniku nedůvěry ap., což ve svých důsledcích může vést k hospodářským nebo jiným potížím. Postižená instituce se snaží zpravidla ve vší tichosti zdokonalit svůj systém ochrany proti průniku nepovolané osoby. Ze zahraniční literatury je znám případ, kdy v důsledku proniknutí do počítače neoprávněnou osobou byl nucen vlastník počítače vynaložit značné prostředky na prověření, zda se proniknutí do systému obešlo bez následků. Při této prověrce sice nebyly zjištěny žádné škodlivé následky, ale zato se podařilo zjistit pachatele a následně byly náklady na prověrku charakterizovány jako způsobená škoda a pachatel byl odsouzen.

Od „hackerů" se odlišují ještě tzv. „crackeři", kteří se zabývají narušením ochrany programů, např. proti neoprávněnému kopírování. V literatuře jsou často tyto dva termíny zaměňovány, i když každý z nich označuje aktéra sledujícího odlišné cíle. K tomu je třeba dodat, že osoba může být jak „hackerem", který se snaží vniknout do cizí databáze, tak i „crackerem", který vymyslí a realizuje odblokování určitého programového vybavení. Činnost obou typů je však nepřijatelná a mnohdy porušuje platná zákonná ustanovení.

Podle [110] *neoprávněný přístup k datům pro získávání utajovaných informací,* tzv. počítačová špionáž, může vyústit

-v *ohrožení utajované skutečnosti* podle §106 trest.zákona; orgány činné v trestním řízení při získávání podkladů podmiňujících zahájení vyšetřování musí respektovat okolnosti,

že většinou jde o data, která jsou předmětem utajení, a že pachatel jednal s úmyslem je vyzradit nepovolané osobě; vyzradit lze i informace v elektronické formě;

-v *porušování průmyslových práv* podle §151 trest.zákona; zde především jde o utajované technologie a technologické postupy, topografie polovodičového výrobku, ale eventuálně i o programy počítačů, veřejné zakázky apod.; ke zpřístupnění těchto informací může být použito výpočetní techniky;

-ve *zkreslování údajů hospodářské a obchodní evidence;* pachatel této trestné činnosti může činit nejen zásahy do programového vybavení, ale i přímo změnit podklady nebo vstupní údaje vkládané do počítače; vždy se jedná o poměrně velmi snadnou trestnou činnost, které se může dopustit nejen zaměstnavatel, ale i zaměstnanec;

-v *porušování předpisů o ochraně osobních údajů v informačních systémech.*

V §3 zákona č. 256/1992 Sb., viz [250], jsou vymezeny informace, které se vztahují k určité osobě, osobnímu údaji, jednoznačně identifikující osobu. K takovým informacím patří např. adresa osoby, pokud je v určitém seznamu. Není rozhodující, zda se jedná o počítačové informační systémy a počítačové databáze, nebo zda je informační systém zpracován i jiným způsobem např. formou kartotéky apod. V podmínkách hospodářské organizace podléhají režimu podle tohoto zákona osobní údaje zaměstnanců organizace a údaje o zákaznících - fyzických osobách. Tyto druhy informací jsou obvykle předmětem útoku pachatelů trestné činnosti. K tomuto okruhu informací je třeba přiřadit i informace, které mají speciální charakter a jejichž režim může, ale nemusí být upraven právním předpisem. Jako příklad může posloužit bankovní zákon, který upravuje režim bankovního tajemství. Zneužití takových dat z informačních systémů bez ohledu na to, zda se tak stalo za úplatu či nikoliv, je v rozporu s ustanovením zákona [250], o ochraně osobních dat v informačních systémech a taková jednání lze kvalifikovat jako trestný čin neoprávněného nakládání s osobními údaj i podle §178 trest.zákona .

Nebezpečnost neoprávněného přístupu ke zneužití počítačových prostředků, sítí, či samotných informací může být značná, zejména pak ve spojení s organizovaným zločinem. Např. této formy počítačové kriminality bylo použito v USA v roce 1998 k vydírání [62]. Do té doby neznámá zločinecká organizace nazývající se *HFG* pronikla na Internetu na webovou stránku listu *The New York Times* s výzvou na propuštění jistého uvězněného počítačového zločince. Redakce musela svou stránku zavřít v době, kdy na ní vzhledem k umístění zprávy nezávislého vyšetřovatele K. Starra o sexuálním poměru prezidenta B. Clintona se stážistkou M. Lewinskou panoval čilý ruch. Podle vyjádření redakce došlo během víkendu k omezení přístupu k informacím pro více než 100 000 uživatelů. Způsob neoprávněného průniku a zjišťování pachatele je vždy i pro špičkové pracovníky, jakými jsou např. specialisté *Federálního úřadu pro vyšetřování (FBI)*, tvrdým oříškem. Podle mluvčího *FBI* vyšetřování uvedeného případu pracovně vázalo po určitou dobu rozsáhlý tým specialistů. Tento útok na Internetovou stránku deníku byl exemplárním případem průniku hackerů na stránku světové sítě *WWW* velké tiskové organizace. Podle odborníků nezůstaly v minulosti ušetřeny před útoky ani internetové stránky tak mocných institucí, jako jsou některá ministerstva USA, Pentagon, či obří společnost Coca-cola.

5. Zneužívání strojového času, latence a modelování problémů počítačové kriminality

Sestaveno převážně z pramenů: [45], [87], [110], [137], [138], [222].

5.1. Některé formy zneužívání strojového času

Zneužívání strojového času patří k problémům, které jsou většinou řešitelné pouze zčásti v kompetenci jednotlivých institucí, kde tyto činy přicházejí v úvahu nejvíce.

V případech zneužívání strojového času „zevnitř“, tj. vlastními zaměstnanci, lze problém řešit pomocí organizačních opatření. Je třeba, aby příslušný provozovatel vydal závazná pravidla (řád, směrnice) pro práci s počítači s jasnou specifikací úloh, které lze pomocí výpočetní techniky zpracovávat. Směrnice by měly též výslovně upozornit na nepřípustnost užívání počítačů, tiskáren a dalších periferních zařízení k mimoslužebním aktivitám. Při provozování interních počítačových sítí je možné též organizovat dozor prostřednictvím správce sítě, tedy dohledem *supervizora*.

Při zneužívání strojového času „zvenčí“, např. při využití rychlých počítačů prostřednictvím globální počítačové sítě je obrana záležitostí ryze technickou, související s tzv. *počítačovou bezpečností*. Pojednáme proto o ní v souvislosti s tímto pojmem v dalším.

Je ovšem známou skutečností, že žádné z takových opatření nevymýtí zneužívání strojového času úplně. Jsou známy případy, kdy za úplatu odpovědných činitelů byly na služebních (sálových) počítačích zpracovávány úlohy cizích institucí, kterým spotřebovaný strojový čas ze strany zpracovatele nebyl fakturován. Náklady šly pak na vrub vlastníka výpočetního střediska. Finanční prostředky na úplatu vedoucích činitelů výpočetního střediska byly zadavatelem čerpány z „černých“ zdrojů, vytvořených nepřípustnými machinacemi. Zneužívání strojového času většího rozsahu bylo v minulosti četnější zejména při dávkovém způsobu zpracování, kdy výpočetní střediska vybavená velkými sálovými počítači pronajímala strojový čas cizím zadavatelům. Machinace se strojovým časem se pak nejčastěji projevovaly v nesrovnalostech ve fakturovaných částkách. Rozvoj stolové a později personální výpočetní techniky tyto nešvary částečně omezil. Přesto však je nutno brát v úvahu existenci počítačové kriminality tohoto typu a zejména dnes v době rozvoje nadnárodních sítí, počítat s její značnou latencí. Dnes velmi často dochází např. k prohledávání sítě Internet zaměstnanci podniku čistě ze soukromých pohnutek. Mimoslužební aktivity pracovníků jsou známy např. při výpisech určitých textových souborů pro soukromé účely, poslechu hudby na počítačích vybavených zvukovými kartami, při zneužívání elektronické pošty, při relaxačních hrách atp. S ohledem na současné pořizovací náklady a cenové relace za provoz sítí nejde o zanedbatelné ztráty, zejména při větším počtu zaměstnanců podniku.

Zneužívání výpočetní techniky pro osobní účely vůbec podle [110] spočívá nejčastěji v práci na počítači, kdy programu nebo komunikačního zařízení zaměstnavatele je bez jeho souhlasu používáno k privátním účelům. Tato trestná činnost spočívá obvykle ve využívání počítače zaměstnavatele, včetně jeho programů, respektive v prodávání programů, které byly vytvořeny v rámci pracovního poměru jiným uživatelům bez vědomí zaměstnavatele. Lze tak rozlišit zneužívání strojového času formou

-*bezprostředních krádeží*, kdy pachatel zneužívá čas přímým blokováním určité kapacity počítače při zpracovávání soukromé úlohy, či při mimopracovním prohledávání sítě apod.;

-*zprostředkovanými krádežemi* spočívajícími v nepřímém zneužívání strojového času při řešení služebních záležitostí tím, že legálně pořízené výsledky (programy) jsou poskytnuty často za úplatu dalším zájemcům mimo služební poměr; hodnota bezprostředně spotřebovaného strojového času, např. na pořízení kopií výsledků (programů), je v tomto případě zpravidla zanedbatelná vůči celkově nelegálně získanému efektu;

-*soukromého (zájmového) užívání* pro zdokonalování operátora v počítačové obsluze mimo jeho pracovní náplň.

Při těchto aktivitách se velmi často využívají počítače i nevýdělečně v pracovní době, a to na úkor pracovních povinností nebo při plném zvládnutí všech požadavků zaměstnavatele. Počítače se však mohou využívat též i v době mimopracovní, a to nevýdělečně i výdělečně. Z hlediska postihu je nezbytné rozlišovat, zda jde o porušování pracovních povinností nebo o porušování vlastnických práv či dokonce o trestnou činnost, např. při výdělečném využívání počítače přímo na pracovišti. Je dobré si uvědomit, že nevýdělečné neoprávněné užívání počítače může dokonce přispět i ke zvyšování kvalifikace zaměstnance. Pachatelé deliktů podobného typu jsou obvykle specialisty na zpracování dat, systémoví programátoři apod. V každém případě je třeba zdůraznit, že nedovolené dispozice s cizí věcí jsou nežádoucí. Používání cizí výpočetní techniky k jiným než zadaným úkolům je nežádoucí bez ohledu na to, zda je realizováno nevýdělečně, mimo pracovní dobu, nebo na úkor plnění pracovních povinností. Takto formulovaný problém svádí v daném případě k aplikaci §249 trest. zák. - *neoprávněné užívání cizí věci*. Určitou nejasnost zde ale vyvolává konkretizování pojmu „neoprávněného užívání cizí věci“ ve vztahu k počítači.

Jak dále uvádí [110], zákonodárce tu předpokládá zmocnění se věci nikoliv malé hodnoty pachatelem, s úmyslem tuto věc přechodně užívat i když je zřejmé, že původní konstrukce zákona mířila jinam, a to do oblasti jednání, v jehož důsledku je majitel věci, byť krátkodobě, omezen v právu s věcí disponovat. Zaměstnavatel by měl dát písemný pokyn v jakém rozsahu je uživatel oprávněn nakládat se svěřeným počítačem. Jedině touto cestou je pak možné posoudit prostor oprávněnosti či neoprávněnosti určité manipulace s počítačem. Dalším faktorem je také samozřejmě intenzita užívání (zásahu), možnost vyčíslení vzniklé škody, např. s ohledem na amortizaci v době užívání ap. Teprve z toho lze dovodit případnou společenskou nebezpečnost příslušného činu. V jednotlivých případech je také nutné rozlišovat mezi porušováním pracovních povinností, porušováním vlastnických práv a spácháním trestného činu. Zde po stránce prevence má značné možnosti majitel zařízení -

zaměstnavatel, který může vhodnými opatřeními legalizovat a současně vhodně regulovat soukromé iniciativy zaměstnanců. Např. tím, že vyčlení jeden počítač mimo běžný provoz pouze k těmto účelům. Pokud však nedovolené manipulace dosáhnou intenzity trestného činu, měl by státní orgán zasáhnout bez ohledu na vlastníka, pokud ovšem vlastník tuto činnost dodatečně nezlegalizuje. Nekalá činnost tohoto typu je okolím posuzována zpravidla velmi shovívavě, i když hodně záleží na konkrétní situaci a celkovém klimatu firmy. Mezi podobnými uživateli by se mělo rozlišovat, zda jde o nevýdělečné užívání počítačové techniky, nebo výdělečné užívání. Při výdělečném užívání by měl být takový uživatel vždy stíhán. Oproti tomu nevýdělečné užívání, které uživatel provádí po zvládnutí všech svých pracovních povinností a které není přímým zdrojem škod, je ve své podstatě přínosem pro zaměstnavatele, neboť takový uživatel si zvyšuje svou kvalifikaci a dovednost při obsluze počítačové techniky.

**

K problematice jak zabránit zaměstnancům, aby ztráceli čas na Internetu se vyjádřil nejbohatší muž planety a šéf firmy Microsoft Bill Gates [87]. Řekl, že tato skutečnost je velice aktuální i v mnohých našich podnicích, institucích či firmách. Firmy mají vždy problémy s tím, co vymyslet, aby lidé jen tak nelelkovali - třeba si neprohlíželi časopisy, netelefonovali známým nebo neklábosili u automatu s nápoji. Internet představuje v tomto ohledu dost velký problém, protože přímo láká lidi, aby strávili zajímavým způsobem hodinku nebo třeba celé odpoledne. V jeho firmě je považováno za normální, stráví-li pracovník putováním po Internetu půl hodiny denně. Souvisí-li to ovšem s jeho pracovní náplní. Chceme, aby lidé Internet používali. Avšak když někdo věnuje prohlížení internetových stránek osm hodin denně, není to už práce ve prospěch firmy. Po technické stránce není problém nejen sledovat, kdo a jak dlouho Internet používá, ale i zavést různá omezení. Softwarové prostředky k tomu určené jsou dnes k dispozici 24 hodin denně. Informace, které proudí do mezinárodní sítě (WWW), procházejí obyčejně přes zařízení nazývané *selektivní skříňka*. Ta je zajištěna proti nežádoucím vstupům, může uživatelům dodávat přehled nejpoužívanějších stránek a umožňuje managementu omezit jak přístup k Internetu, tak rozsah jeho použití. Vedení firmy může, bude-li chtít, mít přehled o jakémkoli užívání Internetu zaměstnanci. Ale toto extrémní řešení už hraničí s vměšováním se do osobních záležitostí. A pokud chceme využívat předností Internetu, nemá asi smysl nasazovat technického „policejního psa“, aby ani na vteřinu nespustil zaměstnance z očí. Má-li člověk používat zařízení, které patří firmě, musí existovat jednoznačná dohoda o tom, jak dlouho denně se může věnovat všeobecné informaci - bud' nula minut, nebo třeba deset. Vedení musí samo vědět, zda je lepší absolutní zákaz, nebo mírná tolerance. Samozřejmě, že v různých firmách se řešení bude lišit podle jejich zaměření. Jiná dohoda je možná v soukromých společnostech, jiná ve veřejných institucích.

5.2. Možnosti odhadů latence trestných činů zneužívání strojového času a dalších počítačových deliktů

Latence zneužívání strojového času, jakož i jiných typů počítačové kriminality je závažným fenoménem, podmíněným řadou specifických faktorů. Nejzávažnějším faktorem latence počítačové kriminality vůbec je technická náročnost zjišťování nějaké neoprávněné počítačové aktivity. Jako např. neoprávněného vstupu či zásahu do systému, zneužití strojového času, dat, programu či jiných konstruktů. Tyto aktivity jsou zjišťovány většinou jen náhodně, při chybě pachatele nebo v případech, kdy je útok předpokládán.

Odhalování rozsahu skryté kriminality je obecně považováno za svízelný metodologický problém; přitom jeho přiměřené řešení má velký a nejen kriminografický význam. Řada autorů se pokoušela o pochycení tohoto problému empirickými přístupy. V tomto směru hrají významnou roli např. výzkumy o obětech trestných činů. I když mnohé z nich si nekladou za cíl uspokojivě řešit otázky latence kriminality, dávají podklady alespoň k hrubé orientaci v dané problematice u vybraných trestných činů. Zajímavým přínosem v tomto směru je výzkum, realizovaný Institutem pro kriminologii a sociální prevenci v roce 1992, kdy bývalá ČSFR byla vyzvána k účasti na mezinárodním výzkumu kriminality, který proběhl pod patronací OSN. Výsledky výzkumu jsou obsaženy v publikaci [45]. Jsou podány v širším mezinárodním kontextu informací o kriminální viktimizaci v industrializovaném světě. Bohužel problémy latence počítačové kriminality však neřeší. Jiný možný způsob řešení otázek rozsahu skryté kriminality přinášejí aplikace určitých analytických modelů. Jde o aproximace reality vhodným matematicko-statistickým aparátem, pomocí něhož možno obdržet konkrétní výsledky [137].

Z pohledu statistiky můžeme na ukazatel skutečné kriminality nahlížet jako na realizaci náhodné veličiny, podmíněné množstvím kriminogenních, těžko postižitelných různorodých účinků. O této veličině víme prakticky s jistotou, že neleží pod hodnotou registrované kriminality. Kdybychom byli schopni popsat zákon jejího rozdělení nad příslušným určujícím intervalem, byl by problém vyřešen. Na základě toho bychom totiž mohli odvodit a sevřít charakteristiky latence do odpovídajících intervalů spolehlivosti. Určujícím intervalem rozumíme interval, v němž se vyskytují hodnoty dané veličiny prakticky s jistotou. Vně určujícího intervalu leží tedy hodnoty jen se zanedbatelnou pravděpodobností. Je zřejmé, že různé typy deliktů budou mít obecně i různá rozdělení této veličiny nad příslušnými určujícími intervaly. Rozsah skutečné kriminality lze přirovnat k ledovci, kdy jeho určitá část je viditelná a zbytek je skryt pod hladinou. Fundovaně statisticky položený problém nespočívá v „hádání“ konkrétní bodové úrovně skutečné kriminality - alespoň přibližné představy o takové úrovni má každý erudovaný kriminolog - ale především ve stanovení míry pravděpodobnosti toho kterého odhadu. Jedním z pozoruhodných výsledků kriminologické statistiky je zdůvodnění předpokladu založeného na tom, že nikoliv ukazatel skutečné kriminality sám, nýbrž jeho (přirozený) logaritmus má normální rozdělení. Vychází

se přitom z toho, že ukazatel intezivního typu celkové skutečné kriminality lze chápat jako pravděpodobnost velkého množství vybraných současně nastupujících nezávislých kriminogenních jevů. Logaritmus této pravděpodobnosti lze pak rozložit na součet určitých nezávislých náhodných veličin, totiž logaritmů pravděpodobností uvažovaných kriminogenních jevů. Blíže k tomu viz práci [138]. Na základě teorie pravděpodobnosti můžeme pak za velmi obecných podmínek dokázat přijatelnost příslušného zákona rozdělení, který nazýváme *normálním modelem latence kriminality*.

5.3. Modelování skutečné a latentní počítačové kriminality

Normální model latence kriminality říká, že daný ukazatel skutečné kriminality má logaritmicko-normální rozdělení (stručně též LN-rozdělení). Na základě dlouholetých zkušeností víme, že je přijatelný u populačních celků velkého rozsahu a globálních typů kriminality měřených absolutním ukazatelem. Pokud bychom studovali subtilnější útvary, kterým bezesporu počítačová kriminalita je, musíme očekávat menší či větší odchylky od normálního modelu latence. Tyto odchylky jsou v podstatě dány oslabením předpokladu nezávislosti zúčastněných kriminogenních jevů. Lze je měřit speciálním parametrem, tzv. činitelem deformace. Ten podle terénních šetření formou expertních odhadů činí v průměru 3,3 z celkového možného rozsahu mezi hodnotami 0 až 6, viz [137]. Čím je činitel deformace menší, tím větší je latence jevu a obráceně. Předpokládáme, že u počítačové kriminality, speciálně pak u deliktů zneužívání strojového času se bude pohybovat v intervalu od 1,3 do 3,3. Jeho upřesnění by bylo možné realizovat rovněž metodou odborných expertíz např. ve spolupráci s policejními specialisty na počítačovou kriminalitu. Pomocí zjištěných objemů registrované kriminality a příslušného činitele deformace lze pak určit objem skutečné a následně i latentní kriminality postupem popsaným ve studii [137]. Podle teorie normálního modelu latence kriminality je nutno každý odhad skutečné kriminality interpretovat jako mez, kterou může odhadovaná neznámá faktická hodnota překročit s určitou pravděpodobností, více či méně vzdálenou jistotě. Takto vypočtené hodnoty nelze proto obecně aplikovat aditivním způsobem na součty hodnot ukazatelů dílčích kategorií deliktů.

Popsaný model je však přesto velmi flexibilní:

-jde o pojetí originální, spočívající v tom, že původní, obtížně stanovitelný parametr deformace se určí postupnou aproximací maximálního rozsahu možných pachatelů, poslední použité pořadí kroku aproximace je pak odhadem parametru deformace;

-maximální rozsah možných pachatelů lze stanovit nejméně dvěma různými, na sobě nezávislými metodami; k jeho určení lze využít např. též postupu v kombinaci s terénním šetřením;

-model lze přizpůsobit pro analýzu většího počtu kategorií deliktů než udávají tabulky [137], např. bezprostředně může být rozšířen na extrémně latentní jevy, což u počítačových deliktů může být vítáno; na činitel deformace lze totiž nahlížet jako na spojitý parametr;

-postup odhadu skutečné a latentní kriminality vůbec, speciálně pak kriminality počítačové, je podle zmíněného modelu natolik universální, že může být využit i na jinak

konstruované určující intervaly nebo jinak stanovené odhady středních hodnot a směrodatných odchylek než předepisuje studie [137].

Pokud zde hovoříme o modelování, je užitečné připomenout, že jde o výzkumnou metodu, jejíž podstata je dána tím, že zkoumanou realitu nahradíme určitým modelem a tento model studujeme s cílem získat informace o analyzovaném reálném objektu. V případech, kdy model je realizován jako exaktní, od povahy věcných aspektů abstrahující, matematicky přesně definovaný objekt, mluvíme o *matematickém modelování*. Lze říci bez nadsázky, že matematické modelování má v české kriminologii již určitou tradici. Jejím konkrétním výrazem je mimo jiné též konstituování *kriminologické statistiky* jako mezní oblasti, která zahrnuje i problematiku adekvátního hodnocení výsledků matematického modelování. Důležitým rysem studia modelu je možnost konat s tímto modelem určité *experimenty, pokusy*. Ty mohou být nejrůznějšího druhu. V minulosti byl u nás např. v resortu bývalé prokuratury realizován rozsáhlý výzkum metodiky prognóz kriminality s cílem co nejlepší anticipace dynamiky určitých kategorií trestné činnosti [138]. Příslušné experimenty modelového pojetí se týkaly výběru a aplikací nejpříhodnějších přístupů k vyjádření trendů, tj. základních směrů a úrovně dosavadního vývoje příslušných trestných činů. Pokud tyto trendy vyjádříme formou statistických závislostí na aktuálních určujících faktorech vývoje, může být zmíněná anticipace pojata alternativně podle zvolených faktorů. Experimentování by pak mělo vyústit v optimalizaci volby faktorů pro odhad zobrazení studovaného vývoje. V tomto smyslu je definice modelování blízká běžnému Dahlovu pojetí *simulace*, v níž se však místo o analyzovaném objektu mluví o dynamickém systému a podle toho je chápán i termín model, srov. též [222].

Pod pojem experimentu však můžeme zahrnout i zdánlivě složitější situace v hodnocení vztahů „realita-model“. Sem patří i náš případ statistického rozboru skryté počítačové kriminality na základě deformací normálního modelu latence kriminality, kdy vhodnou volbou činitele deformace můžeme daný model co nejvíce přizpůsobit specifiku dané kategorie trestné činnosti. Podrobnější zhodnocení zmíněného postupu může však vyplynout jedině z adekvátního terénního šetření v dalších etapách výzkumu počítačové kriminality. Při práci s modely měli bychom si být vědomi určitých úskalí, jež mohou vyústit v chybnou interpretaci výsledků. Někdy dochází k nežádoucímu ztotožňování zvoleného modelu s jeho vzorem. Pak může dojít k dalším nesprávným implikacím a interpretačním závěrům, zejména při méně přehledných způsobech modelování. Jako příklad lze uvést evidentně nesprávné směšování trendu skutečné počítačové kriminality s trendem registrované kriminality, případně navíc s *odhadem trendu* registrované kriminality. Samozřejmě, že tyto veličiny v důsledku latence či volby modelu nejsou obecně totožné. Pojmy jim odpovídající nelze proto libovolně zaměňovat.

V zásadě je nesprávné také zaměňování vlastností *výběrového souboru* s vlastnostmi souboru základního při modelování počítačové kriminality pomocí výběrových přístupů. Výběrový soubor nemůže být obecně nikdy zcela přesnou kopií souboru základního. Formulace podobného typu, které to popírají, ignorují principy teorie výběru a metodiku

generalizace výběrových výsledků a z ní vyplývající závislosti chyb generalizace na způsobu konstrukce a velikosti výběrového souboru.

Pokud jde o *modelování latence zneužívání strojového času*, případně i dalších typů počítačové kriminality, mohou se vyskytnout určité pochybnosti i odmítavé postoje v tom smyslu, že obecný základní normální model latence kriminality nemůže vystihnout specifika skryté kriminality jednotlivých forem těchto deliktů. Je evidentní, že zde jde o jisté nedorozumění, respektive nepochopení podstaty odhadů neznámých veličin statistickými metodami. Použitím uvedeného modelu můžeme získat nanejvýše bodové či intervalové odhady, tedy meze spolehlivosti výskytu hledaných veličin, případně globální charakteristiky těchto mezí (např. jejich střední hodnoty) a nikoliv přímo veličiny samé. Již bylo řečeno, že takto získané modelové veličiny nelze ztotožňovat s jejich momentálně neznámými skutečnými předlohami. Kde přesně neznámá hledaná hodnota v daném rozpětí ve skutečnosti leží, nelze z povahy modelu nikdy blíže specifikovat. Naopak, je třeba zdůraznit, že případ od případu mohou zmíněné meze spolehlivosti vyhovovat méně, např. mohou být příliš široké, jindy opět úzké, ale hovořit o nich jako o nesprávných by nebylo adekvátní. Jejich bližší specifikace, upřesnění je otázkou dalšího přizpůsobení původního modelu, tj. jeho vhodného deformování, dejme tomu odpovídajícím experimentováním směrem k odhadům činitele deformace pro ten který trestný čin. To je snad natolik pochopitelné, že není třeba hlouběji uvedené námitky rozebírat. Problémem ovšem nadále zůstává konkretizace příslušných experimentů. K těmto otázkám je třeba orientovat případné další výzkumy.

Oproti předchozím výhradám lze přijmout celkem ochotně námitku, že modelování jako takové s jeho pojmovým aparátem a aplikacemi není v některých případech nezbytným východiskovým principem. Sama problematika odhadů latence kriminality byla zpočátku rozpracována na základě *teorie her*, jakožto střetu dvou strategií - strategie reality jako hráče skrývajícího skutečný stav a strategie výzkumného pracovníka, estimátora, odhadce, který se snaží skutečný stav naopak odkrýt. Teprve konfrontace takto získaných konkrétních výsledků s důsledky modelového pojetí ukázala neopodstatněnost původní, ojediněle se vyskytující a jinak nezdůvodněné kritiky, že použití teorie her v praxi na tyto otázky je jen pouhou utopií, srov. [138].

Jedním z určujících problémů modelování či simulace jevů počítačové kriminality je stanovení účinnosti modelu. Dostatečná účinnost modelu je zárukou stability a tudíž i spolehlivosti modelu. Otázky měření účinnosti modelu je proto užitečné předřadit vlastnímu zpracování výsledků. *Účinnost modelu* bývá tradičně posuzována jednak podle meritorních hledisek spočívajících v posouzení shody modelové situace s realitou, jednak podle rozsahu pokrytí určujících případů. Je-li shoda modelu s realitou velmi dobrá a model pokrývá většinu studovaných jevů, je i účinnost modelu vysoká. Účinnost modelu se měří zpravidla nějakým poměrem, který nabývá hodnot od 0 do 1. Pokud nabývá hodnoty 1, hovoříme též o úplné (totální) účinnosti modelu. Trochu složitější je posouzení účinnosti normálního modelu latence. Účinnost podle meritorních hledisek je zabezpečena principy výběru a odůvodněním konstrukce normálního modelu latence, včetně způsobů odhadů jeho parametrů, tak jak bylo nastíněno v předchozím. Ve většině případů, které se však bohužel zatím netýkaly počítačové kriminality, byla účinnost popsaných modelů blízká totální účinnosti.

Nyní učiníme několik poznámek ke zkušenostem z dřívějších výzkumů analytických modelů latence kriminality. Přihlédneme též k výhledovým možnostem dalších aplikací metody expertíz odhadů činitele deformace.

1)Relativně velké počty konkrétních odhadů, které se v minulosti uskutečnily na základě daných instrumentů, opodstatňují kladné hodnocení přístupů založených na principech studia hromadných jevů.

2)Výzkumy zpočátku realizované v resortu bývalé prokuratury byly na rozdíl od nynějšího aktuálního přístupu zaměřeny na hrubé (většinou bodové) odhady

-konkrétních hodnot charakteristik skutečné či latentní kriminality,

-činitelů deformace normálního modelu latence podle určité transformace parametrů LN-rozdělení.

3)Nevýhody tohoto dřívějšího pojetí tkví zejména v tom, že

-získané odhady téměř ve všech případech se vzájemně dosti rozcházely, a to i v případech optimistických či pesimistických alternativ extrahovaných běžnými statistickými postupy,

-odhady činitelů deformace v klasickém pojetí byly pro celkově menší průhlednost obtížněji dosažitelné a tím ze strany expertů, tehdy převážně prokurátorů, i méně přesně pojímané.

4)Výhody analytického přístupu podle studie [137] spočívají

-v jednodušším pojetí činitele deformace normálního modelu jako charakteristiky maximálního možného objemu daného ukazatele, která je založena vlastně na předefinování určujícího intervalu,

-v pořizování nikoliv přímých odhadů objemů skutečné kriminality či latence, nýbrž v odhadech relativních relací mezi delikty na základě poměrné stupnice,

-v územní universálnosti v důsledku volby vhodného ukazatele a profesního záběru expertů,

-ve snadné dostupnosti konkrétních výsledků i pro blíže nezasvěcené pracovníky na základě tabulek [137].

5)Aktuální odhady policejních expertů ve srovnání s dřívějšími odhady se zdají být z hlediska latence kriminality poněkud optimistické, podhodnocené. Vzniká proto otázka pořízení případných alternativních, méně optimistických odhadů.

6)Podle metodiky strukturální simulace [222], založené na komparaci a redukci výchozích dat vůči určitým kritickým hodnotám, vyšel pro globální činitel deformace pesimistický odhad asi 1,7krát menší, tedy přibližně v hodnotě 1,9. V tomto poměru je pak nutno počítat též s redukcí činitele deformace pro počítačovou kriminalitu.

7)Tento odhad byl konkrétně stanoven jako střední hodnota podprůměrných odhadů činitele deformace normálního modelu latence. Jeho metodické opodstatnění spočívá

v přijatelném předpokladu symetrické normality rozdělení (rozložení) odhadů expertů na stupnici poměrného zastoupení činitele deformace, zatímco přímé odhady objemu skutečné kriminality či latence by měly počítat s LN-rozdělením, které je asymetrické. Z hlediska psychologie respondenta je proto posuzování relativních relací činitele deformace akceptováno lépe. V tom zřejmě spočívá též i podstatně větší spolehlivost získaných výsledků.

8)Pokud by se v budoucnu prokázala universálnost takových odhadů, bylo by potřeba v daném poměru, dnes odhadovaném asi 2/3, přepočítat stávající hodnoty. Tento postup je ekvivalentní zúžení původního rozpětí činitele deformace <0;6> na rozpětí <0;4>, pokrývající analogicky pojímané kategorie deliktů. Celkově by pak šlo o zmenšení rozlišovací schopnosti modelu.

9)Zatím není známo, zda tímto způsobem pořízené pesimistické odhady by praktickým poznatkům o latenci počítačové kriminality vyhovovaly lépe. K jejich verifikaci by bylo třeba opakovaných výzkumů na ještě širších souborech expertů. V případě pozitivních výsledků nebude aktualizace vhodných pomůcek, ať programů, či tabulek, činit jistě žádných principiálních potíží.

10)Předchozí problém nás přivádí k dosud nedořešeným otázkám vztahu optimistických, pesimistických a optimálních odhadů skutečné a latentní počítačové kriminality pomocí nastíněných přístupů. Strukturální konfigurace získaných dat implikuje též otázky spjaté s možnostmi případného pořízení alternativ odhadů činitele deformace podle časové a územní struktury kriminality. Inspirující se zdá být myšlenka výzkumu zejména v územních celcích s možným extrémním stavem a vývojem kriminality. Tato specifika nebyla dosud ve světle matematického modelování blíže studována.

V případech zneužívání strojového času, či jiných počítačových deliktů jde většinou o relativně malé objemy registrované kriminality ve srovnání s předpokládaným skrytým rozsahem. Hromadnou stránku těchto specifických deliktů nelze samozřejmě v celostátním rozsahu popřít, avšak jak adekvátně uchopit příslušná specifika z pozic kriminologické statistiky bude zřejmě ještě dlouho předmětem odborné diskuse.

6. Počítačová bezpečnost

Sestaveno převážně z pramenů: [12], [28], [46], [47], [63], [64], [65], [72] [73], [74], [75], [98], [102], [119], [121], [122], [123], [138], [153], [154], [157], [158], [164], [165], [168], [183], [184], [199], [215], [232], [235], [250], [251], [258].

6.1. Technické prostředky počítačové bezpečnosti

Opatření v rámci počítačové bezpečnosti proti *vnějším útokům*, např. z externích počítačových sítí, jsou záležitostí převážně technického charakteru. Preventivní opatření tohoto typu je třeba centrálně koordinovat a postavit na předpisech obecně závazného bezpečnostního standardu. U nás doposud tyto útoky ve větším rozsahu bezprostředně nehrozily, případně byly jen velmi málo pravděpodobné, protože zde dosud nejsou externí sítě příliš rozšířeny. Určitý prostor ale skýtá existence faxmodemových karet. Specifickým problémem je ochrana proti odečítání informací z vlnění vycházejícího z počítače. Útoky tohoto typu lze očekávat jen u dat s nejvyšším stupněm důležitosti. Lze jim čelit vhodným architektonickým řešením budov, v nichž počítače pracují, isolací zdí, krytů počítačů a dalšími technickými prostředky.

Při bezpečnostních opatřeních technického charakteru je třeba vycházet z toho, že oprávněný uživatel může disponovat třemi kopiemi software

-datovým nosičem, který zakoupil s originální licencí (diskety, CD-disky),

-záložní (bezpečnostní) kopií,

-kopií na pevném disku počítače.

Každá další kopie je nelegální. V rámci toho můžeme přistoupit na určitá bezpečnostní opatření technického charakteru proti *útokům „zevnitř“*. Technické prostředky prevence jsou obecně buď softwarové nebo hardwarové.

Z nich softwarové jsou častější, početnější a obecněji využitelné. Jejich výhodou je možnost tvorby vlastních produktů nad rámec zabezpečovacích prostředků dodávaných přímo profesionálními výrobci software. Vlastní prostředky mohou být přizpůsobeny přesně potřebám uživatele, typu dat a práce s nimi. Nejběžněji jsou používána přístupová hesla, metody šifrování dat, různé bezpečnostní segmenty, tzv. zámky, vložené do aplikací aj.

Použití hardwarových prostředků je užší, avšak neméně důležité. Zvláště při prevenci zamoření systému viry jsou nenahraditelné. Jde např. o hardwarové odpojení pevného disku při čtení cizí, případně viry zatížené diskety. Ke zvýšení počítačové bezpečnosti lze použít také hardwarových zámků, které jsou dodávány k některým firemním systémům z důvodů autorské ochrany software. Bez připojení takového zámku na vývody počítače, např. k tiskárně, nelze daný systém spustit. Odebráním a uschováním zámku lze zamezit určitým aktivitám neoprávněných osob. Dalším zajímavým a dosud málo využívaným způsobem zvýšení počítačové bezpečnosti je pořízení takové konfigurace počítače, že tento je schopen

číst jen diskety nějak netypicky formátované. Zde pak jde o metodu na pomezí softwarové a hardwarové ochrany.

Ochrana Windows. Počátkem září 1998 bylo na českém trhu představeno originální řešení přístupu do Windows pomocí otisku prstu a čipové kartičky. Tuto technologii původně v 60. a 70. letech využívala pouze policie. Jak šel vývoj výpočetní techniky kupředu, došlo k vývoji a dostupnosti i technologie snímání otisků prstů. Díky software *Skytale Logon Protector* se tento způsob přístupu k datům stane dostupný téměř každému. Podle úvah odborníků se odhaduje, že cena systému by se v průběhu několika let mohla pohybovat pod hranicí dvou tisíc korun. Vývoj systému trval 1 až 1,5 roku. V současnosti existuje na světě několik výrobců, kteří se snaží vyrábět tuto technologii. Technologie otisku prstu je zajímavá pro výrobce, protože je už v současnosti technicky dostupná, a komu se podaří proniknout na trh v největším měřítku, ten bude prosperovat v důsledku její potřebnosti a praktičnosti. Německá společnost *Skytale Data Security* se zabývá vývojem bezpečnostního software pro Windows a další operační systémy. Má velké ambice na opanování trhu v tomto směru. V současné době existuje stále více uživatelů, kteří potřebují chránit svá data před tím, aby je mohl používat někdo jiný. *Logon Protector* chrání přístup k počítačům tak, že přihlásit se do systému mohou jen ty osoby, které prokázaly svou totožnost nejen znalostí hesla, ale i další metodou, a to vlastnictvím identifikačního předmětu, například čipové karty. Nebo se prokázat otiskem prstu, popřípadě obojím. Distributorem *Logon Protector* v České republice je tč. společnost *RKK Informationssysteme*.

Systémy využívající identifikační karty s čipem nejsou zase tak velkou novinkou. V zahraničí i u nás se již celkem běžně používají např. při zabezpečování vstupu do místností, hal, skladů nebo jiných prostor. Jejich výhodou je, že každému držiteli lze do čipu jeho karty naprogramovat podle potřeby naprosto individuální oprávnění, které lze navíc průběžně měnit. Vše lze zajistit například tak, že všichni pracovníci mají možnost projít hlavním vchodem, do jídelny, zasedací místnosti atd. Jen vybraní pracovníci ale mohou vstupovat do skladu, sekretariátu ředitele, výpočetního střediska nebo rizikových provozů apod. Speciální kódy na kartách umožňují dokonce vystopovat vysílačky, přenosné počítače a další cenné předměty nesené návštěvníky. To vše může při vhodně organizovaném provozu podniku zvýšit počítačovou bezpečnost.

**

Bezpečnostní počítačové karty. Zkušenostem s jiným hardwarovým prostředkem u nás vyráběným je věnována recenze [232]. Zabývá se bezpečností dat v počítači pomocí speciální bezpečnostní karty (Security Card), která znemožňuje neoprávněné užití personálního počítače IBM a dat v něm obsažených. Tato karta definuje přístupová práva k počítači několika různým uživatelům, u verze *Security Card Economy* třem, u novější verze *Security Card Stat* až osmi uživatelům, vede statistický přehled o použití počítače a výrazně omezuje až znemožňuje napadení počítače viry, včetně jejich šíření. Karta je výrobcem dodávána s registračním dokladem, licenční smlouvou, zapečetěnou obálkou s hlavním heslem, disketou, dotykovými paměťmi a stručným návodem k rychlé instalaci. Nastavovat

konfiguraci tohoto zařízení může pouze správce systému. Přístup správce systému k nastavování konfigurace je tedy heslem, přiložením dotykové paměti nebo obojím. Pokud správce zapomene svoje heslo nebo ztratí dotykovou paměť, k nastavování konfigurace se dostane pouze zadáním hlavního hesla. Heslo je nejslabším článkem celého systému, neboť jeho ochrana není záležitostí daného zařízení ale chybujících lidí. Proto heslo správce a hesla jednotlivých uživatelů by měla být uložena pouze někde mimo, řekněme pouze v jejich mysli a hlavní heslo pak v trezoru v zapečetěné obálce. Nastavování konfigurace má možnost kontrolovat auditor systému. Ten pod svým heslem má přístup ke všem nastaveným hodnotám, které však nemůže měnit. U bezpečnostní karty přiděluje správce přístupová práva až pro tři uživatele. Každý uživatel musí mít definované maximálně osmiznakové jméno. Přístup k počítači po jeho zapnutí může být uživateli povolen až po zadání hesla, které může být libovolně dlouhé, nejméně však 4 znaky. Správce systému může uživateli povolit, aby si heslo sám měnil. Přístup uživatele k počítači může být rovněž omezen nutností použít osobní dotykovou paměť. Každému z uživatelů správce přiděluje práva přístupu k jednotlivým logickým diskům a disketovým jednotkám. Disk může být pro uživatele zamknut – vypadá jako prázdný a chráněný proti zápisu. Druhou možností je, že disk je přístupný pouze pro čtení na něm uložených dat, která tak nelze měnit ani doplňovat. Dokonce je možné omezit přístup i k jednotlivým adresářům a znemožnit (zrušit) atribut DOSu *Read Only* (soubor pouze pro čtení). Disk je možno i zcela odemknout, data může uživatel číst i zapisovat. Veškerá omezení fungují pochopitelně i pro případný vir. Pro jednotlivé uživatele definuje správce další speciální funkce, jako např. zapnutí ochranného systému, vypnutí určitých funkcí, např. řízení diskových operací, formátování disket, apod. To hraje určitou důležitou roli při ochraně medií před šířením virů či před nežádoucím zavádění operačních systémů. Lze tak zabezpečit bootování pouze z pevného disku a zabránit tak proniknutí bootových virů do počítače ze zapomenuté nakažené diskety při zapnutí počítače. Pokud dané zařízení detekuje činnost viru, zablokuje počítač a informuje uživatele o nálezu výpisem na obrazovku. Rovněž vítaná je záměna disketových snímačů *A* a *B*. Tato funkce realizuje v případě, že počítač je vybaven dvěma disketovými mechanikami, operativní přepojování kabelů uvnitř počítače pro každého uživatele. Systém umožňuje též zamknout klávesnice - je-li tato příslušná volba zapnuta. Brání též uživateli přerušit provádění souborů důležitých startovacích programů *CONFIG.SYS* a *AUTOEXEC.BAT*. Zařízení je vybaveno též testovací funkcí na viry a zablokuje počítač při nebezpečí napadení v běžném provozu. Tím je zabezpečena i standardní úroveň protivirové ochrany. Každému uživateli lze nastavit individuální časový interval během dne, kdy se smí přihlásit a pracovat s počítačem. Při pokusu o práci s počítačem mimo tuto dobu je počítač zablokován. Je-li pracovník označen jako automatický uživatel, dojde po zapnutí počítače k jeho automatickému přihlášení. Tuto funkci lze použít zvláště k automatickému spouštění nějaké činnosti bez přítomnosti obsluhy (v noci) zejména ve spojení s předchozí funkcí časového omezení. Běžný uživatel nemusí po zapnutí počítače při přihlašování psát uživatelské jméno, stačí pouze stisknout určitou klávesu. Nutnost zadávat heslo při nastavení odpovídající funkce zůstává beze změny. Kromě výše uvedených funkcí, které může správce nastavit individuálně každému uživateli jinak, má zařízení další možnosti zamezení neoprávněné manipulace s počítačem. Je to zámek počítače, který zabraňuje přístupu k počítači vyjmutím bezpečnostní karty. Pokud aktivuje správce systému tuto funkci,

upraví se údaje na pevném disku tak, aby nebylo možné počítač používat bez aktivní karty. Pokud nepovolaná osoba vyjme bezpečnostní kartu z počítače a zapne jej, dostane zprávu, že nebyla nalezena bezpečnostní karta. Zároveň je blokována možnost zavedení operačního systému z diskety. Podle výrobce nelze pevný disk z počítače vyjmout a instalovat jej do jiného počítače jako druhý nesystémový pevný disk. Pokud by se pachatel odhodlal k neoprávněnému ovládání počítače myší místo zamknuté klávesnice, může narazit na zamknutí příslušného seriového portu. I na to je v daném systému pamatováno. Bezpečnostní karta umožňuje jednoduchým způsobem aktualizovat své programové vybavení (firmware) změnou obsahu paměti flash. Stačí po smazání starého firmware do počítače zasunout disketu s novým programem a spustit jej. Nejnovější verze tohoto systému umožňuje maximální ochranu dat uživatele. Data na pevném disku nebo disketách mohou být uložena šifrovaně tak, že jsou bez současné znalosti klíče nedostupná. Uživatel může zvolit poměr mezi požadovanou bezpečností dat a rychlostí jejich šifrování a dešifrování. *Security Card Stat* umožňuje definovat osm různých uživatelů jednoho počítače. Mimo správce je v systému definován i auditor, který kontroluje činnost všech uživatelů i správce. Auditor má k dispozici velmi podrobný statistický záznam činnosti všech uživatelů i správce. Systém *Security Card* je určen těm, kteří potřebují maximálně zabezpečit data ve svém počítači především proti působení virů a neoprávněnému přístupu k počítači. Správně nastavené funkce systému mohou znemožnit nebo alespoň velmi ztížit nekalou činnost potenciálního počítačového pachatele.

Speciální ochrana dat. V roce 1994 předvedla poprvé u nás pardubická firma *AIM-computer, s. r. o.* ve spolupráci se zástupci německé firmy *Siemens-Fürth* řadu přístrojů pro zabezpečení dat proti nežádoucímu úniku informací při jejich zpracovávání na osobních počítačích i periferiích a pro jejich kvalitní a bezpečný přenos. Současně představila zařízení pro zabezpečení přístupových cest na chráněná pracoviště. Protože se v řadě případů jedná o výjimečnou techniku, autor studie [258] požádal pořadatele semináře, aby konkrétní informace a technická data zůstala nedostupná třetím osobám kvůli nebezpečí zneužití a možnému oslabení účinnosti příslušných systémů. Proto naše zprostředkovaná informace je jen obecného rázu. O konkrétních otázkách, například o konfiguracích a vybavení počítačů, musí uživatel jednat přímo s odborníky z firmy, případně s prodejci a distributory. Ochrana dat, zpracovávaných na osobních počítačích, patří mezi důležité prvky bezpečné manipulace. Ve vyspělém počítačovém světě je středem zájmu, zejména v ozbrojených a bezpečnostních silách, ve státní správě, ale i v soukromém sektoru, především v bankovnictví a pojišťovnách. Přísné normy, například v USA, SRN, Velké Británii a jiných zemích, určují několik zón bezpečnosti proti vyzařování tzv. kompromitujících informací při práci s daty na personálních počítačích a periferních zařízeních, při jejich přenosu a archivování.

**

Odezírání monitorů pomocí elektromagnetického vyzařování. Je všeobecně známo, že počítače a další elektronická zařízení vyzařují elektromagnetické vlnění, které může rušit příjem rádiového a televizního vysílání. Ale,že je možné vlnění vycházející z počítače zachytit a jeho analýzou zjistit například co zrovna uživatel píše na klávesnici, je už známo méně.

Autor pojednání [157] uvádí, že možnost rekonstrukce dat zpracovávaných počítačem z vlastností vyzařovaného elektromagnetického pole není pouze teoretická. Ze středoškolské fyziky je známo, že při pohybu elektronů se zrychlením, vzniká v okolí vodiče časově proměnné elektrické pole. To je příčinnou vzniku pole magnetického. Výsledné pole má dvě navzájem neoddělitelné složky - elektrickou a magnetickou, které tvoří elektromagnetické pole. Jeho existence je podmíněna vzájemným vztahem mezi oběma složkami. Změnami elektrické složky pole vzniká pole magnetické a změnami magnetické složky pole vzniká pole elektrické. Tento děj vzájemných přeměn obou složek se v podobě elektromagnetického vlnění šíří prostorem. Obě pole oscilují s frekvencí závislou na změnách v pohybu elektronů ve vodiči.O tom že počítače vyzařují elektromagnetické vlnění, které může být využito k nelegálnímu zisku informací o zpracovávaných datech, věděly vojenské a vládní organizace přinejmenším od začátku šedesátých let. Jak dále zdůrazňuje studie [157], tato technologie je vládami stále intenzivně využívána a řada informací proto pochází z těžko verifikovatelných zdrojů. Takové informace jsou pak zpravidla uváděny standardní formulací „existují zprávy…“. Např. při luštění francouzské diplomatické šifry ve Velké Britanii v roce 1960 si operátoři všimli, že spolu s přenášeným šifrovaným signálem je přenášen ještě další, slabší signál. Ukázalo se, že to byl nešifrovaný text, který nějakým způsobem unikal ze šifrovacího stroje. Veřejné publicity se této problematice úniku informací elektromagnetickým vyzařováním dostalo poprvé v roce 1985. Ukázalo se, že rekonstrukce informací ze zachyceného elektromagnetického vlnění není pouze záležitostí profesionálů vybavených komplikovaným a patřičně drahým zařízením. Bylo pokusně ukázáno, že je možné s použitím velmi jednoduchého zařízení odezírat obraz z počítačového monitoru vzdáleného několik stovek metrů. Zařízení se skládalo z jednoduché směrové antény, zesilovače anténního signálu a obyčejného černobílého televizoru, doplněného o ovládatelné oscilátory pro nastavení synchronizace. Aby se rozptýlily pochyby i těch největších skeptiků, z auta zaparkovaného na parkovišti byly pořízeny fotografie obrazovky počítače s textovým editorem, který se nacházel v blízké budově.

Po potvrzení výsledků pokusů s únikem informací z počítačů vlivem elektromagnetického vyzařování, bylo poukázáno na možnosti zneužívání tohoto jevu. Zdrojem největší části vyzařovaného vlnění je pravděpodobně počítačový monitor. Experimentální měření ukazují i na nebezpečí plynoucí například z odposlechu sériových linek. Diskutuje se i o dalších nebezpečích, ale tyto úvahy nejsou zatím podloženy dostupnými praktickými výsledky. Vedle elektromagnetického vlnění vyzařovaného do prostoru, může být zdrojem úniku informací vlnění, které se šíří po připojených vodičích, jako jsou přívod z elektrické sítě a telefonní linka. Podle [157] existují zprávy o tom, že německé tajné služby (možná i některé jiné) využívají sledování elektromagnetického vlnění kabelu klávesnice. Účinnost monitorování je v tomto případě několik stovek metrů a lze tak zjistit i informace, které nejsou vypisovány na obrazovku, ale jen psány na klávesnici. V některých zemích jsou stanoveny standardy uplatňované ve vládních a vojenských organizacích, pokud jde o požadavky odolnosti proti odposlechu elektromagnetického vyzařování. Zařízení, na kterých jsou zpracovávány utajované informace, musí být otestována, zda splňují stanovené požadavky. Tyto požadavky i způsob jejich hodnocení bývají utajovány.

Speciální výzkum TEMPEST. Vláda Spojených států v minulosti financovala utajovaný výzkumný program s kódovým názvem *TEMPEST (Temporary Emanation and Spurious Transmission)*. Jeho cílem bylo vytvoření standardu pro omezení možností úniku informací z počítačů vlivem vyzařování. Jak uvádí [157], kódové označení programu se později stalo synonymem pro celou oblast úniku informací elektromagnetickým vyzařováním. Můžeme se setkat s TEMPEST zařízeními, TEMPEST standardy, TEMPEST útokem atd. Pro zařízení odolná proti TEMPEST útokům je ve Spojených státech v současné době platný standard *NACSIM 5100A.* V *NATO* platí obdobný standard *AMSG 720B.* Oba dokumenty jsou tajné. V Německu a ve Velké Británii navíc existují samostatné normy. Zařízení vyhovující těmto standardům jsou několikanásobně dražší než jejich nechráněné protějšky. Jejich nasazení je proto omezeno na použití v diplomatických službách a ve vojenství pro ochranu citlivých informací. Ochrana tempestovaných zařízení spočívá v omezování vyzařovaných emisí, instalací filtrů na jednotlivá připojená metalická vedení a především použitím vodivého stínění u jednotlivých částí zařízení, případně celých místností nebo budov. Existují i návrhy na jiný, levnější způsob zajištění ochrany před únikem dat. Bylo například navrženo zařízení, které by podle zadaného klíče měnilo pořadí vykreslování řádků na obrazovce. Tím by bylo zabráněno nebo alespoň ztíženo sledování obrazu na monitoru počítače. Softwarové řešení téhož problému navrhují ve své práci z roku 1998 specialisté z univerzity v Cambridge. Je obtížné posoudit do jaké míry jsou tato opatření účinná, protože prakticky všechny informace o reálném použití tempestových technologií jsou utajované.

Podle [157] existují také čerstvé zprávy o možnosti tzv. *aktivního sledování,* kterým je možné získat informace i ze zařízení chráněných proti klasickému pasivnímu monitorování. Při takovémto aktivním sledování je citlivé zařízeni bombardováno vlněním o vysoké frekvenci. Odraz vlnění je deformován a z této deformace je možné získat potřebné informace. Aktivní sledování využívá toho, že stínění je účinné jen pro určité frekvence a zvláště jen v některých místech, jako například poblíž ventilace obyčejně selhává. Podle znalosti tohoto faktu se mimo jiné také vysvětluje, proč byly západní ambasády v Moskvě v takovém rozsahu bombardovány mikrovlnami. Dříve se usuzovalo, že to může být kvůli běžnému odposlechu s použitím mikrofonů ve zdech. Podle [157] neexistují dostupné záznamy, podle kterých by bylo možné usuzovat do jaké míry je v současné době monitorování elektromagnetického vlnění využíváno. I z volně dosažitelných zdrojů je však zcela jasné, že to technicky realizovatelné je. Existují zprávy, že tempestových technik vlády silně využívají a získávají díky tomu cenné informace. Proto se snaží co nejvíce zpomalit či nejlépe zastavit šíření přesných informací o účinnosti, resp. o míře nasazení těchto technik. Podobně tomu bylo u kryptografie a počítačové bezpečnosti citlivých informací vůbec.

**

Nadnárodní aspekty tempestování počítačů. Jak uvádí [258], v blízké budoucnosti se v rámci Evropské unie mají národní normy přiblížit „evropskému“ předpisu *ITSEC*. V NATO platí údajně nejpřísnější norma v tomto oboru, která je tajná a nejsou veřejně přístupné ani její základní technické požadavky, týkající se například způsobů měření vyzařování atd.

Pracovníci firem *AIM-computer, s. r. o.* a *Siemens-Fürth* předvedli osobní počítač se sníženým indukčním elektromagnetickým vyzařováním, který je odolnější proti úniku informací, tzv. *tempestovaný personální počítač*. I bez technických podrobností je zřejmé, že jde o konstrukční úpravy, stínění a zabezpečení ovládacích prvků proti nežádoucí manipulaci, které zabraňují možné detekci počítače, například přes energetické sítě v místnosti a okolí. Ochrana před vyzařováním tempestovaných počítačů odpovídá nejpřísnějším bezpečnostním předpisům a jednotlivé typy přístrojů uvolňují pro práci s utajovanými skutečnostmi příslušné státní orgány. V SRN je to například *Spolkový úřad pro bezpečnost a informační techniku*. Stupeň omezení vyzařování tempestovaných počítačů, jejich velká nebo částečná odolnost vůči detekci, rozhoduje o jejich využití a umístění s ohledem na charakter objektu, dislokaci místnosti, na vzdálenosti například od veřejně přístupných míst a rozvodů sítí. Součástí komplexního zabezpečení jsou zpravidla ještě další prvky, které ve spojení s personálními počítači zabezpečují k nim oprávněný přístup nebo bezpečný přenos a zpracování dat. Jako příklad uveďme podle [258] biometrický osobní identifikátor s elektronickým snímačem otisků prstů s vyhodnocovací elektronikou. Lze ho například využít k ovládání elektrických zámků a k dalšímu identifikování osob pomocí otisků prstů. Přístroj údajně posuzuje nejen obrazce papilárních linií, ale i biometrické prvky, takže není například možné využít tzv. mrtvý prst, tj. preparovanou kůži z amputovaného prstu. K počítači je možné připojit i další snímače, například snímače čipových karet a jiných nosičů, které slouží pro přenos a vyhodnocování dat k identifikaci osob. Ukázky produktů citované firmy se týkaly i dalších stíněných zařízení, kromě stíněné tiskárny. Na místě bylo prakticky předvedeno, jak lze energii vyzařovanou počítačem zachytit a využít. Předváděna byla i technika pro přenos dat pomocí optického vlákna a bezdrátově laserovým paprskem. Současně byla předváděna digitální hovorová a datová paměť, umožňující registraci, snadné vyhledání a využití předávaných hlasových zpráv při telefonických hovorech s možností dokumentovat je například pro potřeby orgánů činných v trestním řízení či pro jiné důležité účely. Signálové kanály, například telefon, rádio, elektrický vrátný a jiné se napojují na záznamovou jednotku. Vyhodnocovací jednotka může být umístěna nezávisle a systém lze využívat k organizačním i technickým účelům uživatele. Datový provoz u všech příchozích spojů je neustále sledován a lze jej kdykoli reprodukovat, smazat či archivovat na běžných kazetách či disketách. Pokus o přepis nebo změnu zaznamenaných dat je registrován, je snadno odhalitelný a údajně vždy neúspěšný. Systém spolehlivě funguje i při velkém zatížení. Jako příklad bylo uvedeno zvládnutí až 7 000 příchozích hovorů týdně.

Postupující miniaturizace. Zahraniční partner firmy *AIM-computer*, s. r. o. předvedl též kompaktní tempestovanou soupravu notebooku, tiskárny a fax-modemu, určenou pro pracovníky v terénu a umístěnou proto v přenosném kufříku standardních rozměrů. Mobilní počítač tak může být provozován v osobních automobilech, na externích a terénních pracovištích apod. Samozřejmostí je, že může být napájen například z palubní sítě dopravních prostředků. Dostupnost předváděných tempestovaných přístrojů pro české zákazníky nebyla v praxi dosud ověřena. Jejich dovoz do České republiky podléhá schvalovacímu řízení, mj. i NATO, ale není již zakázán. Podle podaných informací pracuje v zahraničí na 95 % tempestovaných počítačů ve státní správě na úseku obrany a bezpečnosti a zbytek je uvolněn

pro civilní sféru. Podle [258], v SRN je údajně nasazeno asi 1000 chráněných personálních počítačů. Zajímavé jsou cenové relace. Cena tempestovaného počítače je zhruba desetkrát vyšší než počítače v komerčním provedení, stejně tak tomu je u stíněných tiskáren. Náklady na úpravy místnosti proti nežádoucímu úniku informací přijdou u nás podle odhadu prezentující se firmy asi na 1 mil. Kč.

Nebezpečí oklamání bezpečnostních systémů odečtem. Jak uvádí autor studie [258], pokud jde o ochranu objektů, speciálně o oprávnění přístupu do objektů, upozorňují odborníci na zkušenosti s identifikačními kartami. Doporučují používat takové pomůcky, na kterých nejsou uváděna jména, ale pouze příslušnost k firmě či pracovišti, podle zvážení i fotografie a zejména technický prostředek individuální osobní identifikace. Z praxe policejních i jiných bezpečnostních složek je totiž známo mnoho případů zneužití „odečtených" jmen pro kriminální trestnou činnost. Nerespektování těchto zkušeností může často anulovat účinnost poměrně drahých technických prostředků ochrany objektů.

**

Bezpečnost čipových karet. Čipové karty poskytují velmi levnou implementaci jednoho z bezpečnostních konceptů, který se anglicky nazývá *„tamper resistant hardware"*, hardware odolný proti útoku. Jak je uvedeno v [63], jde o hardwarový modul, obvykle vybavený mikroprocesorem, obsahujícím nějaká chráněná data a algoritmy, které na základě příkazů z vnějšího světa s těmito daty manipulují. Tato vlastnost se obvykle využívá dvojím způsobem:

1)Modul v sobě obsahuje data, se kterými je možno manipulovat pouze jistým způsobem. Příkladem může být předplatní (telefonní) čipová karta, obsahující čítač impulsů, kterým je možno pouze snižovat a nikdy ne zvyšovat počet impulsů.

2)Modul má v sobě tajný kryptografický klíč, který nikdy nevypustí ven a je pouze ochoten s tímto klíčem provést jistou kryptografickou operaci. Příkladem může být *autentizační čipová karta*, která prokazuje totožnost pomocí zašifrování vložených dat uloženým tajným klíčem. Tomuto typu bezpečného hardwaru se někdy také říká *kryptografický bezpečný hardware*.

Základní vlastností čipové karty je skutečnost, že ji nelze implementovat čistě softwarově bez pomocí speciálního hardwaru. Např. předplatní telefonní kartu nelze realizovat softwarově, protože útočník by prostě pomocí binárního editoru přepsal obsah čítače na libovolnou hodnotu a měl by tak nevyčerpatelný zdroj bodů nebo impulsů. Velmi rozšířeným jevem, se kterým je možno se setkat u čipových karet, je utajováni algoritmů. Algoritmy použité v aplikacích s čipovými kartami, ať kryptografické či nekryptografické, bývají poměrně často utajovány nebo aspoň „nezveřejňovány". Děje se tak v daleko větší míře než u softwarových aplikací. Důvodem je to, že vlastnost bezpečného hardwaru, tj. ochránit data před neoprávněným přístupem, se dá velmi snadno využít i pro ochranu použitých algoritmů před prozrazením. Zatímco u čistě softwarového systému nelze efektivně utajit žádný algoritmus, protože nakonec ho vždycky někdo „zreverzuje" a zveřejní, u hardwarového systému tato možnost existuje. A vývojáři aplikací s čipovými kartami ji také zhusta využívají. Zvlášť v minulých letech panovaly v této oblasti až paranoidní názory.

Nejen že se utajovaly algoritmy, kryptografické přístupy šifrování - kryptografické protokoly a datové struktury, ale „nezveřejňovaly“ se ani samotné příkazy čipových karet.

Čipové karty se původně dodávaly pouze „prověřeným“ odběratelům, po podepsání různých závazků a prohlášení, doprovázených vysokými smluvními pokutami. Podle [63] tento způsob zabezpečení, zvaný „*security through obscurity*“, což znamená přibližně „*zabezpečení pomocí obskurnosti*“, je svou účinností asi tak bezpečný, jako ukládání klíče pod rohožku. První pokusy o útoky na čipové karty se vyskytly v oblasti telefonních karet. Telefonní karta typicky není procesorovou kartou, ale jde o kartu se speciální logikou. Telefonní karta má elektronický protokol, kterým říká své identifikační číslo a počet impulsů, které ještě na ní zbývají. Tento protokol samozřejmě není utajován a každý, kdo vyvine určitou energii, si jej může opatřit. Pak ovšem platí, že jakékoli zařízení, které odpoví na dotazy telefonního automatu a bude dodržovat tento protokol, bude telefonním automatem akceptováno jako platná telefonní karta. Tím je také dáno, že nejčastějším útokem na telefonní karty je tzv. *emulace.* Spočívá ve vytvoření zařízení (emulátoru), které se chová z hlediska elektrického protokolu jako platná telefonní karta s jediným rozdílem - neklesá na něm počet impulsů. Konstruktéři stávajícího systému telefonních karet se ani nesnažili o nějaké lepší zabezpečení. Bezpečnost systému totiž spočívá v tom, že cena emulátoru je natolik vysoká, že neodpovídá zisku útočníka. Existence emulátorů - „věčných telefonních karet“ - v tomto případě tudíž neznamená selhání bezpečnostního mechanismu, ale selhání člověka, který vzal systém, vytvořený pro konkrétní provozní prostředí a bez provedení bezpečnostní analýzy jej přemístil do provozního prostředí zcela jiného. Analogické problémy existují i u jiných typů čipových karet. Např. díky chybám v algoritmu čipových karet *SIM* mobilních telefonů *GSM,* je možné během několika hodin vytvořit kopii SIM-karty nazvanou *klon*. Na tomto případu je asi nejmarkantněji vidět škodlivost koncepce přístupu „security through obscurity“ v utajování algoritmů. Uvedené příklady problémů s telefonními čipovými kartami, i když zdánlivě počítačové kriminalitě odlehlé, byly zvoleny pro větší srozumitelnost i názornost.

Výroba čipových karet jako škola počítačového hackerství. Podle [63] emulace telefonních karet není však pro hackery dnes už příliš zajímavá. Hacker potřebuje oblast, která je pro něho intelektuální výzvou, dá se na ní získat sláva i jistý okamžitý prospěch při minimu rizika. Tyto podmínky přesně splňují satelitní šifrovací karty. Satelitní karty slouží pro dekódování satelitních televizních programů, které jsou vysílány zašifrované a které jsou určeny pouze pro ty diváky, kteří si za nemalý peníz koupí odpovídající dekódovací kartu. Dekódovací karta je čipová karta, která v sobě obsahuje tajný klíč (nebo několik klíčů) a šifrovací algoritmus, který je někdy tajný a někdy veřejný. Satelitní přijímač do karty občas zasílá krátkou zprávu, kterou karta pomocí klíče dešifruje a tím se získá tajná hodnota, se kterou je možno dekódovat několik dalších sekund obrazu. Je jasné, že pokud by byl prozrazen klíč (a algoritmus), je možno opět vytvořit emulátor karty, pomocí něhož je možno dekódovat přijímaný signál. Pokud je takový emulátor (obvykle nazývaný pirátská karta) prodáván za rozumnou cenu, může se stát masově prodávaným zbožím. A to se právě stalo. Během několika málo let se vytvořil takřkajíc průmysl na výrobu pirátských čipových karet, který plynule zásobuje své zákazníky kartami. Samotná existence satelitních pirátských karet

není z globálního pohledu příliš závažná. Týká se několika málo společností, které si tento stav vlastně zavinily samy. Jiných technologických odvětví se tato činnost příliš netýká, protože kromě satelitní televize se tímto způsobem čipové karty prakticky nepoužívají. Problémem je zcela jiná věc, daleko závažnější. Satelitní čipové karty se totiž staly objektem, na kterém se vyučili vysoce nebezpečným schopnostem hackeři, kteří by se jinak pravděpodobně vůbec nepustili do útoků proti počítačovým ochranám vyšších stupňů, např. bankovních systémů. To je také důvod, proč zdánlivě odtažitou problematiku deliktů kolem čipových karet lze zahrnout do oblasti počítačové kriminality.

Bezpečnost počítačových systémů s čipovými karatami. Pokud se pozornost útočníků soustředila na satelitní čipové karty mohli vývojáři finančních počítačových aplikací s čipovými kartami tvrdit, že satelitní čipové karty tvoří v bezpečnosti čipových karet nižší úroveň, a že jejich „bankovní" čipové karty jsou na tom z hlediska bezpečnosti zcela jinak a lépe. Vzhledem k důslednému utajováni jak vlastností čipů, tak i samotných kryptografických protokolů, bylo obtížné jim v tomto oponovat. Jedním z těchto elektronických projektů je systém *Mondex*, patřící mezi nejrozšířenější. Jeho výrobce tvrdil např., že „systém poskytuje úroveň bezpečnosti, která předbíhá úroveň zločinců dnes a bude ji předbíhat i zítra". Jak uvádí [63], tato tvrzení bylo opět obtížné zpochybnit. Až v květnu 1996 *Národní banka Nového Zélandu (NBNZ)* v rámci pilotního projektu nechala otestovat bezpečnost systému *Mondex* nezávislou organizací. Výsledkem bylo memorandum, které konstatovalo, že bezpečnost prověřované verze systému je nedostatečná a systém není dostatečně odolný proti útoku, což auditor konkrétně demonstroval. Dalo by se očekávat, že toto odhalení způsobí rozruch. Avšak výsledky auditu byly před veřejností více než jeden rok utajovány a posléze vyzrazeny na Internetu. Celá věc měla mít soudní následky. K vině se však nechtěl přihlásit nikdo. Výrobce čipu (*Hitachi*) prohlásil, že jde o starou verzi, která již není podporována a proto neměl být čip použit. Výrobce systému *Mondex* prohlásil, že bezpečnost systému je „odpovídající způsobu použití", přičemž „způsob použití", jinak maximální částka, uložená v „elektronické peněžence", nebyl nikde jasně definován. Takže „Černý Petr" zůstal asi v rukou bank. Bylo by krátkozraké tvrdit, říká autor studie [63], že tyto případy svědčí o nedostatečné bezpečnosti čipových karet. Spíše jde o to, že čipové karty jsou, jako každý jiný produkt, jen více či méně kvalitní a tedy více či méně bezpečné. Kvalitu čipových karet však nemůžeme nikdy posuzovat podle marketingových tvrzení výrobce nebo vývojáře aplikace, ale pouze podle výsledků nezávislého auditu. Nejde proto většinou o selhání počítačového či jiného systému vlivem špatných čipových karet, ale spíše o selhání člověka, který ve své neznalosti, domýšlivosti či nedbalosti nerespektoval základní bezpečnostní zásady a použil příslušné prvky nesprávným způsobem.

**

Zákon o ochraně topografií polovodičových výrobků. Podle [251] jsou zákonem chráněny topografie polovodičových výrobků, které jsou výsledkem tvůrčí činnosti původce a které nejsou v průmyslu polovodičových výrobků běžné. Ochrana podle tohoto zákona se vztahuje rovněž na části topografie polovodičových prvků, které jsou využitelné samostatně, jakož i na zobrazení sloužící k výrobě topografie. Ochrana se nevztahuje na technologii užitou

při vytváření topografie nebo při výrobě polovodičového výrobku, ani na informace uložené v tomto výrobku. Topografií se pro účely tohoto zákona rozumí série jakkoli zafixovaných nebo zakódovaných vzájemně souvisejících zobrazení, znázorňujících trojrozměrné trvalé uspořádání vrstev z nichž se polovodičový výrobek skládá, přičemž každé zobrazení znázorňuje vzor jedné vrstvy polovodičového výrobku v jednotlivých stupních výroby nebo jeho částí. Polovodičovým výrobkem se pro účely tohoto zákona rozumí konečná nebo mezitímní forma mikroelektronického výrobku, který je určen k plnění elektronické funkce a který se skládá ze základního tělesa obsahujícího vrstvu polovodičového materiálu a opatřeného alespoň jednou vrstvou vodivého izolačního nebo polovodičového materiálu v předem daném uspořádání. Tento zákon nabyl účinnosti dnem l. ledna 1992 a je sankcionován podle ustanovení §151-§152 trestního zákona. Blíže k tomu viz [199].

**

Ochranné valy (firewally). Připojení lokální počítačové sítě do Internetu přináší kromě naprosto zřejmých výhod i některé nevýhody. Protože však potenciální výhody převyšují případné nevýhody, není odpojení od Internetu zrovna nejlepším řešením. Zbývá tedy pouze možnost minimalizovat případné nevýhody nebo hrozby, které takové připojení přináší. Autoři studie [183] k tomuto účelu doporučují využít místo, ve kterém se lokální síť připojuje k Internetu a umístit zde tzv. *firewall*. *Firewall* je kombinace hardwarových a softwarových prostředků poskytující kontrolu přístupu k síťovým službám, adresnou zodpovědnost, jednotný bod pro některé síťové služby a ukrytí části vnitřní sítě. *Firewall* ale nezabrání útoku z vnitřní strany sítě a také není schopen reagovat na neznámé hrozby.

Paketové filtry. Pokud jde o druhy firewallů, rozlišujeme *paketové filtry* a *aplikační brány*. Paketové filtry jsou celkem levným a poměrně účinným způsobem zabezpečení vnitřní sítě. Na většině směrovačů, které se používají pro připojení k Internetu, jsou paketové filtry součástí programového vybavení. Paketový filtr pracuje na principu kontroly některých polí v hlavičkách paketů. Tato pole porovnává s pravidly uloženými v paměti a provádí akce, které jsou v pravidle definovány. Autoři [183] uvádějí, že z hlediska počítačové bezpečnosti paketový filtr má omezené možnosti při kontrole bezpečnostních požadavků. Je schopen rozlišit jednotlivé počítače, používané služby, nebo volby v jednotlivých protokolech na jistých úrovních. Není však již schopen rozlišit, identifikovat a popřípadě autentizovat jednotlivé uživatele, což je jistě žádaná činnost. Některé směrovače navíc realizují tzv. *překlad adres*. Překlad adres umožňuje skrýt celou vnitřní síť za jednu nebo několik síťových adres nebo rozkládat zátěž provozu, který přichází do vnitřní sítě, např. při silně vytíženém *WWW* serveru.

Aplikační brány. Aplikační bránou rozumíme speciální program, ale také počítač, na kterém tento program běží. Způsob ochrany aplikační brány je odlišný od filtrování paketů. Aplikační brána bývá umístěna mezi lokální a rozsáhlou sítí. Uživatelský klientský program místo toho, aby komunikoval se skutečným serverem poskytujícím dané služby, komunikuje s aplikační bránou. Aplikační brána musí rozumět protokolu, kterým klient se serverem komunikují. To jí umožňuje vyhodnocovat požadavky obou stran a zabraňovat tak

nepovoleným operacím. Může tak např. zabraňovat přenosu exekučních souborů. Aplikační brána je schopna autentizovat nejen uživatele, ale i jednotlivé operace. Je tedy podstatně flexibilnější než pouhý paketový filtr. Aplikační brány mají však i své nevýhody. Podle [183] spočívají v tom,

-že každá služba vyžaduje specializovanou aplikační bránu, protože používá jiný protokol,

-že aplikační brány nejsou dostupné pro všechny druhy služeb,

-že použití aplikační brány může vyžadovat modifikaci klientských programů nebo postupů při používání dané služby.

Některé služby poskytují možnost využití aplikační brány automaticky, stačí pouze vhodně nakonfigurovat klientský program. Typickým příkladem mohou být internetové *WWW* prohlížeče, ve kterých je možné nastavit tzv. *proxy*. Tato proxy vyřizuje požadavky za klienta a má možnost kontrolovat přístup k jednotlivým *WWW* stránkám. Pokud není klientský program schopen používat aplikační bránu, je nutné zvolit jiný postup. Tím je buď úprava klientského programu, nebo použití nestandardního přístupu k dané službě. Protože jsou však zdrojové texty klientského programu málokdy dostupné, je použití nestandardního přístupu ke službě tím jednodušším řešením. Autoři [183] dále ukazují na speciálním příkladu jeden z možných nestandardních přístupů. Jde o příliš speciální pojetí, proto se zde jím nebudeme zabývat. Z pohledu počítačové bezpečnosti je však důležité vědět, že uživatelé se snaží těmto opatřením vyhnout, i když jinak nemají nekalé úmysly. Prostě jim to znesnadňuje komunikaci. Pro zachování přiměřené úrovně bezpečnosti je důležité zamezit obcházení aplikační brány např. použitím paketového filtru. Tedy kombinací obou druhů firewallů.

Konstrukce ochranných valů (firewallů). Z paketových filtrů a aplikačních bran je možné konstruovat složitější firewally. Zde pomineme ryze technickou stránku problémů s tím spojených. Studie [183] uvádí čtyři základní typy,

-*jednoduchý filtrující směrovač,* konstrukce vychází z toho, že všechny počítače v lokální síti udržují přímé spojení s rozsáhlou sítí, to pak vyžaduje pečlivě zkonstruovaná filtrovací pravidla; bohužel není možné dostatečně dobře kontrolovat aktivity jednotlivých uživatelů, je tedy obtížné zajistit dostatečnou bezpečnost spolu s co největší dostupností všech služeb;

-*jednoduchá aplikační brána;* lokální síť je možné oddělit od rozsáhlé sítě počítačem se dvěma síťovými rozhraními; tento počítač však není směrovačem a dokonale obě sítě odděluje; počítače z obou stran sítě mohou komunikovat pouze s tímto počítačem, což mu umožňuje jednoduchým způsobem všechna spojení kontrolovat; nevýhodou tohoto přístupu jsou omezené možnosti používání služeb druhé strany sítě; pro každou službu totiž musí na tomto počítači existovat aplikační brána;

-*směrovač a aplikační brána* - aby bylo možné používat i služby, pro které neexistuje aplikační brána, lze jednoduše zkombinovat aplikační bránu s paketovým filtrem; základní bezpečnostní opatření zde poskytuje paketový filtr; pokud pro některou službu existuje aplikační brána, paketový filtr může zablokovat všechny přístupy, které tuto aplikační bránu obcházejí; pro ostatní služby je možné použít pravidla, která tyto služby buď povolují, nebo

zakazují; v některých případech je možné sloučit paketový filtr s aplikační bránou do jednoho celku;

-*směrovač s demilitarizovanou zónou* přidává mezi rozsáhlou síť a lokální síť ještě jednu malou síť, často označovanou jako *demilitarizovaná zóna;* v demilitarizované zóně mohou být umístěny aplikační brány a služby, které lokální síť poskytuje rozsáhlé síti; vnitřní filtrující směrovač poskytuje ochranu vnitřní sítě jak proti vnější síti, tak i proti demilitarizované zóně v případě, že byla narušena; vnitřní směrovač může blokovat spojení tak, aby bylo umožněno spojení pouze mezi demilitarizovanou zónou a vnitřní sítí; vnější směrovač odděluje demilitarizovanou zónu od vnější sítě; většinou je na něm jen minimum filtrovacích pravidel, která zabraňují základním typům útoků, často bývá již ve vlastnictví poskytovatele připojení; tato architektura může být mnohovrstevná a může oddělovat od sebe sítě s různými úrovněmi zabezpečení.

Firewall není všelékem. Vnitřní sítě je sice možné bránit před nepovolaným přístupem, kvalita ochrany však *záleží většinou na finančních možnostech a hlavně na schopnostech správce sítě.*

6.2. Nehmotné prostředky počítačové bezpečnosti

Zneužívání dat. Útoky směřující ke zneužití dat, neoprávněného získání informací či způsobení změn, zničení dat ap. je bezesporu počítačovou kriminalitou velmi závažnou a u nás z hlediska dopadu poměrně opomíjenou. Přitom tyto útoky mohou mít velmi závažné důsledky. Nejedná se přitom jen o značné finanční ztráty, které mohou nastat dejme tomu peněžní instituci při nezákonných machinacích s daty, týkajících se finančních převodů. Může dojít i k jiným újmám, např. nehmotným, na osobnosti pachatele, na strategii vývoje podniku, na výrobě, na obchodních zájmech atp. Ochrana proti útokům tohoto typu tvoří stěžejní část počítačové bezpečnosti. Ke zvýšení počítačové bezpečnosti může přispět i dodatečné zjišťování neoprávněných průniků. To je však velmi obtížné. Určitým příslibem pro budoucnost je v tomto směru používání metod *fuzzy programování při odhalování* neoprávněných průniků do systému.

Ochrana dat na Internetu. Expanze Internetu a snazší přístup do sítě *World Wide Web (WWW)* zprůhledňuje jejich uživatele: Na základě dat o jejich práci v síti mohou odborníci vypracovat jejich profil a odvodit vzorce chování. Počítač na druhém konci linky dokáže vyhodnocovat vstupy do vlastních databází a protokolované záznamy pak lze použít k sestavení profilu nejčastějších uživatelů - a jednou sesbíraná data se dají poté využít, např. pro marketingové účely. Výzkumná skupina pro telekomunikace na brémské universitě zpracovala krátký program, který umožní hrozbě takového zneužití dat čelit. Adresy na Internetu se skládají ze jména uživatele a částí identifikujících počítač. Program nahradí kód uživatele znaky *xxx*. Při užití v lokálních sítích, je registrované jméno uživatele nahrazeno substitučním slovem. Program, který je zřejmě prvním krokem na cestě k dosažení standardu ochrany osobních dat, běžným u jiných komunikačních prostředků, lze získat na Internetu.

Bezpečnostní opatření proti útokům zevnitř po stránce organizační a personální jsou podmíněna množstvím možností podle charakteru podniku, technického a personálního vybavení, rozsahu práce s počítači a významnosti zpracovávaných informací.

V rámci *organizačních opatření* lze zvýšit počítačovou bezpečnost určitými omezeními v přístupu k výpočetní technice, zavedením vhodné evidence užívání systému, monitorováním práce uživatele, skartací výstupů tiskárny, jinými způsoby ochrany tzv. „počítačových sjetin“. Důležité je také stanovení způsobů tvorby, testování a předávání programových produktů pracovníků vlastní instituce dalším zaměstnancům. Tím lze zvýšit bezpečnost vůči útokům typu „trojský kůň“ nebo „zadní vrátka“. Obecně jde u organizačních bezpečnostních opatřeních o stanovení pravidel užívání výpočetní techniky a dat. Tato oblast by měla být dokonale zpracována ve vnitřním bezpečnostním standardu.

Instalace počítačových her. Určitým typem bezpečnostních organizačních opatření může být i oficiální instalace vybraných, regulérně pořízených počítačových her pro relaxační hygienu uživatelů. Význam tohoto opatření spočívá ve snížení rizika vyplývajícího z donášení cizích, často pirátsky pořízených produktů s potenciální možností přenosů virů. Některé typy her mohou působit i jako náhražka pokusů o průnik „ze sportu“, protože jejich hraní je samo o sobě tak složité, že stačí uspokojit potřebu programátora překonávat překážky.

Jako součást opatření ke zvýšení bezpečnosti vůči útokům „zevnitř“ mohou být používány i některé méně tradiční metody, jako je např. vypsání soutěže o průnik do systému, který by odhalil slabiny jeho ochrany. Poněkud diskutabilní je metoda „líčení pastí“ se zdánlivou možností průniku k tajným datům s možností sledovat přitom chování uživatele.

Oblast *personálních opatření* by měla být zaměřena nejen na určitá kriteria výběru pracovníků, ale i na způsoby stabilizace kádru pracovníků a na opatření uplatňovaná při odchodu zaměstnance z instituce. Je třeba zlepšit i finanční hodnocení pracovníků zainteresovaných na bezpečnosti počítačových systémů, což mnohdy platové směrnice zatím neumožňují.

**

Počítačová bezpečnost a aktivity některých softwarových firem. Podle [98], převážná část činnosti softwarových firem je zaměřena na bezpečnostní oblast. Různé aspekty této činnosti vycházejí z jednoho podstatného faktu, kterým je snadnost kopírování softwaru. Vytvořit nový dokonalý software je velmi složité. Stojí to hodně času, úsilí a především kombinačních invencí. Lze říci, že proces vytváření programu má obvykle tři nebo čtyři fáze. V první fázi tvůrce určuje, co bude program dělat, zda to bude například textový editor, databanka atd. Může vytvořit též základní komponenty programu. Po něm přichází na řadu psaní konkrétních instrukcí a kódů. Psaní počítačového programu je něco jako specializovaná, cílená tvůrčí činnost. Jazyk, který je přitom užíván, je speciálně uzpůsoben k tomu, aby počítač mohl jednoznačně pracovat podle posloupnosti instrukcí v programovacím jazyce zapsaných. Obrazně říkáme, že program je zapsán v počítačovém jazyce, kterému počítač rozumí. Když je program napsán, je třeba jej lokalizovat pro použití v konkrétních místech na světě, podle tam nejrozšířenějšího národního jazyka. Tak vznikají například anglické, německé, poměrně nově i české verze programů. Posledním krokem tohoto procesu je kompilování programu a jeho uložení na fyzická média, jež budou využita k distribuci

programu pro veřejnost. Takovým médiem pro program je obvykle pružný disk (disketa). Některé diskety jsou takové, jiné onaké, ale všechny jsou malé a lehké, snadno přenosné. Některý program se vejde na jednu disketu, jiný může potřebovat čtyři, pět či deset disket. Problém, kterému tvůrci v tomto ohledu čelí, je snadnost kopírování programů uložených na disketách. Jedním z charakteristických rysů kopírování videozáznamů nebo zvukových hudebních záznamů je postupné snižování kvality kopií. U hudebního záznamu můžeme podle kvality nahrávky poznat, zda se jedná o první nebo *x*-tou kopii. U počítačových disket je ale desátá, stá, či tisící kopie technicky tak dobrá, jako originál, a proto je tak snadné kopírovat i ve velkém pro případné další distribuce. Existují dva základní způsoby kopírování programů, jednak

-překopírováním programu z jedné diskety na druhou, pochopitelně prostřednictvím počítače,

-jednak překopírováním dříve instalovaného programu z pevného disku na donesenou disketu (diskety), tento způsob je oblíbenější (a rychlejší), někdy bývá označován jako „samoinstalace programu“.

Převážná část problémů výrobce pramení z popisovaného procesu. Je třeba si ale uvědomit, že zmíněný proces kopírování probíhá v rozličných kontextech a uskutečňují jej různé typy lidí. Při snaze zvýšit počítačovou bezpečnost je třeba rozlišovat padělatele, nelegální obchodníky, nelegální poštovní zásilkové služby či domy a konečně i běžné uživatele se sklonem k nelegálnímu pořizování software. K nehmotným prostředkům počítačové bezpečnosti lze pak zařadit vlastně odstrašující funkci postihu takových pachatelů.

Na nekalou činnost padělatelů je především upřena pozornost policie, stejně jako soukromých detektivů jednotlivých firem. Jejich práce začíná v okamžiku, kdy se někde objeví krabice se softwarem, která podle vnějších znaků vzbuzuje podezření o padělku. Firmy se snaží co nejtěsněji spolupracovat s pracovníky celních úřadů, neboť ti bývají často prvními, kteří padělané výrobky zjistí. Specialisté firem se snaží poskytovat policii odborné expertízy ve věci rozpoznávání falešných produktů. Po zjištění padělků, kterých může být v dané lokalitě i velké množství, přichází na řadu represe ze strany orgánů činných v trestním řízení. Je samozřejmé, že tento postup má v každé zemi své specifické rysy v závislosti na místních legislativních úpravách. Společným rysem všude ale musí být bezprostřední zabavení veškerých objevených padělků. Následuje pak jejich prohlídka, testování a prozkoumání. Důležité je také zajištění veškeré provozní dokumentace piráta. Tito lidé si většinou vedou podrobné údaje o výrobě, případně o dalším uplatňování svých padělků. Odtud se lze dovědět kdo jsou jejich partneři, kdo se zabývá distribucí do jednotlivých zemí, komu prodávají, kdo jsou jejich zákazníci a někdy i to nejdůležitější - kdo je dodavatelem. Postih nelegálních obchodníků, zejména *řetězového prodeje* nabývá stále více na účinnosti. Firmy ve spolupráci s policií proti tomuto prodeji zasahují prakticky v celé Evropě. Týká se to i dealerů hardware, jakož i elektronických inzertních systémů a operací poštovní objednávkové služby.

V postihu nelegálního pořizování kopií v rozsáhlých sériích jsou velké softwarové firmy, jako např. Microsoft, často velmi angažovány. S řešením těchto případů mají

zkušenosti zejména ve Velké Británii, Francii, Španělsku, v Itálii a v dalších státech Evropského společenství. V zemích střední Evropy je tato zkušenost zatím značně omezená, i když daný fenomén zde existuje rovněž. Podle [98], v uvedených zemích firma Microsoft byla nucena zahájit soudní stíhání velkých podniků, které zakoupily jeden, dva nebo jen velmi malý počet originálů software a poté z nich udělali velký počet nelegálních kopií. Typický průběh takových případů spočívá zhruba v pěti etapách. Nejdříve je věnována pozornost hlášení, že v podniku se pravděpodobně ilegálně používá software firmy. Tuto zprávu nutno nejprve prověřit. Často se nejdříve jedná s informátory, kteří případ oznámí. Snahou je ověřit, jak dalece je přesná jejich informace, děje se tak nejčastěji několika nezávislými prostředky. Např. kontrolou registračních karet zasílaných uživateli výrobcům. Zde vidíme další význam registrační karty, která jinak zajišťuje legálnímu uživateli dodání nové verze nebo edici programu, až se objeví na trhu. Dále je možné též kontrolovat databázi dodavatele software a tam zjistit, zdali daná společnost skutečně zakoupila software či nikoli. Jestliže ji v seznamu nenajdeme, pomáhá to v potvrzení původního hlášení, že se pravděpodobně jedná o informaci pravdivou. V další etapě je věc předána k soudu s žádostí o povolení k prohlídce, což umožňuje firmě nebo policii prohlédnout počítače daného podniku. V různých zemích to ovšem funguje různě. Například ve Velké Británii jsou to zástupci softwarové firmy (techničtí specialisté a právníci), kteří jsou vykonavateli příkazu k prohlídce. Ve Španělsku a ve Francii je vykonavatelem příkazu k prohlídce policie. V Itálii a v Portugalsku to jsou soudem jmenovaní znalci. Po získání povolení k prohlídce, všechny počítače v podniku jsou prohledány na základě určité předem vypracované metody. Tím se zjistí, jaké programové prostředky jsou instalovány na počítačích podniku a zdali jsou legální nebo nikoliv. Zpravidla již při odchodu z podniku existuje dostatek údajů pro další následnou analýzu, včetně vyčíslení škod. Po prověření důkazů je pak zahájen soudní proces, ať již občanskoprávní nebo trestněprávní, v závislosti na charakteru případu a povaze zákonných předpisů dotyčné země.

Publicita jako nehmotný prostředek zvyšování počítačové bezpečnosti. Zásahy proti pirátům sestávají nejen z vyšetřování, z prohlídky, ze zabavení a zkoumání věcí doličných, ze soudního procesu, ale i z publicity. Publicitu nutno považovat za důležitý faktor zvyšování počítačové bezpečnosti, zejména pokud jde o prevenci počítačového pirátství. Přesto, že existuje možnost zákonného postihu, firmy daleko více spoléhají na publicitu těch případů, kdy by1 zákon porušen, protože taková publicita má větší preventivní účinek, přesněji - působí jako zastrašující prostředek. Abychom zabránili ostatním dealerům s hardwarem ve stejné činnosti, musí vejít ve známost, že zákon je zde a je důsledně prosazován. Např. podle [98], firma Microsoft pořádá ve spolupráci s policií ve Švédsku, Dánsku nebo v Holandsku, tedy v zemích patřících v tomto ohledu k velmi aktivním, speciální tiskové konference. Zde pak popisuje aktuální případy a hovoří společně s ostatními účastníky o tom, co na poli proti softwarovému pirátství nutno udělat. O jednom zátahu proti pirátům v Itálii se firmě podařilo natočit skrytou kamerou videozáznam, který byl pak velice výhodně využit v propagační kampani. Ukazoval ve zkratce

-realizaci zkušebního nákupu, jímž se potvrdilo, že dealer nabízí ilegální software,

-testování zakoupeného počítače a přibaleného software s cílem potvrdit, že nákup obsahuje ilegální software, na základě čehož bylo zahájeno trestní stíhání,

-způsob zveřejnění akce, s cílem zabránit dalším jedincům v téže nelegální činnosti.

6.3. Obecné aspekty počítačové bezpečnosti

Všechny prostředky počítačové bezpečnosti, z nichž některé jsme v předchozím uvedli, nelze jednoznačně hodnotit podle jejich významnosti. Priority při jejich výběru nutno podmínit konkrétními možnostmi podniku a ochotou vedení věnovat na tyto účely určité, často nemalé finanční náklady. Podle toho můžeme mluvit o různých *úrovních počítačové bezpečnosti*. Vždy je však důležité, aby všechna opatření, nehledě na jejich úroveň, úzce na sebe navazovala a logicky se vzájemně doplňovala. Není možné, aby byla nahodile vybrána jen některá z nich, byť by se zdálo, že nejúčinnější, pokud bychom nerespektovali vazby na další podstatné aspekty. Opatření jevící se na první pohled jako redundantní mohou být účinná jen v adekvátním kontextu s jinými způsoby zvýšení počítačové bezpečnosti. Jinak samozřejmě mohou svou účinnost skutečně ztratit.

Projekty počítačové bezpečnosti. Každá instituce, která obhospodařuje citlivá data většího rozsahu by měla ustanovit specialistu pro počítačovou bezpečnost. Jeho opodstatnění je evidentní zejména u podniků s velkou koncentrací výpočetní techniky, při práci ve větších sítích, často s nepřehlednými vazbami mezi jednotlivými účastníky, obsáhlých databázích, či při časté manipulaci s daty početným kolektivem zaměstnanců. Tento pracovník by měl nejenom dohlížet nad realizací opatření zajišťujících počítačovou bezpečnost. Měl by navíc přistupovat k systému ochrany informací tvůrčím způsobem tak, aby byl schopen ji neustále zlepšovat a interaktivně reagovat na případné její nedostatky. K tomu je zpravidla nutno zpracovat určitý *projekt počítačové bezpečnosti,* který musí přihlížet ke všem hypotetickým variantám chování systému či potenciálních narušitelů. Komplexní systém ochrany by měl vycházet z vnitřního bezpečnostního standardu instituce. Měl by přihlížet k několika kriteriím, jako je typ informací, k typu komunikace s dalšími sítěmi, k objemu a frekvenci manipulací s daty, k rozsahu kolektivu uživatelů, k jejich profesnímu charakteru, k typům možné motivace útoků, k rizikům průniku zvenčí či zevnitř atp.

Vedle někdy až přehnaného nadšení, které provází nástup počítačové éry, se občas objevují názory plné pochybností a skepse. Soudí se třeba, že zajištění elektronicky uložených důležitých dat je relativně nedokonalé a dokáže ho nabourat každý zapálený středoškolský student, že Internet je pomalý, v jeho síti není vůbec žádná bezpečnost a přenáší spíš destruktivní viry než potřebné informace. Dokonalá počítačová grafika navíc umožňuje poměrně velmi snadno falšovat nejrůznější dokumenty, razítka a dokonce i bankovky. Falza pomocí scannerů a grafických programů se skutečné dělají, což usnadňuje i to, že předlohy mnoha úředních listin byly už původně na počítačích navrhované a zopakovat podobný postup je poměrně snadné. Na druhé straně zase moderní, počítači řízené přístroje pomáhají podobné podvrhy odhalovat, čímž se klady a zápory těchto aktivit poněkud vyrovnávají. To je ostatně u technického pokroku běžné. I když se orgány činné v trestním řízení setkávají s počítači většinou z té horší stránky, rozhodně nelze říci, že situace v oblasti počítačové kriminality je kritická. Jistě, každý systém ochrany dat vymysleli a zkonstruovali lidé a lidé ho taky dokáží překonat, složitost takového úkolu ovšem už dávno přesahuje možnosti nadšeného amatéra.

Zasáhnout např. do systému nějaké banky může jenom ten, kdo ho dobře zná. Velká většina odhalených podvodů posledních let byla realizována vlastními pracovníky příslušných institucí. Peněžní ústavy na základě toho také upravují preventivní bezpečnostní strategii, vedle technických zábran jde hlavně o politiku v oblasti personální práce. Dnes patří ke světovému trendu pečlivá příprava a výchova svých vlastních spolehlivých zaměstnanců.

**

Klasifikace informací je nezbytná pro vybudování jejich účelné komplexní ochrany. Klasifikaci informací lze řadit podle obsahu k pomocným nástrojům informační bezpečnosti, podle forem pak přímo k principům počítačové bezpečnostní politiky. Klasifikované informace jsou informace označené tak, aby jedincům, kteří s nimi přicházejí do styku, bylo zřejmé, že tyto informace mají určitý stupeň citlivosti, přičemž je nutné vhodným způsobem s nimi zacházet, např. ve smyslu jejich ochrany proti zneužití. Klasifikace informací má význam jak pro organizaci samu, tak i pro vnější subjekty, které přicházejí s danou organizací do styku. Pokud neexistuje v příslušném systému klasifikace informací a zpracovávané nebo vyměňované informace nejsou vhodným způsobem označeny, nemůže být s nimi potom zacházeno jako s informacemi adekvátně chráněnými.

Důsledky absence klasifikace informací. Vedoucí pracovníci, kteří si dostatečně neuvědomují význam klasifikace informací a nezajistí její zavedení, jsou potom často překvapeni zjištěným únikem vysoce citlivých informací. Autoři [74] popisují kauzu, ke které došlo na půdě našeho parlamentu. Návrh zákona, který byl připraven pro konečné hlasování, existoval ve dvou podobách, listinné (byla uložena v trezoru) a elektronické (na paměťovém médiu počítače). Pro jednání parlamentu byla vytištěna elektronická verze. Ačkoliv se při ukládání obě formy nelišily, předkládaný návrh se lišil od oficiálně připravené a odsouhlasené verze návrhu v několika částech, které se týkaly finančního vyrovnávání bývalých zaměstnanců Ministerstva vnitra. Nebýt pečlivosti a odpovědnosti jistého právníka, byl by pravděpodobně schválen zákon s onou úmyslně provedenou úpravou. Došlo k tomu tak, že obsluha počítače neoprávněně změnila elektronickou formu návrhu zákona. Je to ukázkový případ porušení několika zásad bezpečnostní politiky, ke kterému by v žádném případě nemělo na této úrovni dojít. Operátor počítače zřejmě nebyl dostatečně prověřen, nebyla uplatněna zásada oddělení povinností (operátor neměl mít možnost zasahovat do zpracování tímto způsobem), a což nás právě nyní nejvíce zajímá, nebyla zjevně provedena a implementována klasifikace informací. S daným dokumentem při zpracování na počítači nebylo pak zacházeno na úrovni odpovídající jeho citlivosti.

Úrovně citlivosti. Způsob, jakým jsou informace v jednotlivých organizacích chráněny, se liší případ od případu, může být dokonce různý ve správních jednotkách jednoho a téhož podniku. Úroveň ochrany by však měla být jednotná. Ochrana informací by také měla být vždy přiměřená, praktická a cenově odpovídající možným rizikům. Klasifikace informací vždy předpokládá jejich rozdělení do několika úrovní. Do nejvyšší úrovně bývají zahrnovány informace, které mají vztah k národní bezpečnosti. I když terminologie není jednotná, tyto úrovně jsou obvykle označeny jako *„přísně tajné“* a *„tajné“*. Podle studie [74], např. v USA

tyto úrovně společně s další skupinou *„důvěrné“* bývají též souhrnně označovány jako *„klasifikované“*. Druhá skupina, *„neklasifikované“*, označuje informace nižší úrovně citlivosti, které se týkají např. osobních informací, a jimž je věnována ve světě již delší dobu rovněž zvýšená pozornost.

Příklad klasifikace informací. Jak uvádí [74], organizace může k popsání různých úrovní citlivosti použít svou vlastní terminologii a přizpůsobit ji činnosti v závislosti na potenciálních škodách plynoucích z neautorizovaného prozrazení informací. Jestliže však bude sdílet citlivé informace s jinými organizacemi, je třeba předem navzájem dohodnout společnou terminologii, aby citlivost byla posuzována jednotně. Proto byla britskou vládou doporučena pro průmyslové a obchodní organizace třístupňová klasifikace, rozlišující

-informace, jejichž neautorizované odhalení, zejména mimo organizaci, by bylo nevhodné a nevyhovující; jde většinou o běžné informace, které si organizace nepřeje zveřejnit; takto klasifikovaná informace nemusí být označena; do této kategorie spadá většina informací;

-informace, jejichž neautorizované odhalení, dokonce i uvnitř provozní jednotky, může významným způsobem poškodit zájmy organizace; tyto informace zahrnují např. podklady pro různá obchodní vyjednávání, hodnocení konkurenčních vztahů na trhu, osobní informace, informace o zákaznících, informace označené takto vládou apod.; informace s touto úrovní citlivosti by měly být vždy příslušným způsobem označeny, a to i při běžné komunikaci;

-informace, jejichž neautorizované odhalení i uvnitř organizace by jí způsobilo závažné ztráty nebo značně poškodilo její zájmy; jde o poškození vlivem vážných finančních ztrát, závažnou ztrátou příležitosti k zisku, vlivem závažného poškození nebo ztrátou pověsti apod.; tyto informace zahrnují např. detaily týkající se převzetí jiné organizace, uzavření nebo utlumení činnosti některé části organizace, spojení s jinou organizací, globální obchodní strategie, obchodních plánů, velmi citlivého ohodnocení obchodních partnerů, dodavatelů, konkurentů, tajné informace týkající se patentů, nových výrobků, informace takto označené vládou atd.; informace s touto úrovní citlivosti by měly být vždy příslušným způsobem označeny, a to i při povolené komunikaci.

Některé obecné zásady klasifikace informací. Pokud je doporučeno označení, mělo by být realizováno, ať již se tyto citlivé informace nalézají na papíru, disketě, disku, pásce, fólii pro prezentaci, mikrofiši, fotografii nebo jakémkoliv jiném médiu. Organizace nemusí mít implementovány všechny tři úrovně citlivosti, může např. dojít k závěru, že žádná informace uvnitř organizace nespadá do úrovně třetí nejvyšší citlivosti, takže stačí implementovat pouze první dvě úrovně. V takovém případě musí upozornit své partnery, že není schopna korektně pracovat s informacemi na úrovni třetí, protože by s nimi zacházela jako s informacemi citlivosti o stupeň nižší. Organizace může samozřejmě implementovat i větší počet úrovní citlivosti nebo je stanovit tak, že nebudou přesně odpovídat uvedeným úrovním. Spadá-li však informace mezi dvě stanovené úrovně, musí být označena úrovní nejblíže vyšší. Podobně také citlivá informace převzatá od jiné organizace by neměla být označena nižším stupněm citlivosti. Bezpečné sdílení citlivých informací je důležité v případech vytváření nebo fungování rizikových vztahů, uzavírání smluv na subdodávky, kde se předpokládá zacházení s

citlivými informacemi, nebo je-li partnerem vládní organizace. Některé informace jsou citlivé jen po určité časové období. V takovém případě by jejich označení mělo být indikováno kalendářními údaji, případně určitými časovými skutečnostmi, zabezpečujícími odeznění či změnu citlivosti po určitém časovém horizontu. Podle studie [74], např. zápis z jednání bankovní rady centrální banky o případném uvalení nucené správy na určitou komerční banku bude jistě považován za citlivou nebo vysoce citlivou informaci; po rozhodnutí a jeho zveřejnění pominou důvody pro zachování důvěrnosti zápisu.

Systémové prostředky zpracování citlivých informací. Citlivé informace na druhé a třetí nejvyšší úrovni citlivosti by měly být zpracovávány na dostatečně bezpečných systémech. Výpočetní systém by měl mít zabudovány takové kontroly, které omezí přístup pouze na autorizované osoby, ukládá informace způsobem, jenž zabrání jejich náhodnému nebo úmyslnému kompromitování. Dále pak chrání informace při zpracování a přenosu před náhodným nebo úmyslným útokem, snižuje pravděpodobnost možné rekonstrukce dat po jejich vymazání nebo zničení. Pokud jde o jistotu nebo záruku, že daný systém opravdu splňuje tyto bezpečnostní požadavky, nutno brát v úvahu i provozní zkušenosti. Praxe ukázala, že teprve nezávislé hodnocení bezpečnostního produktu podle určitých kritérií a jeho certifikace dávají uživateli produktu jistou záruku, že produkt nemá zásadní slabá místa, kterých by mohlo být zneužito. V současné době již existují nástroje umožňující identifikaci nezávisle testovaných a hodnocených produktů pro počítačovou bezpečnost.

Modely klasifikace v bezpečných informačních systémech. První práce, zaměřující se na úroveň jistoty či na míru záruky u bezpečných informačních systémů, byly započaty za spoluúčasti Ministerstva obrany USA. Toto ministerstvo mělo eminentní zájem na vývoji systémů, které by garantovaly bezpečné zpracování klasifikovaných dat. Mělo i značné zkušenosti v ochraně důvěrných dokumentů, vlastnilo sofistikovaný systém klasifikace bezpečnostních úrovní dokumentů a lidí a mělo dostatečné zdroje na financování vývojových projektů. Prioritním cílem bylo vyvíjení modelů bezpečných systémů s cílem zabránit neautorizovanému odhalení klasifikovaných informací. Výsledkem prací byl *Bell-La Padulův model*, na který navázal vývoj formální bezpečnostní politiky, založené na tomto modelu, dále pak vytvoření počítačového systému, který tuto politiku implementoval, a rigorózní důkaz, že software a hardware tuto politiku skutečně implementoval. V USA v roce 1983 vyšel soubor návodů pro výrobce systémů a systém hodnocení důvěryhodných výpočetních systémů, známý jako *„Oranžová kniha“*. Tato kritéria začala být koncem 80. let využívána také komerčními i vládními organizacemi v USA i v Evropě, které se začaly zvýšenou měrou zabývat bezpečností počítačů. Postupně však vyvstala otázka, zda *Bell-LaPadulův model* je vhodný pro aplikace i mimo vojenský sektor. *Clark-Wilsonův* model z roku 1987, představuje model informační bezpečnosti, který se spíše než na zajištění důvěrnosti klasifikovaných informací zaměřil na zajištění toho, že finanční transakce jsou uskutečňovány v souladu se specifikovanou politikou organizace, tj. byl zaměřen hlavně na integritu. Studie [74] uvádí ještě *„Model čínské zdi“* z roku 1989, který popisuje bezpečnostní politiku určenou pro právní a konzultační firmy, kde prioritním hlediskem je důvěrnost dat. Situace u nás je podle [74] mírně řečeno neutěšená. I když máme zákony, které se zabývají klasifikací informací na

národní úrovni a ochranou informací daných tříd utajení, při počítačovém zpracování, ať už na vládní úrovni nebo na úrovni velkých průmyslových, finančních nebo obchodních organizací, není klasifikace informací důsledně implementována. Dochází k tomu, že informační technologie, kterými jsou tyto úřady nebo organizace vybavovány, neposkytují formální záruky určité úrovně bezpečnosti, která umožňuje zpracování citlivých informací. Při zpracování není bezpečnost informací komplexně zajištěna. To se týká i výměny a přístupu k citlivým informacím ze strany obchodních partnerů a dodavatelů. Odpovědnost za tento stav má jednoznačně management. Otázkou je, zda při našem vstupu do NATO nebo EU budou tyto organizace ochotny tento stav tolerovat nebo nás donutí uvést celou tuto oblast do pořádku.

**

Pro účely specializované výuky jsou v práci [102] uvedeny metody ochrany výpočetní techniky, tedy postupy počítačové bezpečnosti z hlediska jejích nejdůležitějších prvků. Říká se zde, že v západních zemích rozvoj výpočetní techniky umožnil vzniku mnoha forem nedovolené činnosti směřující k dispozici s v výpočetní technikou. Podle [102] snad nejméně nebezpečný je tzv. *hacking*, tedy pronikání k informacím bez úmyslu nějak škodit. Jde vlastně o hnutí zájemců o tento „obor“, které má dokonce vlastní časopisy a organizaci. Trestní odpovědnost *průnikářů* je problematická zejména s přihlédnutím k míře nedovolenosti jejich jednání a způsobenému následku. Na trhu se dokonce objevují návody, jak vnikat do počítačových systémů. Tito průnikáři mohou být potenciálně skutečně velkou hrozbou pro počítačové systémy soukromých firem i veřejnoprávních institucí pracujících s citlivými informacemi. Amatérští průnikáři mají nejen odborné znalosti, ale jsou mnohdy vybaveni i poměrně dokonalou technikou. Nejméně nebezpeční jsou z tohoto hlediska tzv. *„rodents“*, pro něž je průnik hrou, další skupina potenciálně nebezpečných je označována *„hackers“*. Nejnebezpečnější jsou *„crackers“*, kteří jsou schopni užívat čísel cizích kreditních karet a vniknout do systému bankovních kreditů s cílem získat majetkový prospěch. Samostatný problém pak činí *počítačové pirátství*. Rozborem originálního programu a jeho částečným vylepšením v dílčí části vzniká zdánlivě nový program, který je pak za úplatu dále rozšiřován. Toto pronikaní do programu se děje bez souhlasu autora. Tím dochází k poškozování práv autora a někdy též ke vzniku nekvalitních programů, které mohou být zdrojem havarií počítačových systémů či sídlem virů.

Nejzávažnějším problémem jsou v současné době *počítačové viry*. Jde o programy, které mohou infikovat ostatní tak, že do napadeného programu zapisují svoji kopii, přičemž tato si ponechává možnost dalšího množení. Při infikování se může počítačový vir šířit od jednoho programu ke druhému. To je velmi nebezpečné. Nakažené programy se pak mohu rozšiřovat prostřednictvím disket; popř. též pomocí počítačových sítí. Autoři [102] považují počítačové viry za nejbrutálnější formu počítačového vandalismu. První případy masového nakažení byly zjištěny již v roce 1987. Virus *Lehigh* (USA) označovaný podle místa výskytu zničil na univerzitě množství dat uložených na disketách. Za nejnebezpečnější typ viru je považován tzv. *trojský kůň*. Připomeňme, že jsou to programy, které mají v sobě zabudovánu

určitou skrytou část, která je aktivována po splnění nějaké podmínky. Tato skrytá část pak vykonává činnost destruktivního charakteru, zejména modifikaci dat a výmaz souborů.

V práci [102] se rozlišují *dva systémy ochrany výpočetní techniky*, klasický a moderní. *Klasický způsob* je nejběžněji využívaný. Jeho podstatou je identifikace uživatele jako oprávněné osoby. Nejčastěji se jedná o identifikaci podle hesla. V současnosti se však ve světě využívá i identifikace podle dynamiky podpisu uživatele nebo tzv. identifikační karty. V úvahu přichází i kombinace obou způsobů. *Moderní metody* dovolují ověřování oprávněné osoby pomocí otisků prstů či snímků sítnice očí. Tento ochranný systém je dokonalejší a zpravidla bývá užíván u systémů zvláštní důležitosti pro stát. Často jsou také v těchto případech používány kryptografické protokoly. Význam slova *protokol* kromě jiného spočívá obvykle v popisu způsobu umístění a uspořádání účastníků nějaké mezinárodní (diplomatické) konference, a to včetně pořadí jednotlivých vystoupení, případně dalších náležitostí, oblečení, stolování apod. Občas bývají jednání o protokolu takovéto akce delší než akce sama. *Kryptografický protokol* je pak algoritmus, přesněji specifikovaný sled operací a výměny dat, určený pro komunikaci mezi různými stranami a využívající kryptografické transformace. Téměř neřešitelným problémem je však absolutní zabezpečení ochrany přenosu informací mezi počítačovými systémy. Při používání běžných telefonních linek nelze vyloučit odposlech. Jednou z možností ochrany přenosu dat je jejich zašifrování. Počítačová bezpečnost *Computer Security* zahrnuje ochranu výpočetní techniky i programového vybavení. Z hlediska institucionálního představuje systém státních i soukromých institucí zabývajících se vývojem či prodejem, jakož i instalací ochranných systémů. K ochraně dat jsou vytvářeny i určité institucionální předpoklady. V roce 1990 Evropské společenství zahájilo nový program, který se jmenuje *INFOSEC*, tzv. ochrana informací. Jeho cílem je posílení vědomí o důležitosti ochrany informací. Jde v podstatě o dosažení předpokladů pro snížení míry zranitelnosti počítačových systémů před úmyslnými i nedbalostními útoky na informace. K tomu jsou využívány různé systémy ochrany s návazností na speciální testovací metody, umožňující prověřit účinnost ochrany systémů. Snad nejzdařilejším pokusem je v tomto směru metoda *SBA* vytvořená ve Švédsku. Její pomocí lze zjistit úmyslné i neúmyslné zásahy do informačního systému a zpravidla je i přesně identifikovat. U nás není dosud počítačové bezpečnosti věnována dostatečná pozornost.

Ochrana dat a informační právo. V zahraničí jsou známy pokusy o shrnutí problematiky ochrany dat do nové právní disciplíny, která je označována jako *informační právo*. Pro nově se formující obor práva je charakteristická jeho mezinárodní povaha. Informační systémy nabývají stále více mezinárodního charakteru. Proto je nezbytné vytvářet i kompatibilní právní systémy, resp. právní normy poskytující ochranu informacím s přihlédnutím k potřebám mezinárodní ochrany. První zákony na ochranu výpočetní techniky byly přijaty v 70. letech v USA. Zkušenosti ukazují, že zákonodárná úprava podléhá časovým vlivům a je třeba ji velmi často doplňovat v návaznosti na vývoj počítačové techniky a poznatky právní praxe. V posledních letech dospívá právní vývoj ve světě k tomu, že nedotknutelnost osobních dat začíná být pokládána za jedno z důležitých občanských práv, jehož ochrana je úkolem též ústavního práva. V některých západních zemích byly přijaty již dříve speciální legislativní úpravy ochrany osobních dat. Např. francouzský trestní zákon

s účinností od roku 1994 zahrnuje oddíl *„O porušení osobních práv vyplývajících z užití kartoték nebo automatizovaných informačních systémů“*. V souvislosti s akceptováním *Ústavní listiny práv občana* došlo i u nás k zabezpečení ochrany občanských práv na základě zákona o ochraně osobních údajů v informačních systémech, viz [250].

**

Počítačová bezpečnost, bezpečnost informačních systémů a obchodní tajemství. Jak známo, bezpečnost informačního systému a ochrana nejrůznějších firemních tajemství, včetně obchodního, je v dnešní době velice významná, a to především z praktického hlediska. Jak uvádí autor studie [165], tuto bezpečnost a ochranu pak dělíme na *fyzickou, režimovou, bezpečnost pracovníků, bezpečnost technických prostředků, bezpečnost programových prostředků, bezpečnost dat, bezpečnost komunikačních cest.* Na základě důkladného rozboru bylo zjištěno, že právě poslední oblast - bezpečnost komunikačních cest - je jednou z nejzranitelnějších oblastí v celém systému ochrany informačního systému a je zároveň bohužel i dost podceňována. Mnozí, kteří se zabývají bezpečnostními systémy a ochranou informací, se zaměřují především na hardwarovou a softwarovou ochranu, ale zapomínají na to, že nejvíce používaným prostředkem komunikace mezi lidmi i subjekty není jen počítač, ale obyčejný telefon. Vždyť i většina internetových toků informací se děje po telefonu. Všichni známe kvalitu naší telefonní sítě a rovněž i to, že napojení se do cizího telefonního hovoru je zcela běžné a není třeba zdůrazňovat, co se stane s naší informací, která je určena úplně jinému příjemci, adresátovi. Takže, získat i cílevědomě tímto způsobem informace není nic obtížného. Druhým nejpoužívanějším prostředkem v běžném styku je fax. A zde nám opět může uniknout řada skutečností, souvisících s chráněním informací, protože naše faxová zpráva může najít úplně jiného adresáta, než bychom si přáli.

Hovoříme-li o počítačové bezpečnosti, měli bychom mít na zřeteli *informační bezpečnost* jako takovou, včetně bezpečnosti přenosu dat. Řada opatření týkající se této specializace je použitelná i na užší pojetí bezpečnosti počítačové. Dokonce lze říci, počítačová bezpečnost je v určitých systémech vlastně podmíněna bezpečností informační, zvláště pak bezpečností přenosu dat. Proto se např. bezpečnostní agentura *MATT* zabývá ochranou telefonní sítě. Pomocí technických zařízení zabezpečuje kódování přenosu, čímž znesnadňuje zneužívání telefonních hovorů. Agentura pro tento účel zřídila speciální útvary, které „hardwarově“ i „softwarově“ zabezpečují pomocí speciálních produktů nejrůznější typy přenosu dat, dokonce včetně bezpečnostních schránek pro fyzický převoz peněz či jiných důležitých dokumentů. Pomocí různých přenosných i stacionárních kódovacích zařízení, které zároveň monitorují i stav telefonních linek, je možno zjistit připojení cizího účastníka. Totéž lze zabezpečit i při přenosu zpráv faxem. Všechna technická zařízení jsou určena pro ochranu komerčních zájmů dle zákona při přenosu dat, především pak zájmů obchodníků pro ochranu jejich obchodního tajemství. Provozovatelům informačních systémů je navíc podle zákona, viz [250], ukládána ochrana osobních dat. Právní vědomí našich občanů v této oblasti je stále ještě poměrně slabé. Je proto žádoucí přispívat ke zvyšování bezpečnosti informací nejen nabídkou poradenství, projektových služeb a technických prostředků, ale i ke zkvalitňování celkové kulturní a morální úrovně v nazírání na tento problém.

**

Počítačová bezpečnost a organizovaný zločin. Opatření ke zlepšení počítačové, obecně informační bezpečnosti mohou do jisté míry sloužit též ke ztížení aktivit charakterizovaných jako organizovaný zločin. Jak uvádí studie [28], doménou, v níž se asi organizovaný zločin v oblasti počítačové kriminality nejvíce uplatňuje, je zneužití dat. To působí nejen značné ztráty finančním institucím při nezákonných převodech, ale může to narušit i chod těchto institucí. Tím, že je otevírá pro zneužití organizovanými zločineckými skupinami. Pokud jde o porušování autorských práv v oblasti tvorby počítačových systémů, lze se domnívat, že zpřísněná kontrola odstraní do značné míry především laické nelegální aktivity, z nichž organizovaný zločin nemůže příliš profitovat. Zostřené represe a opatření zvyšující počítačovou bezpečnost v tomto směru by však paradoxně mohly vést k tomu, že vzhledem k obtížnější dostupnosti programů zmohutní organizované pirátství, které by pak přinášelo nezanedbatelný nárůst nekalých zisků. To by mohlo napomáhat k rozvoji dalších aktivit organizovaného zločinu, přesahujících rámec klasické počítačové, respektive informační kriminality. Proto adekvátní opatření ke zvyšování počítačové bezpečnosti tvorby systémů, přenosu dat, jejich počítačové systemizace, analýzy či jiného zpracování, nutno považovat za velmi důležitá i z hlediska boje s organizovaným zločinem.

Organizované nelegální aktivity. V práci [102] se vyjmenovávají aktivity spojené s organizovaným zločinem, který je páchán v souvislosti s výpočetní technikou. Jde o formy páchání trestné činnosti, zaručující organizovaným pachatelům naději na úspěch a hlavně na větší zisk. Patří k nim

-ilegální výroba počítačové techniky *(hardware)*, porušující cizí patentová a průmyslová práva,

-ilegální kopírování programů *(software)*, porušující autorská práva,

-neoprávněné užívání práce počítačů *(krádeže strojového času)*,

-ničení a poškozování počítačů, programů a dat *(počítačové sabotáže, počítačové viry)*,

-neoprávněné získávání informací z databází, včetně podkladů pro finanční machinace,

-vkládání lživých dat do databází *(inputmanipulation)*,

-měnění výsledků počítačového zpracování dat *(outputmanipulation)*,

-měnění programů *(programmanipulation)*.

Tyto aktivity jsou pro organizované gangy většinou jen jedním z prostředků dosahování nekalých cílů, zejména pak cílů zištných, ale i prostředkem realizace informačního terorismu atp.

**

Počítačová bezpečnost z hlediska analýzy rizik. Jak uvádějí autoři [72], jediným důvodem, proč všechny počítače na světě dosud nezhavarovaly ve stejnou chvíli je, že nejsou ještě všechny navzájem propojeny. Každý člověk se pravděpodobně určitou formou analýzy rizik ve svém životě již zabýval - při pojišťování domácnosti odhadujeme pravděpodobnost návštěvy zloděje, výši škody, která nám může vzniknout, a tedy částku, na kterou byt pojistíme; pro sníženi rizika např. přidáme na vstupní dveře do bytu dokonalejší zámek nebo si necháme nainstalovat poplašné zařízení. Rychlé zavedení informačních technologií do denní činnosti organizací s sebou přineslo i nové druhy rizik, kterých si vedení organizace

obvykle není vědomo; neuvědomuje si ani svou odpovědnost v tomto směru. Problémy obvykle začne řešit až ve chvíli, kdy dojde k prvnímu případu a následným ztrátám. Teprve potom jsou zkoumány příčiny události a přijímána rozhodnutí, jak se v budoucnu takovým problémům vyhnout. Řešením je *analýza rizik*; což v praxi znamená rozhodování o její realizaci, jak, kým a jakou formou. Vše se zřetelem na její spolehlivost a účinnost. Cílem analýzy rizik je nalezení optimálního poměru mezi možnými ztrátami a náklady vynaloženými na bezpečnostní opatření, která by tyto ztráty měla omezit. Analýza rizik se proto nezabývá čistě jen samotnou analýzou, jak by z názvu mohlo vyplývat, ale zahrnuje několik souvisejících činností. Jde zejména o stanovení, případně odhad rizik, vlastní analýzu rizik, řízení a kontrolu rizik.

Určení či odhad rizika závisí podle [72] na možných hrozbách a zranitelnostech systému. Nalezení všech potenciálních hrozeb a určení typu a účinnosti protiopatření není snadný úkol, protože zde hraje roli mnoho faktorů. Jiné hrozby jsou prioritní např. pro vládní organizace, jiné pro školy nebo nemocnice. Řada hrozeb je naopak charakteristická pro všechny organizace, nezávisle na typu jejich činnosti; tyto hrozby lze rozdělit do skupin na

-vnější vlivy, jako zatopení vodou (včetně vody unikající z rozvodů), následky vichřic (např. padající předměty), požár (včetně blesku), zemětřesení apod.; některé z těchto vlivů mohou mít i motivaci kriminálního charakteru, což nás zajímá zejména ve spojitosti se zranitelností počítačových systémů;

-vlivy způsobené chybnou funkcí infrastruktury, jako např. výpadky v dodávce elektrické energie, poruchami telekomunikace, veřejnou dopravou; vytápěním nebo klimatizací apod.; rovněž zde může jít o zločinné aktivity;

-poruchy hardware, software a dat, komunikačního zařízení, počítačových sítí, počítačů, vstupního a výstupního zařízení;

-faktory způsobené neúmyslnými lidskými chybami uživatelů, operátorů obsluhy, případně nedbalostí ostatního personálu;

-vlivy způsobené zneužitím a kriminálními činy realizovanými

-z vnějšího prostředí hackery, zavirováním, vloupáním, žhářstvím, sabotážemi, krádežemi výpočetní techniky apod.;

-zevnitř organizace krádežemi nebo zničením hardware, software či dat, žhářstvím, stávkou, využíváním vybavení organizace pro soukromé účely apod.

Kromě určení potenciálních hrozeb je nutné také určit nebo odhadnout četnost nebo pravděpodobnost uskutečnění dané hrozby. Např. stávka železničářů může mít pro některou organizaci poměrné značné následky, ale četnost jejího výskytu nebyla až dosud v naší zemi příliš vysoká. Pravděpodobnost, že dojde k zemětřesení, je v naší republice velice nízká. Z hlediska našich cílů nás však zajímají jen ta bezpečnostní opatření, která čelí počítačové kriminalitě. Jakmile jsou určeny hrozby a jejich možná četnost, resp. pravděpodobnost, je nutno stanovit a posoudit vhodná protiopatření, která by měla tyto hrozby zcela nebo částečně eliminovat.

Omezování rizik. Ne vždy je potřebné a účelné omezit rizika úplně. Každé opatření něco stojí a náklady je třeba posoudit též vůči možným ztrátám. Jestliže náklady na protiopatření dosahují výše možných ztrát, nebo je dokonce převyšují, je výhodnější dané riziko akceptovat. Podle [72] protiopatřením nemusí být riziko zcela potlačeno, ale spíše omezeno na úroveň, která je již přijatelná. V případě, že existuje mnoho možných způsobů, jak určité riziko potlačit, je výhodnější volit řešení s lepší návratností investic. Někdy však nutno rizika zcela vyloučit, a to bez ohledu na náklady. Např. pro banku je určitě nepřijatelná situace, kdy nemá zaručenu integritu svých peněžních transakcí, bez ohledu na jejich výši. Rozhodnutí, která rizika jsou přijatelná a která je nutno omezit a do jaké míry, musí učinit vedení organizace. Samotné rozhodnutí je ale pouze jedním z kroků, za kterým by měly následovat další. Je třeba určit konkrétní odpovědnosti uvnitř organizace za implementaci přijatých protiopatření, stanovit způsob jejich implementace a konkrétní časové termíny implementace.

Charakter procesu analýzy rizik podle [72]. Proces analýzy a řízení rizik není a nemůže být statický. Nové technologie přinášejí nová rizika a stará mohou odstranit. Uvažuje-li např. organizace o připojení své lokální sítě na Internet, bude asi jedním z prvních kroků důkladná analýza rizik. Některá protiopatření mohou být neefektivní, neúčinná nebo časem přestanou být nezbytná. Proto je třeba realizovaná řešení pravidelně hodnotit a revidovat, tj. proces analýzy rizik pravidelně v určitém intervalu opakovat. V USA je dokonce analýza rizik povinná pro všechny vládní organizace. Metodologie analýzy je zde upravena speciálním standardem, který se stal základem většiny moderních kvantitativních metodologií. Východiskem při rozhodování je kvantitativní odhad možných ztrát s přiřazením určitého faktoru dle výše ztrát, a odhad pravděpodobnosti, že ke ztrátě dojde. Z nich se potom odvozuje očekávaná roční ztráta, která organizaci hrozí, pokud nepřijme žádná protiopatření. Analýzy a řízení rizik na vládni úrovni se také týká rozhodnutí prezidenta USA z roku 1994.

Nástroje analýzy rizik. Pro zefektivnění a zjednodušení procesu analýzy a řízení rizik byly vyvinuty různé softwarové nástroje. Jak uvádí [72], nejznámějšími jsou *CRAMM, RISCWATCH, MARION, ANALYZ, COBRA, SARA.* Většina těchto programů je zaměřena na určitou oblast činnosti a tedy i na specifická rizika této činnosti. Např. systém *MARION* je zaměřen na oblast pojišťovnictví, *COBRA* vychází z potřeb finančních institucí, *CRAMM* pochází z vládního sektoru. Hlavním přínosem software nástrojů je snadné zaznamenávání informací do databází, pohodlný přístup k datům a rychlá manipulace se zpracovávanými daty. Uživatel může sledovat vliv různých kombinací bezpečnostních opatření na případné ztráty a optimalizovat výběr adekvátního řešení. Např. metodologie *CRAMM* dělí úkoly analýzy rizik do tří etap:

1.etapa zahrnuje identifikace fyzických, softwarových a datových aktiv, odhady hodnoty těchto aktiv podle možných ztrát a navíc výběr aktiv nejdůležitějších;

2.etapa spočívá ve sloučení aktiv do skupin, stanovení hrozeb vůči těmto skupinám, v odhadech zranitelností a stanovení úrovně požadavků na bezpečnost pro jednotlivé skupiny;

3.etapa se týká vypracování programu protiopatření k ochraně vybraných aktiv s danou úrovní bezpečnosti, dále pak porovnání s existujícím programem protiopatření, realizace

úprav a změn a konečně se zabývá též analýzou hodnoty aktiv i samotných nákladů na protiopatření.

O tom, že podceňováni analýzy rizik se nevyplácí, se můžeme pravidelně dočíst v agenturních zprávách z celého světa. Podle [72], v roce 1998 byl např. napaden *WWW* server Ministerstva spravedlnosti USA. Hackeři doplnili domovskou stránku ministerstva protivládními útoky, hákovým křížem, pornoobrázky a dalšími „vylepšeními". Mluvčí ministerstva sdělil, že se nepodařilo zjistit, kdo útok provedl, ani jakým způsobem byl útok realizován. Využití nové technologie *WWW* serveru s sebou přineslo nové možnosti zranitelnosti a hrozeb, které nebyly předmětem dostatečné analýzy. V tomto případě šlo pouze o neoprávněnou změnu veřejných informací. Mnohem vážnější důsledky může mít již zmíněná neoprávněná úprava textu návrhu zákona předkládaného ke schválení. Ve známém filmu *Síť* byl úmyslně modifikován lékařský záznam jednoho z vysoce postavených činitelů ministerstva obrany. Negativní výsledek testu na AIDS byl změněn na pozitivní. Tento člověk kvůli výsledku testu spáchal sebevraždu. *„Jde jen o filmovou fikci nebo je tato hrozba reálná?"*, ptají se autoři studie [72].

K podcenění významu analýzy rizik. Analýza rizik je jedním ze základních prvků bezpečnosti informačních technologií a měla by být povinně realizována každou organizací pracující s citlivými informacemi. S analýzou rizik úzce souvisejí další oblasti bezpečnosti informačních technologií, jako jsou havarijní plány a plánování obnovy činnosti. Je zarážející, že některé tuzemské firmy nabízející služby, včetně školení specialistů v oblasti bezpečnosti informačních technologií nevěnovaly dostatečnou pozornost již překladu samotného termínu a používají zásadně nesprávný překlad - *riziková analýza,* který má z jazykového hlediska zcela jiný význam. Situace v tomto směru je analogická významovému rozdílu v kriminologické statistice používaných termínů *analýza kriminogenních faktorů* a *faktorová analýza* kriminogenních faktorů, viz např. [138]. Druhý z uvedených termínů označuje konkrétní (multivariační matematicko-statistickou) metodu, použitelnou též v jiných oborech, např. v psychologii. Tento nástroj může, ale také nemusí být použitelný v kriminologii jako jeden z mnoha dalších přístupů k předmětné analýze příčin kriminality, tedy k analýze konkrétních faktorů zločinnosti, což odpovídá pojetí podle prvního z uvedených termínů.

**

Informační soukromí v praxi. Soukromé informace jsou informace, které nechceme sdílet s jinými, nebo u kterých chceme osobně kontrolovat jejich pohyb, tzn. sdílíme je s někým, ale ne s „ostatními". Jak uvádí autor studie [119], rozhodujícím ukazatelem úrovně ochrany je cena osobních dat na černém či šedém trhu. Jako příklad volí autor [119] cenu zdravotních dat v Anglii a v kanadské provincii Quebec. Podle specialistů by zde faktická cena měla být výrazně nad uvedenou reálnou úrovní. Pokud je cena velmi nízká, je nevýznamnou položkou nákladů pojišťovacích firem, které tak mají jednodušší rozhodování o tom, jak vysoké splátky pojistného nasadit tomu či onomu jedinci. Cenu osobních dat a tím i úroveň ochrany ovlivňuje

-výše trestu těm, kdo data jiných řádně neohlídali a spolupodíleli se tak na jejich úniku,

-výše trestu těm, kdo s nimi neoprávněně manipulují,

-úroveň ochranných mechanismů.

Podle [119] zásadními problémy či přímo nedostatky aktuální právní úpravy ochrany osobních dat v informačních systémech u nás jsou

-široká formulace pojmu osobní údaje, která nepřímo způsobuje „znehodnocení“ skutečně důležitých dat,

-široká formulace pojmu informační systém,

-nejasná sankční opatření,

-nespecifikované pojmy „osobnost“, „soukromí“,

-neexistence úřadu pro registraci systémů s osobními údaji, pro kontrolu dodržování zákonné úpravy apod.,

-neetické snahy o přiřčení této pravomoci státnímu úřadu, navíc úřadu, který by měl být nositelem řízení *Státního informačního systému* a největším provozovatelem a uživatelem systémů s osobními daty v celé zemi.

Aktuální problémy ochrany osobních dat. Díky současnému charakteru společenských vztahů, nerozhodnosti odpovědných orgánů a snaze některých podnikatelů mnohdy protiprávně zasahovat do soukromí zaměstnanců, často nevíme, které osobní údaje můžeme sdílet s jinými a jakou hodnotu mají naše osobní informace pro stát i mnohé firmy, či jaká škoda nám může vzniknout jejich únikem mimo naši kontrolu. Pro zajímavost, podle [119], v Anglii je ke svým osobním datům a zacházení s nimi necelých 20% občanů totálně lhostejných, stejný počet velmi obezřetných až paranoidních a okolo 60% je ochotno část svých práv nechat omezit za „přiměřenou úhradu“ - finanční, věcnou či nejčastěji v podobě výrazného zlepšení služeb. To konkrétně znamená

-*„ano“* částečnému omezení práv, když finanční informace budou dostupné komukoliv v rámci banky - za možnost skutečně rychlého a nekomplikovaného obsloužení ve kterékoliv pobočce nebo bankomatu;

-*„ne“* výraznému omezení práv zavedením jednotného občanského záznamu ve státním informačním systému, kde navíc za pravdivost a úplnost informací zodpovídá občan(!).

Poučení pro prevenci zneužívání osobních údajů. Vzhledem k rozsahu a možným přehmatům státního aparátu v podmínkách současného společenského klimatu, lze do jisté míry zpochybnit ujišťování o zárukách ochrany dat. Podle [119], hlavním zájmem by mělo být zachování práva občana na ochranu osobních dat, která lze poskytovat jen v nutných případech, zákonem stanovených. Pokud občan plní základní povinnosti, neporušuje zákon a platí daně, a nežádá od státu žádné zvláštní služby, má právo jako plnohodnotný partner, tedy jako právní strana, kontrolovat pohyb informací o sobě. Pro našeho občana odtud plyne určité *ponaučení*. Každý by měl

-dávat své osobní informace jen pro jasně stanovené účely a jasně definovaným subjektům,

-dávat je jen tehdy, pokud je to skutečně nutné, nikdy nevěřit na rčení „to se tak dělá“, „vždyť o nic nejde“ a pod.,

-nedůvěřovat bezmezně „informovanosti“ státních úředníků, zejména policie ve složitějších a pro občana závažných situacích,

-být obezřetný ohledně rodného čísla, které bude v dohledné době velmi kritickým údajem; ve většině případů by místo sdělení rodného čísla mělo stačit datum narození či jen letopočet,

-ve vlastním zájmu si zjistit, jak s jeho daty zachází banka, lékař, pojišťovna atd.,

-vést v patrnosti své údaje, kdy je dal a komu, a využívat zákonné úpravy o ochraně dat podle [250],

-pokud má tituly, neváhat je kombinovat při sdělování adres spolu s případně i dalšími iniciálami; lze tak snadněji zjistit, kdo předával data dál, či kdo je jinak zneužil,

-dávat pozor na formuláře různých firem, loterií a klubů, s ohledem na celkovou nepřehlednou „džungli“ v této oblasti našeho hospodářství,

-nepodléhat zbytečně reklamním akcím a omezit na minimum nebo vůbec nerealizovat objednávky zboží u různých zásilkových organizací, které mnohdy zakládají databáze svých klientů a za úplatu jsou ochotny neoprávněně poskytovat o nich informace dalším zájemcům.

6.4. Bezpečnostní politika

Obecně *bezpečnostní politikou* rozumíme tvorbu a uplatňování souboru zásad a pravidel určujících základní aspekty bezpečnosti nějakého chování. Zmíněný soubor by měl být vyjádřený písemnou formou a zaměřený na konkrétní činnost organizace či jedince. Z hlediska počítačové kriminality nás zajímají ty zásady, které se týkají bezpečnosti provozu informačních technologií, tedy počítačů, počítačových sítí a všech dalších systémů provozovaných ve spojitosti s počítači nebo jejich prostřednictvím. V souladu s autorem studie [168] lze tvrdit, že smyslem bezpečnostní politiky je poskytování základního rámce řešení bezpečnosti všem uživatelům a pracovníkům odpovědným za implementaci bezpečnosti. S rostoucí závislostí každodenních činností organizace na informačních technologiích roste i její závislost na zachování důvěrnosti, integrity a dostupnosti informací, s kterými pracuje. Dosažení účinné bezpečnosti je úkolem, nebo spíše výzvou pro vedení organizace na všech úrovních. Bezpečnost je většinou finančně nákladná, může znepříjemnit dříve snadné používání systémů, např. zavedením řízení přístupu. Může bránit efektivnímu využití systémů, např. omezením vzájemného propojení systémů. Nejbezpečnější je systém, který není používán. Takový systém není ovšem funkční, takže je potřeba hledat optimální řešení bezpečnosti vůči funkčnosti systému.

Lidský faktor a bezpečnost. Příliš mnoho jedinců považuje bezpečnost za pouze technický nebo technologický problém. Přitom právě lidský faktor zde hraje velice důležitou roli. Jak uvádí autor [168], největší hrozbou bezpečnosti informačních technologií v dané organizaci jsou její vlastní zaměstnanci. Připojí-li např. organizace svou interní síť přes *firewall* (prostředek adresné zodpovědnosti a kontroly přístupu) na síť veřejnou, pak jediný nedisciplinovaný uživatel, který propojí svůj personální počítač z interní sítě modemem např.

na Internet, může účinnost firewallu značné omezit a ohrozit tím bezpečnost sítě. Jako příklad jiného ohrožení bezpečnosti uveďme situaci podle [168]: Jistá významná společnost každoročně zveřejňovala k určitému datu své hospodářské výsledky a po několik let vykazovala stabilní růst. Jeden rok však došlo k obratu ve vývoji, několik dní před oficiálním oznámením výsledků bylo prodáno velké množství akcií společnosti. Následné vyšetřování ukázalo, že zpráva o výsledku byla vytvářena na počítači připojeném do sítě a výchozí přístupová práva umožňovala kterémukoliv zaměstnanci společnosti seznámit se s výsledky již pět dní před jejich zveřejněním. Tuto možnost zjevně někdo ze zaměstnanců zneužil a informace prodal.

Komplexní posuzování hledisek bezpečnosti. U nás je v současné době dosti běžné, že vedení určité organizace ví nebo jen tuší, že je pracováno s citlivými informacemi, přičemž nejsou promýšleny komplexně všechny aspekty jejich ochrany. Podle [168], přijímají se zpravidla jen dílčí opatření, která řeší bezpečnost jen nedůsledně či přímo nedostatečně. Např. banka řeší ochranu osobních dat svého klienta šifrováním, avšak důvěrnost jeho dat zajistí jen zdánlivě, protože dostatečně nezabezpečila ochranu šifrovacích klíčů v rámci přístupu k citlivým informacím. Proto je důležité přijetí komplexních zásad, mezi které patří právě zajištění důvěrnosti dat, přístupu k citlivým informacím, ale i zásada oddělení povinností, princip dvojité kontroly, prověřování a výběr zaměstnanců, zásady spolupráce s třetími stranami, např. s firmou implementující šifrování apod. Dokumentace bezpečnostní politiky zahrnuje zpravidla obecné prohlášení o cílech, účelu, povinnostech a odpovědnostech. Obvykle se definují obecné prostředky pro dosažení těchto cílů, např. interní předpisy nebo standardy organizace. V hierarchii interních předpisů organizace jsou zásady bezpečnostní politiky nadřazené ostatním materiálům a jejich dodržování je povinné. Zásady bezpečnostní politiky nesmějí být ve sporu s právní úpravou větší síly, např. se zákony. Použité formulace musí být dostatečné obecné, představují dlouhodobě platné zásady, které by neměly podléhat častým změnám. V tom se daný dokument podstatné liší od standardů nebo předpisů konkrétně upravujících určité činnosti. Bezpečnostní politika může např. obecně stanovit povinnost zachování důvěrnosti a integrity dat přenášených počítačovými sítěmi. Příslušný interní standard konkrétně určí, že zachování důvěrnosti a integrity dat bude realizováno šifrováním přenášených dat určitým algoritmem podle národní nebo mezinárodní normy. Pokud tento algoritmus přestane vyhovovat a bude nahrazen jiným, změní se pouze interní standard.

Nezbytnost bezpečnostní politiky. Dojde-li v organizaci např. k úniku informací nebo zneužití dat, následuje obvykle rozhodnutí vedení, že přístup k informacím a datům musí být omezen, řízen a kontrolován. Ale jak a kým bude omezen, jak a kým bude řízen, jak a kým bude kontrolován? A kterých informaci se omezení bude týkat? Právě bezpečnostní politika stanoví povinnost realizovat *analýzu rizik,* která vymezí citlivé informace, stanoví obecná pravidla řídící přístup k těmto informacím, způsob kontroly přístupu a případný postih, nebo i další potřebné specifikace. Zaměstnanci nemají tendenci si sami přidělávat práci. Častým argumentem při vysvětlování nějakého bezpečnostního problému bývá rčení *„kdyby mi to*

vedoucí nařídil, tak bych to udělal". Bezpečnostní politika je jednou z možností, jak z nejvyšší úrovně demonstrovat význam a důležitost informační bezpečnosti pro organizaci a uložit každému zaměstnanci povinnost informace chránit. Řídící pracovníci na střední úrovni potom nemohou bezpečnost ignorovat. V organizacích, kde se pravidelně plánuje a sestavuje rozpočet na další období, to donutí příslušné vedoucí pamatovat i na výdaje na informační bezpečnost jejich útvarů. Naopak, pracovníkům zabývajícím se bezpečností to zaručuje přidělení nezbytných zdrojů. Pokud organizace není schopna přesně určit a vyhlásit, co je např. při používání počítačů zakázáno, nebo co je povoleno, těžko bude schopna postihovat případy, kdy dojde k nějakému zneužití práce s počítačem. Bezpečnostní politika je pro vedení poměrně levným a účinným nástrojem, umožňujícím definovat, co je pro organizaci přijatelné a co nikoliv. Je celkově výrazem určitého zájmu na dodržování pravidel a norem uvnitř organizace i zákonnosti vůbec.

Aspekty minimální ochrany a vztahu k jiným organizacím. Mnohdy se stává, že některé organizační jednotky podporují snahy o dosažení informační bezpečnosti, jiné se jim brání, protože je považují za omezení jejich činnosti. Jestliže obě jednotky sdílejí tytéž zdroje, např. interní síť a obslužný systém, souborový server apod., může být snaha na jedné straně znehodnocována nečinností na straně druhé. Bezpečnostní politika může v tomto případě určit *minimální úroveň ochrany*, kterou pak musí všichni dodržovat. Existence bezpečnostní politiky, včetně zásad minimální ochrany, hraje důležitou roli také ve vztahu k jiným, zejména kooperujícím organizacím. Pro každého partnera je jasným signálem, že informační bezpečnost v daném podniku není podceňována, že je jí věnována odpovídající pozornost. Při vzájemné výměně informací mají zúčastněné strany záruku, že předávané informace budou dostatečně chráněny. Rozhodne-li se např. finanční instituce z kapacitních důvodů pro zajišťování některé své činnosti prostřednictvím externí firmy, pak by existence bezpečnostní politiky měla být jedním z faktorů výběru konkrétní firmy. Bezpečnostní politika má i preventivní aspekty v oblasti počítačové kriminality, protože svými zásadami může odradit případné potenciální pachatele. Podle [168], v USA mohou být vedoucí pracovníci organizací trestně postiženi za nedostatečné řešení informační bezpečnosti např. v porovnání s úrovní bezpečnosti dosažené v jiných organizacích zabývajících se stejnou činností. Bezpečnostní politika musí být v USA propracována v každé vládní organizaci.

Aktivní role zaměstnanců je v bezpečnostní politice velmi důležitá. Je třeba pravidelně vysvětlovat její smysl a účel všem zaměstnancům. Je to náročný úkol, protože měnit dosavadní způsob uvažování a zažité zvyky není snadné. Důležitou roli přitom hrají pravidelná bezpečnostní školení všech zaměstnanců, neustálé zvyšování povědomí zaměstnanců o informační bezpečnosti. Bezpečnost musí být začleněna do programu školení a vzdělávání pro všechny úrovně zaměstnanců. Bezpečnost musí mít na zřeteli ve větší či menší míře při své práci všichni, jinak bude naplňování bezpečnostní politiky obtížné a pomalé. Klíčovou roli přitom hraje vedení organizace, pokud nepovažuje informace za jeden z kritických faktorů pro činnost organizace, nebude věnovat pozornost ani zajištění jejich bezpečnosti. Výchozím aktem může být uskutečnění analýzy rizik a využití jejích výsledků

jako základu pro definování bezpečnostní politiky. Bezpečnostní politika může mít různé formy, různý rozsah a různé zaměření podle typu činnosti organizace; typicky však řeší vždy fyzické, personální, administrativní a technické aspekty bezpečnosti. Politika může být definována na více úrovních, přičemž na nižších úrovních se zaměřuje na jednotlivé aspekty bezpečnosti a řeší je konkrétněji. Je vhodným východiskem pro řešení souladu činnosti organizace a jejích vnitřních předpisů s platnou legislativou. Každý zaměstnanec organizace by měl být při nástupu do zaměstnání s bezpečnostní politikou seznámen a podepsat prohlášení, kde se zaváže ji dodržovat.

Zajištění kontroly bezpečnostní politiky. Dodržování politiky musí být kontrolováno nezávislým útvarem, např. vnitřním auditem. Samotný fakt, že dodržování bezpečnostní politiky je sledováno, většinou dále přispívá k jejímu naplňování. Bezpečnostní politika by měla být v pravidelných intervalech hodnocena a revidována. Ve větších podnicích je užitečné určitým způsobem také formalizovat hlášení a řešení případů porušení bezpečnosti, tzv. *hlášení incidentů.* Analýzou incidentů lze identifikovat oblasti s nedostatečně zajištěnou bezpečností a přijímat pak příslušná nápravná opatření, resp. modifikovat nebo aktualizovat samotnou bezpečnostní politiku. Bezpečnost není samoúčelná, je důležitá, ale i finančně náročná, proto je třeba vždy hledat vhodný kompromis, např. mezi bezpečností a její cenou, mezi bezpečností a její schůdností při praktickém provozu apod. Jednou z prvních otázek externího auditora při zahájení auditu v organizaci je obvykle dotaz na existenci bezpečnostní politiky. V zemích s vyspělou úrovní informačních technologií existuje bezpečnostní politika i na národních úrovních. Bohužel u nás se úloha informačních technologií stále ještě plně nedoceňuje, takže vyhlášení všenárodní bezpečnostní politiky v této oblasti není asi zatím příliš aktuální.

**

Mnohoúrovňová bezpečnost, bezpečnost na vysoké úrovni. Pokud hodláme řešit otázky počítačové bezpečnosti v rámci rozsáhlého systému informací při velkém počtu uživatelů, nabízí se možnost využití tzv. *mnohoúrovňového přístupu*. Při použití klasických bezpečnostních modelů by nám nezbylo než usednout a sepsat obsáhlý seznam, který bude popisovat, kdo má jaká práva. V tom případě by šlo o značný objem nezáživné práce, při které by mohla vzniknout spousta chyb. Další těžkosti spočívají v průběžném udržování velkého seznamu práv a v jeho aktualizaci. Za cenu jisté ztráty pružnosti lze popsané problémy velmi elegantně vyřešit. Všechny datové objekty rozdělíme na třídy podle předpokládaného stupně nutného utajení. Každému z uživatelů pak určíme rozsah práce s příslušnými tajnými daty. V případě dat hovoříme o *klasifikaci*, v případě uživatelů o *prověření* na jistou úroveň utajení. Zbývá ještě určit pravidla, podle kterých se bude rozhodovat, zda danému uživateli poskytneme přístup k požadovaným datům. Na první pohled se zdá být vše jednoduché, každý smí pracovat s daty až do té úrovně klasifikace, pro kterou má prověření.

Některé problémy mnohoúrovňové počítačové bezpečnosti. Uživatel pracující s daty různé klasifikace by omylem, nebo i úmyslně mohl přenést informace z jedné úrovně utajení na jinou. Tak by mohlo docházet k únikům informací, či k narušeni integrity při přenosu na vyšší úroveň. Zajímavý přístup k prezentování informací na nižší úrovni při reálném použití mnohoúrovňových systémů se vyskytuje např. v armádách. Podle autorů studie [12], řešení, které preferují v USA spočívá ve smyšlených či krycích informacích, které zaručují správné splnění úkolu níže postaveným operátorem, aniž by u něho vzniklo jakékoliv podezření na kamufláž. V Británii je tento přístup odmítán, operátor se k dané informaci nedostane s tím, že mu tato kvůli utajení nepřísluší, nanejvýše se dozví úroveň utajení Takto se Angličané vyvarují chyb při vymýšlení krycích příběhů, ale musí být ještě pečlivější při klasifikaci informací. To je ale všeobecný problém, příliš úzkostlivá klasifikace na co nejvyšší úroveň je nepraktická pro ztíženou použitelnost informací, bezstarostná klasifikace na nízkou úroveň může vést ke ztrátě hodnoty informací. V principu potřebujeme dobře vzájemně oddělit informace s různou klasifikací. Kvůli efektivitě by však naopak bylo vhodné všechny informace zpracovávat na jednom určitém místě v rámci jediného informačního systému.

Modely klasifikace počítačové bezpečnosti. Z předchozího je jasné, že nevystačíme pouze se sledováním přístupů k datům. Je nezbytné zkoumat též toky informací v systému. Musíme stanovit bezpečnostní politiku, na základě které budeme rozhodovat, které přesuny informací povolit a které nikoliv. K tomuto účelu byly vyvinuty dva formální bezpečnostní modely, viz např. [12].

Prvním z nich je *Bell-LaPadulův model*. Tento model popisuje, jaké přesuny dat jsou povolené, aby nemohlo docházet ke kompromitaci utajených informací. Model pracuje se stupni utajení informace, kdy

-subjekt nesmí číst objekty s vyšší klasifikací, než ty, pro něž má prověření,

-subjekt smí zapisovat informace jen do úrovně jemu přístupné pro čtení a do úrovní vyšších.

Naopak zachování integrity zpracovávaných informací zaručuje *Bibův model*. Tento model definuje stupně integrity a povolené přesuny informací právě ve vztahu k těmto stupňům, kdy

-subjekt může modifikovat pouze objekty s nižší klasifikací, než ty, pro něž má prověření,

-subjekt smí zapisovat informace jen do úrovně jemu přístupné pro čtení a do úrovní nižších.

Všimněme si jisté protichůdnosti obou popsaných modelů. Je pravděpodobné, že objekty s vyšším stupněm utajení budou mít přiřazeny i vyšší stupně integrity. Oba modely dovolují pouze jednosměrný tok informací. To by, například v případě *Bell-LaPadulova* modelu, umožňovalo rozvědce sbírat data, ale znemožňovalo by na základě těchto dat vydávat rozkazy nižším složkám. Problém se řeší tak, že informace, které chceme posunout „zakázaným“ směrem, nejprve vytvoříme na nějaké povolené úrovni a následně oprávněná

osoba uskuteční jejich administrativní reklasifikaci na požadovanou úroveň. Modely tedy popisují pouze ty přesuny, které je možno provádět rutinně. Někdy se přistupuje k určitému omezení tvrdosti modelů tím, že se povoluje zápis i do jiných úrovní, pokud zapisovaná informace nezávisí na žádných datech s klasifikací pro níž má operátor oprávnění ke čtení.

Od teorie k praxi mnohoúrovňové počítačové bezpečnosti. Podle [12], jednoduché myšlenky není zcela jednoduché uvést do praxe. Jak již bylo naznačeno, je třeba zajistit vzájemné oddělení informací s různou klasifikací a zároveň umožnit uživatelům s nimi simultánně pracovat. Ne za všech okolností je to snadné. Uvažme například, že chceme vytvořit novou kopii souboru na vyšší úrovni klasifikace. Doručení potvrzení, že se operace povedla, však již je v rozporu s *Bell-LaPadulovým* modelem. Systém musí dávat bedlivý pozor na možnost vzniku skrytých kanálů jimiž mohou unikat informace na nižší stupně utajení a musí zajistit bezpečné sdílení technických zařízení apod. Historie nám zanechala množství jednoúrovňových informačních systémů. Každý z těchto navzájem dobře oddělených systémů spravuje data s určitou klasifikací. Chce-li zde uživatel získat veškeré informace o jisté skutečnosti, nezbude mu než obejít všechny systémy s daty různých úrovní a informace doslova posbírat. Cílem je nějakým způsobem integrovat tyto doposud oddělené systémy. Umožníme tak jednodušší a efektivnější přístup k datům a zároveň omezíme jejich redundanci. Nejjednodušším prostředkem integrace systémů jsou tzv. *mnohoúrovňové stráže*. Jejich prostřednictvím je možno spojit systémy dat s různou klasifikací. Stráže tak v podstatě hlídají rozhraní mezi systémy a zajišťují, že při přesunech dat mezi systémy nedochází k porušení bezpečnostní politiky. Jejich nevýhodou je, že uživateli jednoho systému poskytují pouze omezený přistup k informacím v druhém systému.

Plnohodnotný přístup k službám jiného systému poskytují mnohoúrovňové pracovní stanice. Zpravidla jde o terminály, na kterých lze v jednotlivých oknech provozovat rozhraní několika systémů. Uživatel tak může střídat práci v několika systémech, může mezi nimi přenášet informace apod. V tomto případě je automaticky kontrolováno dodržení bezpečnostní politiky a data jsou před novým uložením automaticky reklasifikována. Za vyšší vývojový stupeň lze nepochybně považovat *mnohoúrovňové databázové systémy*. Tyto systémy jsou již samy o sobě schopny zajistit dodržování bezpečnostní politiky a pravidel formálních modelů. Na jednom místě dokáží spravovat a zpřístupňovat informace různého stupně utajení. Zcela odbourávají redundanci uložených dat, poskytují daleko konzistentnější a komplexnější pohled na spravované informace. Bez zajímavosti není ani jejich jednodušší správa a levnější provoz ve srovnání s několika systémy jednoúrovňovými. Dnes již realizovatelnou metou bezpečnostní techniky je mnohoúrovňový bezpečnostní systém, poskytující komplexní repertoár služeb elektronického zpracování informací. V takovém systému je zahrnuta nejen databáze, ale i podpora zpracování textů, poštovní systém, systém pro podporu rozhodování a řízení, a ostatní kancelářské služby a potřeby. Dokonalý mnohoúrovňový systém by měl být schopen připojit k sobě okolní jednoúrovňové systémy a spolupracovat s nimi. Aby mohl mnohoúrovňový bezpečnostní systém dobře fungovat, musí přesně vědět, jaká je klasifikace jednotlivých dat. Z tohoto důvodu musí být každý objekt opatřen bezpečnostním návěstím,

které specifikuje jeho přesnou bezpečnostní klasifikaci a případná další omezení manipulace s objektem.

Nehierarchické členění informací. Rozdělení informací podle stupně utajení je pro většinu aplikací příliš hrubé. Proto jsou všechny informace, podle toho, o čem pojednávají, rozděleny na tematické okruhy, nebo též oddělení. Rozdělení není disjunktní, daná informace může být zařazena do většího počtu oddělení. Ve všech odděleních je však prezentována se stejným stupněm utajení. Každý subjekt má právo pracovat s informacemi pouze z některých oddělení. Toto nehierarchické členění informací se používá zároveň s hierarchickým členěním dle stupně utajení. Pokud subjekt žádá přístup k datům, musí být prověřen na dostatečnou úroveň a musí mít přístup do všech oddělení, do kterých je zařazena požadovaná informace. Důležitým pravidlem pro přidělování prověření subjektům je *princip nejmenších práv*. V zásadě jde o to, že každý subjekt by měl mít přidělena pouze taková oprávnění, která zcela nezbytně potřebuje pro to, aby mohl korektně vykonávat své úkoly.

Svazový bezpečnostní model. Výsledkem aplikace hierarchického a nehierarchického členění informací je svazový bezpečnostní model. Jde o částečně uspořádanou (vzhledem k množinové inkluzi) množinu, která má největší a nejmenší prvek. Nejmenším prvkem je prověření na nejnižší úroveň a pro žádné oddělení, největším prvkem potom prověření na nejvyšší úroveň a pro všechna oddělení. Požaduje-li subjekt přístup k datům, systém podle modelu ověří, zda má dostatečné prověření v rámci hierarchického členění a zda má prověření pro všechna oddělení, do kterých byla daná data zařazena. Svazový model se tedy uplatní pro *statické přístupy k datům*. Pokud dochází k přesunům dat, přijdou navíc ke slovu *Bell-LaPadulův* nebo *Bibův* model, aby bylo zajištěno utajení nebo integrita dat v rámci a po ukončení přesunu. Speciálním případem svazového modelu je tzv. *military security model*, používaný americkým ministerstvem obrany. Podle hierarchického členění rozeznává informace neklasifikované, důvěrné, tajné a přísně tajné. Nehierarchické členění může zahrnovat všechny oblasti lidské činnosti, na které lze jen pomyslet. Z našeho pohledu je však podstatné to, že svazový bezpečnostní model může asi nejlépe předcházet kriminalitě v oblasti informačních technologií.

**

Bezpečnost počítačové sítě. Jak uvádí [47], počítačová síť a zvláště Internet - to je to, co činí počítačovou bezpečnost aktuální. Jediní, kteří na dobu uzavřených výpočetních středisek vzpomínají v dobrém, jsou právě bezpečnostní úředníci. Děrné štítky, resp. pásky uživatel podal žádankou okénkem operátorce a později přišel pro zaevidované výstupní sestavy. Která organizace, podnik či instituce dnes nemá (alespoň lokální) síť; kdo z pracovníků v oblasti řízení dnes nekomunikuje na Internetu? Internet lze v dnešní době chápat i jako informační síť hackerů a jejich protivníků. Internet vytváří synergický efekt mezi svými účastníky, samozřejmě i hackery. V USA 80% počítačových zločinů vyšetřovaných FBI se dnes týká Internetu. Počítačové incidenty exponenciálně narůstají, v posledních pěti letech řádově stouply z tisíců na statisíce případů. Například Pentagon zaznamenal v roce 1996 přes 250 tisíc útoků, z toho 65% úspěšných. Internetová komunita se také brání - již v roce 1988 vzniklo fórum *FIRST (Forum of Incident Response and Security)*, které nyní sdružuje více než 30 bezpečnostních týmů na celém světě. Nejznámější z nich jsou *CERT*

(Computer Emergency Respose Team) a *CIAC (Computer Incident Advisory Capability).* *CERT* je koordinační centrum s nepřetržitou službou, s cílem kdykoliv pomoci administrátorům systému při vzniku problémů v oblasti počítačové bezpečnosti a poskytovat rady, jak těmto problémům předcházet. *CIAC* především vydává bezpečnostní bulletiny, ve kterých informuje o nových problémech v oblasti bezpečnosti Internetu.

Bezpečnostní služby sítě. Cílem bezpečnostního systému je poskytnout služby, které by eliminovaly nebo minimalizovaly jednotlivé hrozby a rizika. *ISO* (Mezinárodní organizace pro standardizaci) se pokusila standardizovat služby a mechanismy počítačových sítí v rámci dodatku ke standardu otevřených systémů *OSI (Open Systems Interconnection).* Síťové prostředí přináší pro bezpečnostní služby určitá specifika. Podle [47] jsou jimi

-*autentizace* - v síti jde nejen o jednostrannou či vzájemnou autentizaci entit, ale také o zdroje posílaných dat; přitom je zřejmé, že tato služba díky síťovému prostředí neochrání data před zdvojením nebo modifikací;

-*řízení přístupu* - řídit přístup lze nejen k samotným datům, ale i k síťovým zdrojům; zjemnění autentizace tímto typem služby se v rámci síťového řízení používá běžně; jako příklad lze uvést seznam síťových adres, resp. čísel portů akceptovatelných pro daný fyzický port směrovače, resp. přepínače;

-*důvěrnost informací* - v síti je třeba službu zajištění důvěrnosti dat rozšířit o službu zajištění důvěrnosti spojení a ochranu před pasivním sledováním provozu sítě, např. před sledováním intenzity toků informací, což bývá označováno jako *důvěrnost provozu;*

-*integrita* - pokud je v síti realizován přenos s navázáním spojení, je třeba kromě datových celků (bloků, polí) zajišťovat celé toky dat, např. číslováním, spolehlivým označováním času, digitálním podpisem ap.;

-*nepopiratelnost* - využívá se pouze v mimořádně důležitých aplikacích, např. v bankovnictví a vojenství; je to náročná služba, protože souvisí s právní problematikou a její realizační mechanismy se obvykle opírají o koncepci (nezávislé) důvěryhodné třetí strany; na rozdíl od předchozích služeb je to služba, která je poskytována výhradně v rámci sítě, lze na ni nahlížet velmi zjednodušeně jako na silnější verzi autentizace a řízení přístupu.

Autentizace, integrita a důvěrnost, jsou třemi základními pilíři bezpečnostní služby; zbývající dvě služby lze považovat za odvozené. Tři základní bezpečnostní služby mají autonomní postavení. Svědčí o tom i to, že každá z těchto služeb může používat samostatné klíče, dokonce i takové, které jsou získány stejným *kryptografickým mechanismem*, např. klíčem pro zajištění důvěrnosti a autenticity.

Hrozby v síti. Základními hrozbami, resp. riziky v oblasti informačních systémů jsou podle [47] obecně únik informace, narušení integrity dat, výpadek služby, neoprávněné použití. Nejčastějším terčem útoků jsou systémy utajení - protokoly sady *TCP/IP*, které dnes ovládly svět sítí. Na úrovni protokolu *IP* jde zpravidla

-o odposlech; tento pasivní typ útoku žádný paket nepoškodí, ale nelze ho také obvykle zjistit,

-o přehrávání; např. odchycením a opakovaným vysíláním paketu s legálním příkazem k platbě,

-o změnu paketu s odpovídající opravou kontrolního pole,

-o ničení paketů, např. zásahem do kódu, resp. filtračních pravidel směrovačů,

-o zahlcení sítě záplavou odchycených anebo uměle generovaných paketů,

-o kradení paketů, např. přihlášením se do sítě s adresou některé dočasně odpojené stanice,

-o hledání cest k obcházení filtrujících směrovačů záplavovým směrováním,

-o změnu nastavení směrovačů příkazem pro přesměrování.

Oproti tomu na úrovni *TCP* již byly použity útoky spočívající

-v záplavě příkazů pro navázání spojení, po kterých „klekaly“ servery díky obsazení všech vyhrazených soketů,

-v odhadu správného číslování nedostupné odpovědi stanice ve vnitřní síti na příkaz pro navázání spojení a tedy ve správném potvrzení této odpovědi.

Na aplikační úrovni jsou nejčastější útoky založeny na přepisování webových stránek Internetu, kradení a falšování pošty a spousta dalších. Největším nebezpečím však obvykle nejsou hackeři, nýbrž špatně připravená nebo nezodpovědná obsluha a účastníci, včetně chyb v nastavení směrovačů, špatně zvolená hesla ap.

**

Bezpečné komunikační protokoly. Podle [184], protokoly rodiny *TCP/IP* byly původně vyvíjeny pro Ministerstvo obrany USA. Jejich hlavním cílem nebylo zajištění bezpečné komunikace, ale hlavně co největší odolnost proti výpadkům částí komunikačních sítí. V potenciální válce by byly totiž nejdříve zničeny hlavní komunikační uzly. Ve veřejné síti je proto nutné provozovat bezpečnostní protokoly na hladinách vyšších než *IP*. Bezpečnostní protokoly musí zajistit důvěrnost spojení, integritu dat a možnost ověření identity komunikujících stran, tedy autentizaci.

SSL (Secure Socket Layer) je bezpečnostní protokol navržený firmou *Netscape*. Tento protokol je možné zařadit do relační vrstvy otevřených modelů *OSI*. Je možné jej provozovat nad jakoukoliv spolehlivou spojovanou službou. *SSL* domlouvá bezpečnostní parametry během ustavování spojení. Když klient a server začínají spolu komunikovat, musí vzájemně dohodnout především kryptografické parametry, verzi protokolu, metodu předání tajných klíčů pomocí šifrovacího algoritmu s veřejným klíčem a volitelně se mohou autentizovat.

Protokol sám neřeší ověřování platnosti certifikátů, avšak definuje rámec, kterým probíhá bezpečná komunikace. Protokol nevyžaduje využití specifických šifrovacích a autentizačních metod. Bezpečnost tohoto protokolu závisí na tom, jaké parametry klient se serverem dohodne. V případě, že je umožněna neautentizovaná komunikace, může být bezpečnost ohrožena pomocí modifikace zprávy třetím účastníkem, příp. prolomením klíče. Další nevýhoda tohoto protokolu spočívá v tom, že obsahuje též některé patentované algoritmy, což může způsobit problémy při implementaci.

PCT (Private Communication Technology) - protokol podobný předchozímu, avšak od firmy *Microsoft*. Používá týž základní formát jako *SSL*, liší se pouze ve formách výměny zpráv při oddělení autentizačních klíčů od šifrovacích. Výhody i nevýhody protokolu jsou obdobné jako u *SSL*.

Protokolem SHTTP je možné zabezpečit komunikaci pomocí přenosových protokolů *HTTP (HyperText Transfer Protocol)* . Byl vytvořen tak, aby byl snadno integrovatelný přímo s *HTTP* a je s ním kompatibilní. Je to protokol na aplikační úrovni a funguje na bázi typu „dotaz-odpověď", což může být pro uživatele výhodné. Pro zabezpečení zprávy poskytuje digitální podpis, autentizaci a šifrování. Není závislý na určitém druhu algoritmů a umožňuje používat různé metody předávání klíčů a certifikátů. Je však svázán s protokolem *HTTP* a nelze jej použít pro jiný druh přenosu.

Ačkoliv existují i další protokoly pro bezpečnou komunikaci, protokol *SSL* má zatím určité prioritní postavení; je hojně používán a podporován hlavně ve webových aplikacích Internetu. Jak uvádí [184], jeho podstatný náskok před ostatními protokoly může v budoucnu zmírnit protokol *TLS (Transport Layer Security)* připravovaný *WWW konzorciem*.

**

Bezpečnost databází. Moderní systémy řízení bází dat zajišťují bezpečnost uložených dat cestou všech známých bezpečnostních služeb vyjma nepopiratelnosti; jsou tedy schopny zajistit autentizaci, důvěrnost a integritu, dat včetně řízení přístupu k nim. Jak uvádí autor studie [46], kromě řízení přístupu jsou všechny tyto služby použitelné i pro přenos dat, naopak řízení přístupu slouží výhradné pro zabezpečení uložení dat a je službou typickou pro databáze. Opírá se navíc o specificky výlučné mechanismy, zatímco např. všechny ostatní bezpečnostní služby lze zajistit všeobecně používanými mechanismy, např. šifrováním nebo digitálním podpisem. Proto právě *řízení přístupu* je třeba věnovat hlavní pozornost. Zde se ovšem nebudeme zabývat všemi problémy spojenými s bezpečností, jako např. otázkami *inference*, tedy implikacemi nových informací ze zjištěných dat, např. kdy ze specializace lékaře lze přibližné vyvodit chorobu pacienta atp. Totéž platí pro problém *agregace*, např. kdy celková suma peněz na platy není utajovaná, ale platy jednotlivých pracovníků ano apod.

Dvě podoby řízení přístupu k databázi. Podle studie [46], řízení přístupu k databázi má dvě podoby. Je to

-*volitelné řízení přístupu*, kdy oprávněný uživatel přiděluje potřebná přístupová práva (privilegia) k objektu individuálně pro jednotlivé uživatele nebo jejich skupiny; přístupová práva mohou být pružně měněna a kombinována objekt od objektu, zatímco jeden subjekt má u jednoho objektu vyšší úroveň přístupových práv, u druhého objektu tomu může být naopak;

-*povinné řízení přístupu,* kdy bezpečnostní úředník objekty člení do předem stanovených bezpečnostních úrovní pomocí bezpečnostních návěstí a subjekty zařazuje do skupin s příslušnými přístupovými právy; autorizace je zde neměnným procesem pro celou bezpečnostní úroveň; pokud má subjekt více privilegií k nějakému objektu než jiný subjekt, nemůže jich mít k jinému objektu méně.

Schéma volitelného řízení přístupu. Bezpečnostní politika v tomto případě musí být vyjádřena příslušnými bezpečnostními pravidly, konkrétně u databází jde o autorizační pravidla. Nad jejich vykonáváním musí dohlížet bezpečnostní systém, u databází autorizační podsystém. Autorizační podsystém musí obdržet autorizační pravidla, kterým bude „rozumět". Vymezení oprávněného uživatele závisí na konkrétním systému řízení databáze, protože administraci autorizace lze řešit různými politikami. Vše může určovat administrátor databáze, administrovat objekt může také ten, kdo ho vytvořil, anebo kdokoliv, kdo obdrží povolení od jeho vlastníka v rámci delegování práv. V každém případě je schéma volitelného řízení přístupu založeno na principu vlastnictví objektu. Výsledkem je velká pružnost tohoto schématu. Jeho použití však přesto přináší několik omezení a rizik. Jde zejména o

-*nevýhody plynoucí z koncepce vlastnictví informace,* jednak lze každé vlastnictví odcizit a navíc je zde problém s centrálním monitorováním stavu zodpovědnosti;

-*kaskádování autorizace* předáváním vlastnictví, což vede k problémům s revokací, znejišťující vlastníky;

-*riziko útoků typu trojský kůň,* kdy např. jeden uživatel může získat neoprávněně přístupové právo k objektu, jehož vlastníkem je jiný uživatel, tím, že vytvoří vlastní verzi třídicího nástroje doplněním standardního programu o instrukce čtení příslušného objektu; pak stačí třídicí program nahradit upravenou verzí a v klidu čekat, až se jiný uživatel pustí do třídění;

-*problémy s předzpracovanými pohledy na databázi*, tzv. view - skutečnost, že má každý uživatel přiděleno své *view* je z jedné strany velká výhoda; např. nastoupí-li nová operátorka může mít ihned své *view* standardně vytvořené pro operátory; z druhé strany je to však také nevýhoda - operátorka může pořizovat data pouze v rozsahu svého *view*, ale ne v rozsahu *view* např. ředitele; konkrétně pak ředitel musí pořizovat všechny údaje o platech sám, i když jsou tajné jen některé; je zřejmé, že za této situace může snadno dojít k porušení pravidel utajení a k nežádoucímu úniku informací.

Schéma povinného řízení přístupu je aplikací principu mnohoúrovňové bezpečnosti do databázového prostředí. Toto schéma je vhodné pro databáze, ve kterých mají data spíše statický a rigidní charakter, tj. hodí se např. pro prostředí armády a dalších státních institucí.

Zatímco známá *Oranžová kniha* amerického ministerstva obrany definuje množinu bezpečnostních požadavků pro libovolný systém, interpretaci požadavků na databázové systémy popisuje tzv. *Levandulová kniha* s obalem modrofialové barvy. V rámci schémat povinného řízení přístupu by se měly uplatit zásady v souladu s modelem Bell-LaPadula *„No-read-up, No-write-down“*, v praxi se však většinou připouští zápis pouze na vlastní úrovni. Je zřejmé, že zde nejde jen o ochranu před neautorizovaným přístupem jako u předchozího schématu, ale i o řízení toku dat v databázi, neboli o ochranu před útoky typu *trojského koně*. V relacích vytvořených dle schématu povinně řízených přístupů se lze setkat s problémem mnohonásobného výskytu informací. Původcem může být

-uživatel nižší úrovně, který doplňuje danou hladinu o data vyšší úrovně, přičemž výsledek nemůže vidět,

-uživatel vyšší úrovně, který přesouvá data z nižší na vyšší úroveň, ten výsledek samozřejmě uvidí.

Důsledkem mohou být situace, kdy vzniknou

-mnohonásobné řádky, více řádků má stejný primární klíč,

-mnohonásobné položky, kdy k témuž primárnímu klíči jsou vztaženy hodnoty atributů s různými úrovněmi.

Mnohonásobné řádky se mohou vztahovat k téže nebo k různým entitám; hovoříme pak o položkové anebo řádkové mnohonásobnosti. Moderní modely, např. *SeaView*, umožňují oba přístupy. Schéma povinného řízení přístupu má také své problémy, zejména přichází v úvahu

-granualita bezpečnostních objektů - existuje široká škála názorů na to, na jaké úrovni přidělovat bezpečnostní návěsti, zda celé databázi, souborům, relacím, atributům nebo dokonce i hodnotám atributů; čím je zvolen detailnější přístup, tím obtížněji se uživateli specifikuje bezpečnostní úroveň, u rozsáhlé databáze to bývá opravdu pracný proces;

-těžkopádnost pravidel *Bell-LaPadulova* modelu, např. bezpečnostní pravidla organizace vyžadují, aby uživatel vyšší úrovně podepsal dokument zpracovaný pracovníkem nižší úrovně, ale podle pravidel Bell-LaPadulova modelu zapisovat na nižší úroveň nelze.

Bezpečnost objektově orientovaných databází. Relační modely jsou vhodné pro realizaci mnohoúrovňové bezpečnosti, zatímco objektově orientovaný přístup se zde setkává s řadou problémů. Když je totiž přístup řízený k určité rozsáhlé třídě objektů, dotaz na jeden z nich si vyžaduje autorizaci na celou třídu. Koncepce vlastnictví v kontextu objektově orientovaných databází nemá rovněž jednoznačnou interpretaci. Kdo může být vlastníkem instance vytvořené jiným uživatelem, než sám vlastník třídy? U objektově orientovaných modelů jsou jednotkou přístupu instance objektů, bylo by proto logické, aby autorizace byla vztažena právě k nim. To by však mohlo zvětšit neúměrně zátěže na databázi. Dalším problémem je vytvoření modelů povinného řízení přístupu pro objektově orientované databáze. Aby mohl být z důvodu verifikovatelnosti splněn požadavek na co nejmenší bezpečnostní monitor, je vhodné, aby všechny atributy objektu měly tutéž úroveň. Pro řadu

objektů je však toto omezení nepřijatelné. Snaha po vyřešení rozporuplných požadavků na zabezpečení objektově orientovaných databází je dodnes aktuální tématem vědeckého výzkumu počítačové bezpečnosti.

Podle [46], prakticky vzato z bezpečnostního, výkonového i uživatelského hlediska poskytuje dlouhodobě nejlepší řešení nejspíše asi systém *Oracle*. Zejména poslední aktualizované verze tohoto systému mohou uspokojit i projektanty s vysokými nároky na počítačovou bezpečnost.

**

Bezpečnost elektronické pošty. Jak správně uvádí autorka studie [75], většina zaměstnanců firem, včetně technických specialistů, při implementaci elektronické pošty do denní praxe obvykle automaticky předpokládá její bezpečnost. Například zaměstnanci předpokládají u vyměňovaných zpráv zachování důvěrnosti zpráv. Monitorování zpráv nadřízeným pracovníkem v případě hanlivých výroků na jeho adresu ze strany podřízeného zaměstnance, které má za následek třeba i ukončení pracovního poměru, se jim jeví jako porušení práva na soukromí. Platné zákony a nařízení obvykle tuto problematiku neřeší, přesto dnes velká část podniků nebo úřadů nemá vypracovanou bezpečnostní politiku pro používáni e-mailu.

K významným bezpečnostním službám, které může elektronická pošta nabízet, patří

-*důvěrnost zprávy (zajištění soukromí),* nikdo kromě zamýšleného příjemce nesmí být schopen přečíst zprávu,

-*autentizace,* příjemce má záruku o identitě odesilatele,

-*integrita,* příjemce má záruku, že zpráva nebyla změněna,

-*nepopiratelnost původu*, příjemce musí být schopen prokázat třetí straně, že odesilatel skutečně zprávu odeslal (odesilatel nemůže později odeslání zprávy popřít),

-*nepopiratelnost podání,* odesilatel získá ověření, že zpráva byla podána systému pro předání pošty (ekvivalentem je u běžné pošty doporučená pošta),

-*nepopiratelnost přijetí*, ověření, že příjemce obdržel zprávu,

-*důvěrnost toku zpráv,* jde o rozšíření služby důvěrnosti v tom smyslu, že nejen nikdo kromě zamýšleného příjemce nemůže znát obsah zprávy, ale nemůže dokonce ani zjistit, zda odesilatel zprávu příjemci odeslal,

-*anonymita,* zprávu je možné poslat takovým způsobem, že příjemce nemůže zjistit identitu odesilatele,

-*zamezení úniku,* síť je schopna zabránit tomu, aby nedošlo k úniku informací určitých bezpečnostních úrovní mimo konkrétní oblast,

-*audit,* síť je schopna zaznamenat případy, které mají určitý vztah k bezpečnosti,

-*samozničení zprávy,* možná volba pro uživatele, zajišťující zničení zprávy po jejím doručení příjemci (přesněji po jejím dešifrování a zobrazení); příjemci je tak znemožněno uložit nebo poslat zprávu dál,

-*integrita pořadí zpráv*, jistota, že nedošlo ke změně pořadí zpráv.

Prostředky realizace bezpečnostních služeb elektronické pošty. Většina bezpečnostních služeb vyžaduje kryptografické prostředky. Chce-li strana *A* poslat straně *B* zprávu, musí mezi sebou ustavit správné klíče a to v závislosti na použité technologii veřejných nebo tajných klíčů. Klíče mohou být sdíleny mezi stranou *A* a *B*, ale do hry může vstupovat infrastruktura sítě nebo ti, kdo rozšiřují distribuční seznamy. U jednotlivých služeb nutno objasnit, kdo klíče potřebuje.

Bezpečnostní služba zajištění důvěrnosti (soukromí). Chce-li strana *A* poslat straně *B* zprávu tak, aby ji nikdo jiný nemohl přečíst, použije kryptografii k zašifrování zprávy. Protože obvyklý postup by nebyl v případě pošty efektivní, postupuje se tak, že strana *A* vybere náhodný tajný klíč *S* a zašifruje jím danou zprávu. Potom zašifruje tajný klíč *S* veřejným klíčem strany *B*. I v případě většího počtu příjemců tak šifruje zprávu pouze jednou. Tajný klíč *S* pak zakóduje jednou pro každého příjemce příslušným klíčem. Pokud strana *A* posílá zprávu distribučnímu seznamu, umístěnému ve vzdáleném uzlu, a strana *B* je pouze jedním z příjemců seznamu, nemusí strana *A* znát jednotlivé strany seznamu a nemá obvykle ani jejich klíče. Má ale klíč toho, kdo distribuční seznam rozšiřuje. Ten pak musí mít klíče jednotlivých stran, umístěných na seznamu.

Bezpečnostní služba autentizace zdroje. Není-li systém pošty správně v tomto smyslu zabezpečen, může strana *B* obdržet od nepřátelské strany *C* zprávu, kde je v políčku FROM uvedena strana *A*. Jestliže strana *B* tuto zprávu vezme vážně, může to vyvolat značnou škodu. Je proto důležité, aby strana *B* měla jistotu, že zpráva skutečné přišla od strany *A*. V případě použití technologie veřejného klíče můžeme předpokládat, že strana *B* zná veřejný klíč strany *A*, a ta může pomocí svého soukromého klíče zprávu digitálně podepsat. To dává straně *B* záruku, že autorem zprávy je strana *A*. Posílá-li strana *A* zprávu většímu počtu příjemců, týž podpis bude funkční pro všechny příjemce (schéma využívající distribuční seznamy). Při použití tajných klíčů musí strana *A* ujistit stranu *B*, že je opravdu stranou *A* tak, že prokáže znalost sdíleného tajného klíče. Obvykle to prokáže kryptografickým výpočtem na zprávě pomocí tohoto tajného klíče.

Bezpečnostní služba integrity. Mechanismy uváděné při autentizaci zdroje poskytují rovněž integritu zprávy. Všechny standardy elektronické pošty poskytují inegritu zprávy i autentizaci zdroje společně.

Bezpečnostní služby nepopiratelnosti. Význam této služby je dosti zásadní, zejména v oblasti boje s hospodářskou počítačovou kriminalitou. Banka by jistě neměla reagovat na transakci, kterou požaduje v poslané zprávě strana *A*, a která se týká např. převodu vysoké částky na účet strany *B*, pokud nemá jistotu, že zpráva skutečně pochází od strany *A*. To zejména tehdy, nebude-li schopna v případě potřeby soudu prokázat legálnost požadavku transakce. Využití kryptografie umožňuje poskytnutí silnější služby, než je certifikace

odeslání zprávy běžnou poštou, kdy zaplacením určitého obnosu navíc získáme od pošty potvrzení, že jsme určitého dne předali určitou zprávu s uvedením určité adresy. Uživatel může později prokázat, že zpráva byla předložena, i pokud třeba nebyla doručena. V běžné poště uplatňujeme požadavek, aby nám bylo předloženo potvrzení příjmu zprávy. U elektronické pošty podepíše místo určení, nebo poštovní služba dodání, výtah zprávy zřetězené s jakoukoliv další užitečnou informací, např. s vyznačením času převzetí.

Bezpečnostní služba zajištění důvěrnosti toku zpráv. Tato služba má význam tehdy, když zpráva odeslaná stranou *A* straně *B*, je pro někoho dalšího užitečná, a to i v případě, že je obsah zprávy šifrován. Může to být případ zneužití informací při jejich předávání, kdy strana *B* je novinářem a strana *A* členem vládního výboru s přístupem k tajným informacím.

Bezpečnostní služba anonymity. Význam služby vynikne, když strana *A* chce poslat zprávu straně *B*, ale přitom si nepřeje, aby strana *B* věděla, kdo zprávu poslal. V tomto případě nestačí, že by strana *A* zprávu pouze nepodepsala. Obvykle je např. příjemci dostupný záznam cesty zprávy, obsažený v přenosu pošty. Chce-li proto strana *A* zajistit anonymitu zprávy, může postupovat stejně, jako při důvěrnosti toku zpráv. Dá zprávu třetí straně a ta odešle nepodepsanou zprávu straně *B*. Tuto službu poskytují běžně tzv. *anonymní remailery,* které jsou však údajně často provozovány zpravodajskými službami.

Bezpečnostní služba zamezení úniku. Tato služba je využívána u systémů, aplikujících model povinného řízení přístupu. Síť je v tomto případě rozdělena do částí, které mají schopnost zacházet s určitými bezpečnostními třídami. Každá zpráva musí být označena v souladu s její bezpečnostní klasifikací a směrovače zprávy by pak měly odmítnout předání zprávy té části sítě, která není schopna zacházet s požadovanou bezpečnostní třídou.

Bezpečnostní standardy systémů elektronické pošty. Ke světovým bezpečnostním standardům elektronické pošty patří normy *PEM, PGP* a *X.400.* Norma *X.400* je standard elektronické pošty *CCITT.* Na rozdíl od *PEM* a *PGP*, které podávají úplné specifikace, takže podle nich můžeme přímo vytvořit implementace, u *X.400* najdeme často pouze rámce, vymezení struktur pro danou implementaci. Z hlediska bezpečnosti si musíme uvědomit, že *X.400* je systém pro přenášení zpráv, a elektronická pošta je jedním typem zprávy, kterou můžeme přenášet. Elektronická pošta je definovaná v *X.420.*

Aplikace norem bezpečnosti, pokud jde o certifikáty. V *PEM* existuje pro jakékoliv jméno pouze jedna certifikační cesta k tomuto jménu. Od všech uživatelů se očekává, že jí budou důvěřovat. *PGP* nechává na uživatelích, které cestě budou důvěřovat. Může existovat mnoho řetězců certifikátů, a je na každém uživateli, zda např. vyřadí každou cestu zahrnující určitou osobu. Norma *X.400* nespecifikuje pravidla důvěryhodnosti pro certifikační hierarchii. Každá implementace se rozhoduje sama, jsou možná schémata typu *PEM, PGP,* eventuálně další.

Distribuce certifikátů podle norem bezpečnosti elektronické pošty. V *PEM* je pro distribuci certifikátů stanoveno místo v hlavičce pošty, určené původně pro umístění vlastního certifikátu, což není využíváno, protože *PEM* není spojena se službou adresářů. Posílání podepsané zprávy je bez problémů, ale při posílání šifrované zprávy musí před odesláním

zprávy strana *A* získat certifikáty strany *B*. Standard *PGP* předpokládá distribuci certifikátů jinými prostředky.

Aplikace norem bezpečnosti, pokud jde o šifrování. S ohledem na výkonnost používají systémy e-mail při šifrování symetrické algoritmy, shodné pro obě strany. U *PGP* i *PEM* je tajný klíč použitý k zašifrování zprávy sám zašifrován veřejným klíčem příjemce. V případě většího počtu příjemců je odesílaná zpráva jednou zašifrována tajným klíčem náhodně vybraným odesilatelem a klíč je pak pro každou zprávu zašifrován veřejným klíčem konkrétního příjemce. Výhoda *PGP* spočívá v možnostech komprese odesílaného textu, čímž se urychlí šifrování a dešifrování, ztíží se eventuální kryptoanalýza a šetří se místo na disku i doba přenosu.

Zakódování zpráv přenášených elektronickou poštou. Ve všech systémech pošty je poskytnuta podpora podepsaným zprávám, šifrovaným i nešifrovaným. *PEM* a *PGP* podporují dvě verze nezašifrovaných a podepsaných zpráv. Norma *X.400* byla navržena k přenosu pošty, aniž by mohlo dojít v průběhu přenosu k modifikaci pošty. Podle *PEM* se přenáší zašifrovaná zpráva v *ASCII* kódech, v *PGP* lze poslat šifrovanou zprávu modifikovanou, nebo zakódovanou v *ASCII*.

Kryptografické algoritmy při přenosu zpráv elektronickou poštou. Podle [75] uvedené standardy e-mailu byly všechny navrženy jako nezávislé na kryptografickém algoritmu. Při implementaci nutně musí systém pošty podporovat algoritmus, vybraný pro konkrétní zprávu, jinak by dvě implementace nemohly spolupracovat. Teoreticky sice je u všech standardů podpora zajištěna, v praxi však *PEM* i *PGP* podporuje určité algoritmy, resp. klíče šifrování, ale *X.400* však nikoliv. Rozdíly v podpoře kryptografických prostředků existují rovněž např. pokud jde o příjemce s mnoha klíči a v poskytování funkcí v infrastruktuře dodání pošty.

**

Politické a legislativní návaznosti ochrany informací podle studie [215]. Jakkoliv je z nejrůznějších hardwarových, softwarových, organizačních i jiných pohledů pro informatika zajímavý problém ochrany dat, celá věc má, nebo přesněji řečeno měla by mít, z důvodu průhlednosti jasný právní rámec. Z něho by mělo být co možná nejlépe patrno, jaké informace lze sbírat, kdo to může dělat a jak lze celý tento proces kontrolovat. Informace o občanech jsou více či méně a lépe či hůře sbírány velmi dlouho. Snad až kam lidská paměť sahá. Přesto se však úvahy o tom, že tuto sféru zájmů člověka je třeba chránit, skutečně datují až od doby, kdy se reálně objevují počítače. Logicky se to váže

-na skutečnost, že není třeba příliš se bránit existenci obrovských „skládek“, obsahujících spousty údajů, v nichž naleznout adekvátní informaci v požadovaném čase klasickými postupy není prakticky možné,

-na možnosti tyto informace automatizovaně rychle třídit, vybírat a analyzovat.

Extrémní přístupy k řešení těchto otázek jsou v zásadě dva:

1)Umožnit shromažďování veškerých informací o jedinci na jednom místě; jakákoliv stránka osobnosti jedince musí přitom být informačně podchycena tak, aby držitel oněch informací mohl mít přehled o tom, co ho zajímá. Držitel informací pak může jednak působit

ve prospěch daného jedince, např. pokud jde o zdravotnické informace, nebo se bránit před jeho negativní činností, např. využitím informací o jeho trestné činnosti.

2)Neshromažďovat vůbec žádné informace, protože všechno, co se týká občana, je jeho výlučnou záležitostí a nikdo nemá právo jakkoliv do jeho soukromí zasahovat.

Autor studie [215] podotýká, že snad není třeba za těmito tendencemi hledat konkrétní zemi či politické zřízení, protože historicky vzato se projevovaly prakticky všude. V každém případě je zřejmé, že absolutní volba jednoho či druhého extrému není myslitelná. Zásadní problém spočívá v nalezení vhodného a přijatelného kompromisu mezi nimi. Vzhledem k tomu, že snahy po racionálním řešení zazněly v období poměrně vyhraněné pozornosti věnované lidským právům, došlo k odklonu od prvního extrému, dříve z praktických důvodů poněkud preferovaného, spíše k extrému druhému. Pokud bychom měli jasno v otázce, jaké informace co do struktury dovolíme sbírat, vzniká problém druhý, problém *pravdivosti evidovaných informací*. S tím pak souvisí celý dosti složitý právní aparát, který má za cíl umožnit kontrolu evidovaných informací, a to jak ze strany držitele informace, tak i ze strany občana, jehož se týkají. Zdánlivě zde nejde o příliš závažné otázky, ale pokud si uvědomíme např. složitosti doprovázené zveřejňováním informací ze svazků bývalé StB, svůj názor jistě poopravíme. Bohužel, v současné době navržený zákon o poskytování informací otázky pravdivosti údajů neřeší. Další dimenze tohoto problému spočívá i v tom, že s rozvojem počítačové techniky může nakládat často i s citlivými daty v podstatě kdokoliv, kdo vlastní běžný personální počítač, vybavený všeobecně dostupným softwarem. Zatímco dříve z finančních a technických možností mohl operovat s takovými údaji zpravidla pouze stát. Z toho pak vychází nutnost právně omezovat okruh subjektů, oprávněných informace daného typu shromažďovat. Navíc si musíme uvědomit, že právo na získávání informací patří k základním lidským právům a jakkoliv je omezit lze zpravidla pouze zákonem v případech hodných zvláštního zřetele. Ke složitosti situace přispívá ještě nutnost účinné kontroly, včetně praktických otázek její realizace a vymahatelnosti předepsaných pravidel bezpečnosti.

Prvním orgánem, který se snad vůbec kdy touto problematikou z hlediska práva zabýval, byla *Rada Evropy*. Ta již v roce 1950 vydává *Konvenci o ochraně lidských práv a základních svobod,* která obsahuje dokonce dva články, zabývající se nakládáním s informacemi. Mezi první vnitrostátní právní normy, stanovující základní pravidla ochrany soukromí občanů, pak patří „informační zákony“ ve Švédsku (1973), v Německu (1977) a v Rakousku (1998). Rada Evropy svou činnost v této oblasti rozvíjela i nadále, a tak v roce 1981 vydala *Úmluvu na ochranu osob se zřetelem na automatizované zpracování osobních údajů č.108.* Ta již tehdy definovala závaznost takových pravidel pro veřejný i soukromý sektor, určila nutnost vzniku státního orgánu pro dozor nad jejich dodržováním, stanovila podmínky pro získávání, aktualizaci a likvidaci informací, vyhradila zvláštní podmínky pro práci s tzv. citlivými informacemi, vymezenými jako informace ryze soukromého a intimního typu, a stanovila záruky pro občana k tomu, aby věděl, co a kde se o něm shromažďuje. *Úmluva* v současné době prochází výraznou novelizací, která má snahu reagovat na změněné podmínky s ohledem na rozsah sbíraných údajů, možnosti komunikace mezi subjekty sbírajícími data atd. Rozbor jednotlivých ustanovení těchto dokumentů by přesáhl vymezený

rozsah tohoto textu. Závaznost uvedených dokumentů pro jednotlivé členské státy *Rady Evropy* je dána pouze explicitním zvážením okolností místního dodržování a aplikace do vlastního vnitrostátního práva. V každém případě jde však o velmi kvalitní právní text, který vzešel z dílny předních evropských právníků z této oblasti a stal se také vzorem pro další informační zákony konkrétních států, včetně našeho.

Do poněkud jiné sféry náleží dokumenty *OECD* z této oblasti. Tato organizace, jíž se stala Česká republika členem teprve historicky nedávno, rovněž již řešila problémy vztahující se nejen k bezpečnosti informačních systémů, ale také ke kryptografii nebo třeba k toku personálních dat přes hranice států. K tomu je však dobré poznamenat, že právní vazby některých států na tyto dokumenty jsou poněkud složitější, protože nezanedbatelná část států *OECD* patří do oblasti tzv. angloamerického práva, které se značně liší od práva našeho typu, tzv. kontinentálního. Odlišnosti se podle [215] týkají především procesu vzniku právních norem. Z tohoto důvodu se styčné plochy hledají pochopitelně mnohem obtížněji.

**

Optimální způsoby zajišťování počítačové bezpečnosti jsou u různých autorů pojímány celkem jednotně. Určité rozdíly lze vidět pouze ve strategii realizace podle profesního zaměření ochrany. Obecně při zajišťování počítačové bezpečnosti je nutno podle [121] realizovat

-*analýzu hrozeb*, tedy co všechno by mělo být chráněno, a především analyzovat, jaké jsou hrozby vůči ochraňovaným hodnotám; tento krok je směrodatný pro další postup, často však lze vycházet pouze z analýzy empirických poznatků o problémech v okolí, o jiných útocích na podobné hodnoty atd.; chybně uskutečněná analýza hrozeb má za důsledek téměř vždy chybná bezpečnostní opatření; hodnoty pak mohou být chráněny velmi nákladným, nepřiměřeným a neúčinným způsobem;

-*specifikaci bezpečnostní politiky a architektury;* bezpečnostní politika stanoví cíle ochranných opatření; zahrnuje požadavky, pravidla a postupy určující způsob ochrany a zacházení s ochraňovanými hodnotami; architektura na vyšší úrovni popisuje strukturu celého komplexu opatření a jednotlivým částem přiřadí bezpečnostní funkce;

-*popis bezpečnostních mechanismů* s rozepsáním techniky pro implementaci bezpečnostních funkcí nebo jejích částí; účinnost mechanismu musí být v souladu s bezpečnostní politikou a přiměřená odpovídajícím hrozbám.

Podívejme se nyní na některé *základní prvky bezpečnostní politiky* a jejich provázanost s bezpečnostní architekturou. V konkrétních případech nejsou vždy upotřebitelné všechny uvedené prvky. Pro praxi v předcházení počítačové kriminalitě je významná

-*důvěrnost*; provozovatel se bude snažit zabránit zjištění výskytu informací nepovolanými osobami; může se o to snažit obecně utajením existence informací, což je značně obtížné, kontrolou přístupu k informacím či jejich šifrováním; je jasné, že stoprocentní ochrana v tomto směru je v podstatě nemožná a provozovatel se musí spokojit s určitým kompromisem;

-*integrita*; informace bez povolení provozovatele nesmí změnit svůj charakter; pokud bude zajištěna na dobré úrovni důvěrnost, pak zachování integrity je rozhodně snazší;

-*dostupnost* záleží na vhodně definovaném přístupu oprávněných uživatelů; přitom provozovatel si přeje, aby vhodní uživatelé měli přístup k informacím co nejméně komplikovaný;

-*zodpovědnost z*a veškeré aktivity vyvíjené vůči informacím má provozovatel, správce systému ochrany, ale i uživatel v rámci zodpovědnosti vůči provozovateli; tato zodpovědnost nemusí být přímá, provozovatel nekontroluje bezprostředně každého uživatele, ale v případě potřeby musí vždy existovat možnosti pohybu informací vůči operujícím jednotlivcům.

Nevhodnost doplňkové bezpečnosti. V reálném světě počítačů a informací jde o postup dosti častý. Nejprve je vybudován rozsáhlý systém a teprve dodatečně se přichází na to, že bude potřeba nějak zajistit ochranu spravovaných informací. Dodatečně se proto vyčlení určitá částka z rozpočtu a začne se doplňovat. Důsledky a výsledky bývají tytéž, jako při doplňování jedné z pozapomenutých stěžejních funkcí systému těsně před dodáním zákazníkovi. Doplňková bezpečnost v naprosté většině případů neposkytuje stejnou míru ochrany jako bezpečnost budovaná pro začlenění v prvotní specifikaci systému. Důsledkem pozdního doplnění bezpečnosti může být vybudování ochrany na nižší úrovni, než by za stejné náklady poskytla ochrana plánovitá.

Fyzická a personální bezpečnost. Počítačová bezpečnost nespočívá jen v pořízení a nainstalování ochran do systému. I v dokonalých počítačových systémech hraje významnou roli fyzická bezpečnost. Jde o to zjistit, kdo má fyzický přístup k prvkům systému, bez ohledu na hardwarovou či softwarovou ochranu, nebo jaký může být dopad přírodních katastrof. Dokonalá ochrana uživatelských stanic je mnohdy k ničemu, pokud je k systému připojena konzola, ze které operátor může neoprávněně (a nepozorovaně) sledovat informace na uživatelských obrazovkách. A dokonale šifrovaná data na serveru, z něhož někdo bez problémů ukradl celý pevný disk, řešení podnikové strategie nezachrání. Proto personální bezpečnost je dalším významným pilířem dobré ochrany.

Praktické aspekty návrhu počítačové bezpečnostní politiky. Při návrhu bezpečnostní politiky je třeba si uvědomit, že mnohé hrozby nelze přímo odvrátit, ale lze jen snížit pravděpodobnost jejich případné realizace, eventuálně s minimálními ztrátami (zdržením) zajistit následnou nápravu. Informace je možné lehce duplikovat a záložní kopie bezpečně ukládat na vzdáleném místě. Ani velmi přísný provozovatel nemůže obecně zabránit šíření virů, může však usilovat o přiměřené metody profylaxe. Zajištění bezpečnosti nikdy neznamená zajištění úplné ochrany, nýbrž minimalizaci rizik na tolerovatelnou úroveň. Lze to podle [121] vidět i na skutečném případu budování bezpečnosti v celostátní počítačové síti *Národního zdravotního systému (NHS)* v Anglii. Předběžný odhad nákladů pouze na zavedení šifrovacích služeb pro zajištění důvěrnosti dat je téměř 20 milionů liber, na roční údržbu a provoz padnou zhruba 3 miliony liber. Podle názoru mnohých expertů budou skutečné náklady několikanásobné vyšší, i když se pominou investice na zajištění jiných, pro medicínskou praxi životně důležitých funkcí spolehlivé počítačové sítě. S budováním systému se vlastně ještě nezačalo, zatím probíhají případové testy. Je uvažováno o dvou

zásadních hrozbách, možnosti neautorizovaného připojení jedinců (hackerů) k síti a možnosti odposlechu zasílaných informací. Kritiku tohoto přístupu lze shrnout uvedením dvou údajů. Podle posledních údajů z nezávislého auditu *Národního zdravotního systému* je jen 6 % případů narušení bezpečnosti způsobeno zvenčí. Podle slov vedoucího organizace *UNIRAS,* která je zodpovědná za analýzu incidentů v oblasti bezpečnosti informačních technologií v celé vládě, byla v předchozích letech jen 2 % případů narušení bezpečnosti způsobena zvenčí. Na základě těchto údajů lze do určité míry zpochybnit zajištění důvěrnosti jako stěžejního problému. Problematickým je do značné míry i přístup vedení *NHS*, které vše vyvíjí do značné míry utajeně a jen nerado slyší praktické připomínky, požadavky i dotazy budoucích uživatelů sítě - lékařů a zdravotnických pracovníků. Nedůvěra k systému dospěla tak daleko, že *British Medical Association* doporučila nepřipojovat k síti *NHS* žádné počítače a zařízení, které zpracovávají klinické nebo i citlivé administrativní informace. Síť *NHS* se tak stává velmi nákladným zařízením, kterým putují jen úřednická memoranda a oběžníky. Tento příklad lze pojímat jako varování před prosazováním nepromyšlených koncepcí drahých informačních systémů v některých našich resortech. V důsledcích takových aktivit může jít pak o kriminální fenomén mrhání společenskými prostředky.

**

Variabilita aplikací bezpečnostních opatření. Počítačová bezpečnost nemusí pro každého znamenat totéž. Bude jiná pro armádu, jiná pro banky a nemocnice a jiná pro správce různých rubrik v inzertních a jiných časopisech. Jak uvádí autor studie [123], existují dvě zásadní sféry aplikací bezpečnosti. Ta prapůvodní je vojenská, kde se např. kryptografické techniky, tedy bezpečnostní mechanismy, uplatňují zprvu nezávisle na počítačích již po historicky dlouhou dobu. V současné době však začíná nabývat na významu sféra obchodní či komerční. Požadavky obou se často významně liší a přestože vojenské aplikace daly oboru bezpečnosti informačních technologií první uplatnění, dnes se musí i vojenští činitelé často přizpůsobovat požadavkům sféry druhé. Velká přeorganizovanost armády, v určitém smyslu ústící až do nepřehlednosti, vytváří potřebu zajišťovat určité složitější systémy ve zpracování a využití informací. To v zásadě spočívá

-v zajištění vlastní informační dominance - je třeba mít správné informace na správném místě ve správný čas,

-v minimalizaci nepřátelské informační dominance - omezit šíření vlastních informací k nepříteli, případně dokonce zajistit dodání špatných (klamavých) informací.

Hierarchické členění informací je z hlediska počítačové bezpečnosti zásadním problémem. V přeorganizovaných strukturách není systematizace dat a jiných informací jednoduchou záležitostí; částečné řešení přináší hierarchická klasifikace informací. Pro minimalizaci nepřátelské informační dominance je důležité svěřovat pracovníkům jen nejpotřebnější informace a také tyto pracovníky předem i průběžné prověřovat. Odtud plyne, že důvěrnost je zásadním požadavkem v obdobných systémech. Hierarchické členění je jednoduchým modelem vhodným pro tento účel. Počet úrovní a klasifikace informací na určitou úroveň záleží na požadavcích organizace. Podle [123] uživatel prověřený pro určitou úroveň má obvykle možnost prohlížet informace na úrovni své a všech nižších. Jedna z

nejčastěji aplikovaných bezpečnostních politik je založena na modelu *Bell-LaPadula*. Což, jak již bylo uvedeno, znamená, že

-procesy nesmějí číst data na vyšší úrovni; to je tzv. jednoduchá bezpečnostní vlastnost, též *NRU* – „no read up“,

-procesy nesmějí zapisovat data do nižší úrovně; tzv. vlastnost *NWD* – „no write down“.

Tyto dvě základní vlastnosti a formální aparát pro sledování stavu bezpečnosti počítače tvoří podklad pro budování mnohoúrovňových systémů. Model má drobné nedostatky, přesto je důležitým mezníkem v oboru počítačové bezpečnosti. Jak uvádí [123], dnes je na základě tohoto horizontálního pohledu hodnocena úroveň bezpečnostních technik a aplikací. Celý obor informační, speciálně pak i počítačové bezpečnosti je tímto pohledem do značné míry ovlivněn. Řešení reálné bezpečnosti tímto modelem je ale opravdu jen částečné, poněvadž je do značné míry umělé a neodráží skutečnou situaci. I v armádě se řeší problémy s ohledem na původ protivníka, druh krizové situace apod. Tedy nikoliv s ohledem na začlenění informací o protivníkovi do určité kategorie. Např. americká armáda má dnes „nastavenou“ úroveň *„přísně tajné“,* rozšířenou o oborové podúrovně, jako třeba *„přísně tajné nukleární“, „přísné tajné chemické“, „přísně tajné kryptografické“* atd. Další problémy mohou souviset se způsobem prosazování takovéto bezpečnostní politiky. To, že nelze zapisovat data do nižší úrovně, je např. u tajných služeb dosti problematické. Část zpravodajské sítě může totiž padnout díky zrádci na vyšší úrovni, o jehož přístupu k materiálům na nižší úrovni nejsou správci těchto materiálů informováni. Kdyby se údaje o přístupu (požadavek zodpovědnosti) zapisovaly, pak lze srovnáním těchto údajů u „odstraněných“ agentů zjistit, kdo si jejich materiály prohlížel. V praxi se na tyto souvislosti přichází obvykle jen náhodou.

Bezpečnost v komerční problematice. V komerční sféře je běžné, že práce se člení podle obchodních případů, rozmístění poboček atd. Často sice záleží na utajení informací (např. před konkurencí), nejdůležitějším požadavkem je však integrita dat. Nemusí vždy jít o integritu ve striktním pojetí, ale o smysluplnost a správnost využívaných informací. Modelem, který je nejčastěji citován pro komerční bezpečnost, je podle [123] model *Clark Wilsonův,* který přihlíží ke stoletým zkušenostem z obchodování a účetnictví. Model formalizuje pohled na data a operace nad daty při zachováni integrity, ale též i na pojmy jako auditní záznam a řízení přístupu. To, že se v komerční sféře řeší problémy s ohledem na „téma“ podle obchodního partnera či případu apod., vede k odlišnému přístupu ke zpracování informací oproti jiným oblastem. Svou roli zde samozřejmě hraje i menší rozsah drtivé většiny firem a potřeba pružného jednání. Pokud komerční pohled hodně zjednodušíme, pak jej lze shrnout do *vertikálního modelu* členění informací. Hrozby vojenským systémům pocházejí primárně od vnějších činitelů, kdežto komerčním systémům hrozí větší nebezpečí od vlastních pracovníků. Vždyť i celý systém podvojného účetnictví je kontrolním systémem proti neúmyslným a často i proti úmyslným chybám, pokud knihu zápisu pro kreditní a debetní pohyby vedou dvě různé osoby či skupiny. Zaměstnanci mohou kromě zadávání nesmyslných informací do firemních informačních systémů, informace také roznášet vně firmy, např. i pro konkurenci. Zde má opodstatnění tendence některých firem, aby zaměstnanci nevěděli

více, než je pro jejich práci nezbytně nutné. Informace jsou pro armádu velmi důležité, pro komerční organizace však naprosto nezbytné, často i existenčně. Také interakce pracovníků armády s okolním světem je podstatně menší než u pracovníků komerční organizace. Důležitým aspektem pro úschovu a zpracování informací v komerční sféře jsou právní závazky a do značné míry i podpora zákazníka. K výše uvedenému přistupuje potřeba zajištění bezpečnosti při plně elektronickém obchodování. Téměř vždy je třeba zajistit integritu dat, často i ve spojení se zajištěním důvěrnosti. Nehledě k autentizaci (ověření původu) dat, zajištění nepopiratelnosti původu zprávy nebo jejího přijetí atd. Zkusme si představit, jak bychom např. přes Internet realizovali „jen" běžný styk s bankou, s poštou, stručné dotazy lékařům či právníkům, nákup akcií, objednávání dovolené a lístků na vlak ap. Zkusme popřemýšlet, které z našich činností by bylo možno realizovat podobným způsobem a jaká bezpečnostní opatření bychom při realizaci očekávali nebo přímo požadovali. Bylo by případné zjištění nebo dokonce pozměnění přenášených dat k něčemu dobré zaměstnavateli, sousedovi z našeho bydliště, hackerovi z odlehlého města nebo zlodějské bandě z nejbližšího okolí? A co když banka omylem odečte z účtu jinou částku než bylo dohodnuto? Na těchto případech vidíme ve velmi zjednodušené podobě složitost problematiky informační, speciálně pak počítačové bezpečnosti.

Vše však nelze zjednodušovat. Uvedené zjednodušení vojenského a komerčního pohledu na využívané informace může být v některých ohledech násilné, pro popsání rozdílu v pohledech na různé aspekty bezpečnosti je však výstižné. Svět není černobílý, ale výše popsané rozdíly mohou být pro pochopení mnohých otázek užitečné. Je důležité si uvědomit, že „bezpečnost" nemusí pro každého znamenat totéž. Bude jiná pro generála, jiná pro šéfa pobočky banky a jiná pro správce firemní databáze. Nyní se dostáváme k novince posledního desetiletí tzv. *soukromé bezpečnosti*. Není to sice úplná novinka, již např. Caesar si dopisoval s Kleopatrou šifrovaně, ale je zřejmé, že významu nabývá právě s dostupností počítačů i pro osobní potřebu. Pak lze příliš vtíravému pronikání do osobního života účinně bránit často právě zase počítačem.

**

Kritéria hodnocení bezpečnosti informačních technologií. Standardy v průmyslovém světě znamenají jednu ze zásadních cest předávání znalostí, snižování nákladů a umožňování vzájemné spolupráce a kompatibility nejrůznějších produktů. Podle [122] lze v bezpečnosti informačních technologií standardy členit do skupin

-na *základní standardy* určené pro obecné požadavky uživatelů, sem patří např. bezpečnostní architektura *OSI*, mechanismy autentizace entit a další podobné,

-na *funkční standardy* pro zajištění a certifikaci produktů, pro nejrůznější služby apod.; tyto standardy vysvětlují obecný přístup k využití základních standardů, patří sem např. požadavky k autentizaci dat, základům integrity atd.,

-na *kritéria hodnocení* určená pro hodnocení produktů a systémů, např. různé speciální oborové normy informačních technologií,

-na *průmyslové standardy a postupy,* což jsou technické a procedurální normy, vyžadované specifickými skupinami uživatelů nebo společnostmi, např. bankovní standardy,

-na *výkladové dokumenty*, jako jsou rukověti, průvodcovská kompendia, slovníky pro informovanost a vzdělání, pokyny k ochraně soukromí, seznamy termínů atd.

Potřeba standardizace, a to nejen v bezpečnosti informačních technologií, vyvstala s přechodem od sálových počítačových systémů k otevřeným systémům a samozřejmě též s rozšířením významu zejména počítačových komunikací. Kritéria pro hodnocení bezpečnosti informačních technologií slouží především jako měřítko používané k hodnocení informačních technologií s ohledem na jejich bezpečnost, na konkrétní aplikace služeb a na opatření k zajištění bezpečnosti. Vládní kritéria většinou určují hlavní směr vývoje i pro kritéria bankovní, komerční atd. Obvykle však jsou vládní kritéria používána i nevládními organizacemi. Hodnocené objekty se často dělí

-na produkty, které nemají specifikováno provozní prostředí a tedy ani rizika či hrozby,

-na systémy jako větší spojité celky s vyhraněným rysem spočívajícím v tom, že je při hodnocení známa i konfigurace a provozní prostředí.

Jak uvádí autor [122], při hodnocení je od výrobce, resp. iniciátora hodnocení vyžadováno utajení podrobné specifikace, dokumentace a popisu postupu při vývoji daného produktu. Lze tím do jisté míry čelit úniku informací, jež jsou pro výrobce často životně významné. To je důležité mimo jiné též pro omezování případného věcného zneužití informačních technologií či oddalování rizik jiných typů počítačové kriminality. U jiné než komerčně nezávislé agentury mohou být tyto dokumenty vystaveny většímu riziku zneužití. Vlastní hodnocení je realizováno na základě žádosti (a za prostředky) výrobce, který také specifikuje úroveň či rozsah hodnocení produktu či systému. Podle specifikace požadavků v kritériích musí výrobce hodnotiteli poskytnout potřebnou dokumentaci, podporu odborníků ap. Hodnocení probíhá v určitém prostředí a konfiguraci, proto je také nutno tyto údaje uvádět při prezentování výsledků hodnocení a akreditace. Např. u databázových systémů nutno uvést základnu a operační systém, včetně verzí produktů, pomocí nichž se hodnocení uskutečnilo.

Nejdůležitější světové standardy. Oranžová kniha. Koncem šedesátých let si odpovědní činitelé amerických vládních agentur začali uvědomovat potřebu jednotného měřítka pro hodnocení produktů informační technologie s ohledem na specifické služby při ochraně informací. Hodnocení produktů pro jednotlivé úřady bylo jak časově, tak i finančně náročné a perspektiva jednoho zhodnocení a akreditace, která by byla platná pro daný produkt na celém území USA, byla snad nejjednodušším řešením. Daná akreditace šetří čas a vládní prostředky, protože bez ní by bylo nutno hodnotit vždy znovu při každém nákupu. Druhým pozitivním aspektem je pak možnost srovnání a snazší specifikace potřeb jednotlivých úřadů. Výsledek dlouholeté práce ministerstva obrany, standardizačních orgánů a také vládě blízkých firem se dostavil v podobě kritérií pro hodnocení důvěryhodných výpočetních systémů. Tato kritéria byla vydána v roce 1985 jako standard ministerstva obrany. Oranžový přebal charakterizoval tuto publikaci, která je pod názvem *Orange Book* známa po celém světě.

Trusted Computer System Evaluation Criteria (TCSEC). Tento standard je ovlivněn dobou vzniku a slouží především pro potřeby víceuživatelských monolitických počítačů. Databázové systémy, sítě, menší části systémů atd. byly pak s postupem času brány v úvahu dílčími interpretacemi, jako např. *Trusted Database Interpretation, Trusted Network Interpretation atd.* I jejich barvy přebalů pak daly podnět k názvům jako *Red Book* ap. Čtyři skupiny *TCSEC A,B,C,D* odpovídají vždy jednomu kvalitativně odlišnému stupni bezpečnosti a jsou dále děleny do tříd *A1, B1, B2, B3, C1, C2, D*. Každá ze tříd pokrývá a popisuje čtyři aspekty hodnocení - bezpečnostní směrnice, zodpovědnost, zabezpečení a dokumentaci. Jednotlivé požadavky pro dané třídy se postupně zpřesňují a tvoří hierarchii s třídou *D* jako prvkem nejnižším a s třídou *A1* jako prvkem nejvyšším. Praktického užití se dostává především skupinám *B* a hlavně *C*, neboť třída *D* zahrnuje prostě produkty, které byly podrobeny hodnocení s užitím *TCSEC*, ale které nedosáhly žádné z vyšších tříd. Třída *A1* stanovuje požadavky, které jsou pro většinu produktů z finančních důvodů nerealizovatelné. Např. dobře zkonstruovaný systém *Unix* se pohybuje na úrovni *C1*, po určitých úpravách jej lze dostat na úroveň *C2*. Pro přechod do vyšší úrovně by bylo třeba vynaložit skutečně velké úsilí a náklady.

Nová kritéria *Federal Criteria for Information Technology Security (FC)* jsou vyvíjena ve spolupráci *National Security Agency (NSA)* a *National Institute of Standards and Technology (NIST).*

Information Technology Security Evaluation Criteria (ITSEC). S ohledem na neorganizovaný vývoj a aktivity v EC, rozdílná vládní a komerční kritéria v Británii, jiná kritéria ve Francii i v Německu, došlo ke shodě vlád těchto zemí a Nizozemí. Výsledkem byla později formulovaná kriteria *ITSEC*. Ta přinesla změnu v podobě zavedení možnosti hodnocení celých systémů, tedy nejen jednotlivých produktů. Hlavně však uvedla dvě dimenze pro hodnocení systémů - funkčnost (popisující funkční rysy) a záruky (poskytující nové měřítko pro celkové obecné hodnocení efektivnosti a správnosti zajištění bezpečnosti). Kritéria *ITSEC* s třídami *E0* (nevyhovující) až *E6* (maximálně vyhovující) jsou skutečně vynikajícím nástrojem a měřítkem ve své dimenzi záruky. Požadavky na bezpečnostní služby i architekturu jsou precizně specifikovány stylem odpovídajícím některým náročným modelům bezpečnostní politiky, resp. směrnic. Na druhé straně ale kritéria *ITSEC* neposkytují mnoho informací pro hodnocení prvků funkčnosti a vzhledem k době svého vzniku by mohla věnovat více pozornosti sítím. Funkční třídy jsou uvedeny spíše jako příklady a je možné je dále doplňovat a rozšiřovat - existuje např. třída pro čipové karty. V roce 1993 došlo k doplnění *ITSEC* o metodologickou příručku pro hodnocení - *Information Technology Security Evaluation Manual (ITSEM).*

Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), kanadská kritéria. V roce 1989 byla vydána první verze kanadských kritérií *CTCPEC,* jejichž současná verze poskytuje velice kvalitní měřítko pro hodnocení bezpečnosti a tato kritéria jsou podle [122] nejpropracovanější podobou kritérií ve skutečně použitelné podobě. Podobně jako *ITSEC*, jsou i kanadská kritéria rozdělena na dvě části - funkčnost a záruku. Funkčnost je v

kanadských kritériích dále dělena do čtyř částí, které také odpovídají čtyřem základním skupinám požadavků na bezpečnost informačních technologií. Je to

-důvěrnost (požadavky na omezení odhalení informačního obsahu),

-integrita (požadavky na omezení modifikace informací),

-dostupnost (požadavky na zajištění přístupu autorizovaných osob k ochraňovanému systému a na zajištění procesů s tím souvisejících),

-zodpovědnost (požadavky na sledování a řízení přístupu k systému).

Takto definované oblasti pak přímo specifikují možné hrozby a prvky běžné zranitelnosti systémů. Každá z oblastí se skládá z několika služeb, které mohou sloužit jako protiopatření k zajištění bezpečnosti. Tento rys, přímé adresování služeb jako protiopatření k možným hrozbám, je typickým rysem kanadských kritérií. Rozpracování záruk je v *CTCPEC* v podstatě doplněním některých praktických požadavků a detailů k *ITSEC*. Vlastní klasifikace do tříd je pak dána označením *T0* (nevyhovující) až *T7* (zahrnující formální model návrhu hodnoceného bezpečnostního systému a jasný popis návaznosti praktické implementace a zvoleného designu). Jako nezávislá část kanadského systému hodnocení bezpečnosti byla současně s *CTCPEC* vydána kritéria pro hodnocení *kryptografických modulů*.

Společná kritéria. V zájmu praktické realizace zájmů zainteresovaných stran v Severní Americe a v Evropě, zástupci Evropských společenství, Kanady a Spojených států se shodli na vývoji *Společných kritérií -Common Criteria (CC).* Podle [122] jsou však tato kriteria příliš obsáhlá, návrh *CC* ve verzi 0.9 čítal přibližně 850 stran dokumentace. Podle názorů německé strany se výsledný návrh stal příliš rozsáhlým, čtenáři, zvláště zákazníci a pořizovatelé nebudou schopni jej číst a rozumět mu jako celku. Odborná veřejnost také kritizovala povrchní zpracování hodnocení kryptografických mechanismů, jemuž se nedostalo patřičné pozornosti pro individualistické zájmy vlád některých zemí, především vlády USA. Společná kritéria v následující verzi 1.0 byla poněkud uvolněna začátkem roku 1996. Bohužel nejsou však v této verzi stále dokončena.

Jak uvádí [122], kritéria byla, jsou a zůstanou velmi důležitou problematikou bezpečnosti informačních technologií. Jejich existence

-usnadňuje aplikaci a použití informačních technologií s bezpečnostními prvky;

-poskytuje měřítko k hodnocení a srovnávání;

-umožňuje jednodušší specifikaci požadavků při pořizování prostředků informačních technologií;

-napomáhá při návrhu a vývoji nových technologií, kdy kritéria slouží jako pomocný ukazatel;

-nepřímo napomáhá zvyšování bezpečnosti nově konstituovaných systémů a tím i omezování deliktů typu informační či počítačové kriminality.

**

Standardy bezpečnosti informačních technologií usnadňující vytváření bezpečného systému. Doposud jsme se věnovali standardům, umožňujícím *zhodnotit* bezpečnost systémů

informačních technologií; nyní k těm, které usnadňují *vytváření* bezpečného systému. Existuje mnoho kategorií standardů, též nazývaných normy, zabývajících se tvorbou bezpečných informačních systémů. Jde o standardy mezinárodní, kontinentální, např. evropské standardy, regionální, národní standardy, standardy státní správy některého státu, standardy určitého zájmového sdružení nebo průmyslové standardy. Význam každého z těchto standardů zcela závisí na rozsahu jeho použití. Obecně lze říci, že jsou významným nástrojem prevence v boji s počítačovou, resp. informační kriminalitou. Podle [65], rozsah jejich použití nemusí vždy odpovídat úmyslům tvůrců standardu. Známe mnoho případů, kdy ambiciózní standardy upadly v zapomnění, nebo kdy původně zcela opomíjený standard dosáhl celosvětového významu. Zpravidla však platí, že nejširší platnost mají standardy mezinárodní a regionální. Použití národních standardů a standardů státní správy zpravidla nepřesahuje hranice státu, ve kterém byly tyto standardy vytvořeny. Výjimkou z tohoto pravidla jsou národní standardy USA (označované ANSI) a standardy státní správy USA, které jsou někdy používány i mimo hranice USA.

Mezinárodní standardy ISO/IEC patří k nejdůležitějším mezinárodním standardům v oblasti bezpečnosti informačních systémů. Mezinárodní organizace pro standardizaci *ISO (International Organization for Standardization)* je mezinárodní federací národních standardizačních orgánů. Mezinárodní elektrotechnická komise *IEC (International Electrotechnical Commision)* je organizace, která se věnuje standardizaci v oblasti elektrotechniky a elektroniky a úzce spolupracuje s organizací *ISO*. V roce 1987 vytvořily *ISO* a *IEC* společný technický výbor, který vytváří standardy v oblasti informačních technologií a který je nyní také zodpovědný za většinu standardů *ISO/IEC* v oblasti bezpečnosti informačních technologií. Technický výbor je složen z několika podvýborů, které se zabývají standardizací v různých oblastech informačních technologií. Tento výbor se však nezabývá standardy pro zabezpečení informačních technologií v bankovnictví. Této činnosti se věnuje speciální technická komise, která vytváří standardy pro zabezpečení bankovních a jiných finančních služeb.

Současné standardizační aktivity ISO/IEC v oblasti obecné bezpečnosti informačních technologií zahrnují projekty

-bezpečnostní architektury otevřených systémů a bezpečnostních zásad,

-zabezpečení vyšších a nižších vrstev otevřených systémů,

-bezpečnostních mechanismů informačních technologií,

-kriterií pro hodnocení bezpečnosti informačních technologií.

Mimo to *ISO/IEC* vyvinuly a vyvíjejí standardy pro zabezpečení informačních technologií ve specializovaných oblastech. Jsou to standardy

-pro čipové karty,

-pro zabezpečení speciálních systémů podle požadavků uživatelů,

-pro zabezpečení adresářových služeb,

-pro vynucení obecných bezpečnostních požadavků,

-pro zabezpečení informačních technologií v bankovnictví,

-pro budování bezpečnostní architektury bankovních systémů s čipovými kartami.

Standardy *ISO/IEC* nejsou na síti Internet přímo dostupné. Informace o nich lze však zde získat, společně ještě s pojednáním o aktivitách jednotlivých standardizačních komisí a podvýborů a o stavu jednotlivých standardů.

Mezinárodní telekomunikační standardy CCITT/ITU jsou důležitým prostředkem prevence informační kriminality v oblasti přenosu dat. *Mezinárodní telekomunikační unie ITU (International Telecommunication Union)* je mezinárodní organizace zabývající se standardizací v oblasti telekomunikací a v současné době reprezentuje více než 170 zemí. Mezi aktivity *ITU* patří též tvorba standardů, nazývaných *doporučení*. Organizace *ITU* převzala původně údržbu dřívějších standardů *CCITT* a nyní vyvíjí i standardy nové, které se zabývají výhradně bezpečností otevřených systémů. Tyto standardy mají označení *X.8xx*. Podle [65], nejvýznamnějším z nich je patrně standard *X.800*, týkající se bezpečnostní architektury otevřených systémů. Z něho pak vychází většina dalších standardů této řady. Bezpečnosti se týkají i některé jiné standardy, jako např. *X.509*, který definuje strukturu certifikátů pro kryptografii veřejným klíčem a který dnes využívá většina systémů pracujících s kryptografií pomocí veřejného klíče.

Standardy bezpečnosti informačních technologií v USA. Hlavní standardizační organizací v USA je *Americký národní ústav pro standardizaci (ANSI, American National Standards Institute)*, který koordinuje vývoj standardů v USA. *ANSI* má několik akreditovaných standardizačních výborů, zabývajících se standardizací i v oblasti bezpečnosti informačních technologií. Jde především o výbor pro systémy zpracování informací, který vydává obecné standardy z oblasti informatiky, dále výbor pro finanční služby, vydávající standardy z oblasti bankovnictví a konečně výbor pro elektronickou výměnu obchodních dat. Tyto výbory vydaly v minulých letech značné množství standardů, které mají vztah k bezpečnosti informačních systémů a především ke kryptografii. Mnohé z nich jsou využívány i mimo USA a některé rovněž sloužily jako předloha při vytváření standardů mezinárodních. Podle [65], z nich nejznámější je standard definující autentizaci zpráv v bankovnictví, standard vymazující správu kryptografických klíčů v bankovnictví, standard pro kryptografické zabezpečení bankovních zpráv a některé další pro algoritmy při kryptografii veřejným klíčem.

Státní správa USA, resp. federální orgány, věnují také značnou pozornost standardizaci v oblasti zabezpečení informačních technologií. Její standardy se nazývají *FIPS (Federal Information Processing Standards)* a jsou vydávány organizací *NIST (National Institute of Standards and Technology)*. Platnost standardů *FIPS* je omezena pouze na federální orgány USA. Značný význam těchto standardů však spočívá v tom, že v těchto standardech se obvykle poprvé objeví výsledky aktivit státní správy USA v oblasti prevence počítačové bezpečnosti. Teprve později jsou mechanismy, publikované ve standardech *FIPS*, standardizovány ve standardech *ANSI* nebo i v mezinárodních standardech. V publikacích *FIPS* se například poprvé objevily standardy, které souvisely s kryptografickými algoritmy a které byly vytvořeny státní správou USA. V USA existuje mimo standardizační aktivity státní

správy také několik aktivit průmyslových firem, které vytvářejí tzv. průmyslové standardy. V oblasti kryptografie je nejznámější z těchto průmyslových standardů série snažící se pokrýt podstatnou oblast kryptografie veřejným klíčem.

Evropské standardy bezpečnosti informačních technologií. Evropské sdružení pro standardizaci *CEN (Comité Européen de Normalisation)* vyvíjí evropské standardy v mnoha oborech, včetně oborů elektrotechnických. Některé standardy *CEN* se zabývají také bezpečností informačních systémů, především systémů otevřených a dále aplikovanou kryptografií, například v oblasti systémů s čipovými kartami. Jinou evropskou standardizační institucí je *Sdružení evropských výrobců počítačů ECMA (European Computer Manufacturers Association)*. Sdružení *ECMA* je nezisková organizace, jejímiž členy jsou evropské firmy, které vyvíjejí, vyrábějí a prodávají hardware a software. Sdružení vydalo přes dvě stovky standardů informačních technologií a technických zpráv, které byly často použity jako podklady pro tvorbu *ISO/IEC* a *ITU* standardů. Organizace *ECMA* je aktivní především v oblasti otevřených systémů a standardy v oblasti bezpečnosti informačních systémů se zabývá její technický výbor.

Bezpečnostní standardy pro Internet. Provoz sítě Internet je silně závislý na komunikačních standardech, zajišťujících propojení jednotlivých uzlů sítě. Proto je standardizace v síti Internet jedním z jejích nejdůležitějších elementů. Orgánem zodpovědným za architekturu, rozvoj a správu sítě je tzv. *Internet Activities Board (IAB).* Tento orgán delegoval zodpovědnost za tvorbu a vývoj standardů pro síť Internet na orgán zvaný *Internet Engineering Task Force (IETF).* Personální obsazení *IETF* není založeno na existenci formálních zástupců jednotlivých organizací, jako tomu bývá u jiných standardizačních orgánů, ale na individuálním členství jednotlivců s vysokou odbornou úrovní. Proces standardizace do značné míry závisí na duchu spolupráce mezi jednotlivými účastníky. Standardy pro Internet jsou publikovány v publikacích, zvaných *Request for Comments (RFC).* Ve standardech *RFC* je specifikována většina běžně používaných bezpečnostních protokolů sítě Internet. Těchto standardů je velké množství, týkají se bezpečných komunikačních protokolů, definují zabezpečení zpráv elektronické pošty, specifikují platební protokoly, strukturu bezpečnosti zasílaných zpráv atd. Dokumenty *RFC* je možno získat na mnoha serverech v síti Internet.

Jak uvádí autor studie [65], situace v oblasti standardů pro vytváření bezpečných informačních systémů je ještě nepřehlednější než u standardů pro hodnocení bezpečnosti. Světový trend však jednoznačné směřuje ke standardizaci bezpečnostních mechanismů. Nestandardizovaná proprietární (tj. naše vlastní) řešení jsou ve většině oblastí odmítána zejména pro nedostatečné záruky účinnosti prevence v boji s počítačovou kriminalitou. Přestože vývoj bezpečnostních mechanismů, odpovídající standardům, bývá někdy nákladnější než přímočará intuitivní řešení, vložené náklady se bohatě vrátí při instalaci, údržbě a hlavně při modifikacích informačního systému, nehledě navíc ke generálně preventivním účinkům při omezování počítačových deliktů.

**

Kryptografie je jedním z velmi účinných nástrojů prevence informační kriminality. Kryptografii lze řadit do oblasti problematiky počítačové bezpečnosti, speciálně pak sehrává důležitou roli při realizaci záměrů informační bezpečnostní politiky. Vychází z jednoduchého požadavku komunikujících stran, totiž z toho, že někteří uživatelé výpočetní techniky a síťového spojení potřebují sdílet utajené informace, aby dosáhli společného cíle. Případně chtějí spojit své možnosti, aniž by žádná z komunikujících stran seznámila ostatní se svou informací, nebo jedna ze stran chce přesvědčit ostatní, že je jí známá nějaká tajná informace, aniž by ji zveřejnila apod. Nejjednodušším příkladem takové komunikace může být přenos elektronické pošty, kdy je odesílaná zpráva zašifrována veřejným klíčem příjemce, a proto ji může dešifrovat pouze on. V takovém případě hovoříme o komunikačním styku pomocí kryptografického protokolu. Připomeňme, že podle studie [154], kryptografický protokol je posloupnost operací, určená pro komunikaci mezi různými stranami a využívající kryptografické transformace. Konkrétní kryptografický protokol vychází z požadavků komunikujících stran a při jeho dodržení by mělo být zajištěno splnění všech předem daných požadavků. Kryptografický protokol specifikuje, jakým způsobem každá strana vysílá, přijímá a odpovídá na zprávy, a to včetně chybných nebo ilegálních zpráv. Protokol může rovněž specifikovat požadavky na definici prostředí, jako je např. nastavení knihovny veřejných klíčů. Strana, která se řídí protokolem, bude ochráněna proti specifikovaným nebezpečím i v tom případě, že ostatní strany se protokolem neřídí. Účelem protokolu je např. výměna kryptografických klíčů pro následný přenos šifrovaných dat, autentizace účastníků protokolu, generování kryptografických klíčů atd. Ovšem příjemce neví, zda mu tuto zprávu zasílá přítel či nepřítel, který se za něj vydává. Proto je vhodné na nezašifrovanou zprávu použít soukromý klíč odesilatele a pak veřejný klíč příjemce. Pak příjemce následovně dešifruje zprávu svým soukromým klíčem a veřejným klíčem odesilatele. Spolehlivost této metody je založena na důvěryhodnosti správce veřejných klíčů. Totéž platí samozřejmě u určení příjemce. Falešný příjemce, který by získal přístup na server důvěryhodné instituce a zaměnil by veřejný klíč správného příjemce svým veřejným klíčem, by mohl číst zprávy určené správnému příjemci.

Silná kryptografie. Ve shodě se studií [73], jako silné šifry jsou obecně označovány takové šifry, které jsou schopny odolat všem formám kryptoanalýzy s výjimkou tzv. útoku hrubou silou, tj. útoku s vyčerpáním všech možných hodnot klíčů. Obranou proti tomuto typu útoku je výběr šifry, která má tak velký prostor pro klíče, aby se vyčerpávající prohledávání uskutečnilo v čase, který není realizovatelný, nebo jak se často říká, aby bylo výpočetně neproveditelné. Obecně je za silnou kryptografii považována kvalitní symetrická šifra (oboustranně aplikovatelná) s dostatečnou délkou klíče. Úprava dostatečné délky není pojímána ve všech státech jednotně. Charakteristickým příkladem produktů silné kryptografie je šifrovací algoritmus *DES*, v posledních dvaceti letech nejvíce studovaný. Jeho konstrukcí se zde nebudeme zabývat, neboť jde o ryze technický problém. Metody schopné prolomit *DES* jsou i dnes velmi obtížně dostupné a drahé, takže tento systém při realizaci bezpečnostní politiky je ve světě hojně využíván, včetně jeho modifikovaných verzí. Jak uvádí [73], studie expertů *Japonské národní banky* a *Yokohamské národní univerzity* z roku 1996 jej považují za bezpečný systém asi tak do poloviny příštího století. Tento názor na délku časového intervalu

spolehlivosti byl poněkud upraven (k roku 2020) s přihlédnutím k důsledkům dvou speciálních útoků, při nichž došlo k narušení systému. Je zajímavé, že různé „odborné“ články v našem tisku, které s cílem propagovat vlastní bezpečnostní algoritmy, šíří neúplné informace o údajně „vyřízeném“ systému *DES,* blíže k tomu viz [73].

Některé speciální typy kryptografických protokolů. Podle [154] přichází v úvahu zejména

-protokol typu *stále uzavřené truhly,* který spočívá v tom, že odesilatel zašifruje zprávu svým klíčem a odešle ji příjemci, příjemce totéž provede se zašifrovanou zprávou svým klíčem a odešle odesilateli; odesilatel dešifruje tuto zprávu a obdrží svou původní zprávu zašifrovanou klíčem příjemce; takto zašifrovanou zprávu odešle příjemci, který ji následně dešifruje svým klíčem a obdrží původní zprávu odesilatele; to vše lze realizovat za předpokladu, že operace šifrování a dešifrování jsou pro všechny účastníky protokolu vzájemně záměnné a účastníci se mohou přesvědčit o své identitě;

-*hod mincí po telefonu,* což je protokol, který se týká náhodného výběru ze dvou variant odeslaných zpráv, zašifrovaných symetrickým (oboustranně známým) klíčem; příjemce vybere jednu ze zpráv a dále pokračuje podle předchozího protokolu; na konci protokolu příjemce přečte otevřenou zprávu týkající se zvolené varianty a oba aktéři si pro kontrolu po telefonu sdělí své tajné klíče;

-*protokol s nulovým rozšířením informací* je dvoustranný protokol; jedna strana je tzv. dokazovatel, druhá prověřovatel; dokazovatel zná nějakou skutečnost a přeje si přesvědčit pomocí protokolu prověřovatele o této skutečnosti; prověřovatel se chce pomocí protokolu přesvědčit o platnosti této skutečnosti právě tehdy, když je tato skutečnost pravdivá; přitom si dokazovatel nepřeje podat žádnou informaci o podstatě skutečnosti; základními příklady tohoto protokolu jsou schopnost faktorizovat nějaké přirozené číslo či schopnost nalezení řešení nějakého matematického problému v reálně efektivním čase;

-protokol typu *jeskyňka* je obvyklým jednoduchým příkladem protokolu s nulovým rozšířením informací; dokazovatel má přesvědčit ověřovatele, že zná heslo k tajným dveřím rozdělujícím kruhovitou jeskyni na pravou a levou část, přičemž vchod pro obě části je společný; dokazovatel vejde do náhodné části jeskyně tak, že prověřovatel, který stojí mimo jeskyni nevidí, do které části vešel; prověřovatel pak vejde do vchodu jeskyně a zavolá na dokazovatele stojícího již u uzavřených dveří, kterou částí má k němu přijít; zná-li dokazovatel tajné heslo, může vždy správně vyjít; nezná-li ho ale, má pouze 50% šanci, že vešel do správné části a po dostatečném počtu opakování výše uvedeného postupu prověřovatel zjistí, že klamal; navíc prověřovatel nemůže ubezpečit nikoho jiného než sebe, že dokazovatel tajné heslo zná.

Praktický význam kryptografických protokolů. Při zběžném pohledu by se zdálo, že uvedené protokoly jsou spíše logickými hříčkami, než praktickými nástroji v boji s informační kriminalitou. Že tomu tak není, může napovědět příklad praktické verze protokolu s nulovým rozšířením informací při identifikaci kreditní karty či počítačového hesla systému s citlivými či přísně tajnými informacemi. Zde totiž dokazovatel může dokázat, že je pověřenou osobou, aniž by prověřovateli, který může hrát falešně, sdělil své heslo či jinak přenechal informaci,

jak za sebe vystupovat. Rovněž společensky velmi významnou roli může sehrát kryptografie při demokratických volbách, při zajišťování ideálního způsobu jejich realizace, aby byly bezpečné a odpovídaly požadavkům na ně kladeným. Protokol tradičního volebního systému je velmi jednoduchý. Korektnost voleb je zajištěna tím, že každý volič je při příchodu do volební místnosti pozitivně identifikován na základě občanského průkazu, resp. znalostí člena volební komise a v průběhu voleb je vytvářen záznam těch voličů, kteří již odvolili. Tajné hlasování je zajištěno volební plentou, nikdo nemůže vidět, jak který volič volí, až na speciální, zákonem předem stanovené případy, např. při volebním aktu invalidů ap. Prověřitelnost výsledku voleb by měla být zajištěna opětovným sečtením volebních lístků, které by měly být do konce určitého období uschovány a nepřístupné. Spojení mezi voličem a volební obálkou je ukončeno po vložení obálky do urny. Volební obálky jsou otvírány jako celek. Jediným spojením s voličem je tedy lokální volební místnost a počet hlasů, které byly na základě příslušné komise sečteny. Bohužel, je dobře známo, že se během existence tohoto protokolu vyskytly různé typy podvodů. Např. sdělení volebních komisí při sčítání neodpovídala skutečnosti. Jiná, inteligentnější možnost spočívá v tom, že volební lístky se počtem a jmény kandidátů neliší, zato ale jejich pořadím. Lze tedy na základě volebního lístku identifikovat příslušného voliče. Pokud by se volby uskutečnily pomocí počítačové sítě, pak jako hlavní požadavky vystupují zároveň požadavek legitimity a požadavek utajení. To jsou zdánlivě dva zcela nesourodé požadavky, protože jak může být zajištěno utajení, když se volič musí prokázat? Autor studie [154] popisuje dvě hlavní metody řešení tohoto problému. První způsob je založen na zašifrování jinak veřejně uskutečněné volby. Jednotlivé volby pak nesmí být dešifrovatelné, ale musí umožňovat celkovou sumarizaci volebních hlasů. Druhou možností je realizace voleb anonymních, ale společně s důkazem oprávnění pro daného občana volit. Toto oprávnění by měla poskytovat předem příslušná volební komise. Z důkazu oprávnění by ovšem nesměla být umožněna identifikace voliče. Zároveň voliči nesmí být schopni samostatně vytvořit důkaz oprávnění.

Otázky dokazování bezpečnosti protokolů. Je obvykle velmi obtížné předložit exaktní důkaz bezpečnosti protokolu jak samotného, tak i v závislosti na použití šifrovacího systému. To bývá celkem dobře známo při analýze obvyklých algoritmů. Případ kryptografických protokolů navíc v sobě zahrnuje to, že každý z účastníků má jistou exekutivní sílu a usuzovací schopnosti, závisející na předtím obdržených informacích. Tím se celý proces dokazování stává ještě náročnějším. Přitom je potřebné, aby každý navržený protokol byl zkoumán co nejpodrobněji, aby byla nalezena jeho případná slabá místa, která potenciálně umožňují jeho obcházení či zneužití. Proto byly vypracovány speciální metody dokazování správnosti a síly protokolu. Bez ohledu na to lze říci, že vhodně utvořené protokoly nám zajistí bezpečnější a důvěryhodnější komunikaci.

Kryptografická rozhraní. Služby kryptografie jsou využívány ve stále větším počtu nejrůznějších aplikací. Jsou potřebné např. pro zajištění služeb, jako je důvěrnost a integrita zpracovávaných dat, autentizace, neodmítnutelnost atd. S tím vyvstává otázka jak dosáhnout optimálního propojení kódu aplikace s moduly implementujícími jednotlivé kryptografické funkce. Podle [158] implementace kryptografických funkci může být integrována přímo do kódu aplikace. To ovšem s sebou přináší určité nevýhody: Změna kteréhokoli člena dvojice

typu *„aplikace - kryptografické moduly“* znamená zásah do celého systému. Navíc ne každý tvůrce softwaru je odborníkem na kryptografii. Proto se zpravidla odděluje aplikace a její vývoj od implementace kryptografických mechanizmů. Hledají se cesty jak standardizovat volání bezpečnostních služeb v aplikacích, aby použití kryptografických procesů bylo co nejvíce schůdné i pro méně zasvěceného uživatele. Proto byla vyvinuta *kryptografická rozhraní,* která z hlediska počítačové kriminality chápeme jako účinný prostředek prevence v rámci informační bezpečnosti.

Základní typy aplikací kryptografických rozhraní. Jak uvádí autor studie [158], stejně jako se liší požadavky různých aplikací na zajištění bezpečnosti a úroveň přístupu ke kryptografickým funkcím, liší se i jednotlivá kryptografická rozhraní. Aplikace využívající služby kryptografie můžeme rozdělit do dvou skupin na

-aplikace bez povědomí o kryptografii, kdy jde o případy s omezeným systémem volání kryptografického rozhraní pro ochranu dat; typickým příkladem je textový editor, poštovní agent, ap.; do této kategorie patří většina aplikací;

-aplikace s povědomím o kryptografii, které potřebují množinu volání umožňujících přístup ke kryptografickým modulům s možným maximem jejich kontroly; příkladem takové aplikace může být server certifikační autority.

Na tom, do které z uvedených skupin aplikace patří, závisí rozhodnutí o typu rozhraní, které bude při implementaci použito. Izolace kódu aplikace od kryptografických služeb přináší výhody jak při vývoji aplikací, tak při jejich následném nasazení a údržbě. K výhodám lze počítat především

-modularitu software spočívající v oddělení rozdílně zaměřených částí systému; tato vlastnost je společná pro všechna programová rozhraní;

-nezávislost na použitém bezpečnostním mechanizmu; použitím různých kryptografických modulů, implementujících různé kryptografické funkce, může každá aplikace využívat kryptografické funkce o různé síle v závislosti na prostředí, ve kterém je nasazena;

-skutečnost, že vývojoví pracovníci nejsou zatěžováni detaily kryptografických funkcí; aplikace neobsahuje vlastní implementaci kryptografických algoritmů;

-oddělení vývoje aplikací od vývoje bezpečnostních mechanizmů nižších vrstev; vývojáři aplikací mohou při použití standardních rozhraní používat kryptografické moduly dodané třetí stranou; naopak je možné vyvíjet a nabízet samostatné kryptografické moduly implementující požadované algoritmy.

Aplikace, které nemají implementovány kryptografické funkce, ale využívají volání kryptografického rozhraní, se mohou vyhnout exportním omezením na vývoz silné kryptografie. V exportní verzi aplikace může být kryptografický modul nahrazen modulem podporujícím pouze kryptografické funkce o síle, která nepodléhá exportním omezením. Tento způsob obcházení exportních omezení z USA se sice dříve také zakazoval, ale v současné době s tím už, až na jisté výjimky, nebývají problémy.

Konkrétní kryptografická rozhraní. Kryptografických rozhraní existuje mnoho, můžeme je rozdělit v závislosti na jejich určení podle klasifikace použité v projektu *ICE (International Cryptography Experiment).* Autor studie [158] je dělí na

-rozhraní pracující na vysoké úrovni abstrakce s určením pro přístup k bezpečnostním službám, jako je autentizace, integrita, důvěrnost, řízení přístupu, nepopíratelnost, které poskytují speciální bezpečnostní mechanizmy; mezi ně je možno zařadit *Generic Security Services API (GSS-API), Microsoft Security Provider Interface (SSPI),* vyšší funkci rozhraní *Microsoft CryptoAPI, Common Secutity Services Manager API (CSSM API),* jako konkrétní případy rozhraní typu *SSAPI (Security Service APIs)*;

-rozhraní určené pro pomocné bezpečnostní funkce, *SSSAPI (Security Support Service APIs)*, zajišťující služby jako je management certifikátů a klíčů, autentizace, depozitování a obnova klíčů atd.;

-rozhraní určená pro přístup ke kryptografickým modulům, *CAPI (Cryptographic APIs);* v kryptografických modulech jsou implementovány samotné kryptografické algoritmy; kryptografické moduly mohou být jak softwarové, tak hardwarové, sem patří např.: *Labs Crypto Token Interface (RSA), Microsoft CryptoAPI, Common Security Services Manager API (CSSM).*

Zkušenosti s doporučenými rozhraními. Na míře kryptografického povědomí aplikace závisí i rozhodnutí jaké rozhraní při implementaci použít. *NSA - Agentura pro národní bezpečnost* vytvořila tým, který vydává doporučení pro výběr a použití kryptografických rozhraní. Týká se ochrany spojově orientované komunikace, ochrany dat, nabídek služeb vyšší úrovně, jako jsou management klíčů nebo obnova klíčů, podpory šifrování a digitálního podpisu, autentizace a managementu certifikátů, přístupu ke kryptografickým modulům atd. Některá z doporučených rozhraní vyžadují vysokou úroveň povědomí o kryptografii, poskytují však jako protihodnotu vysokou míru bezpečnosti. Čím je rozhraní obecnější, tím více využívá omezenou množinu volání. Nevýhodou je pak omezení možnosti ovlivnění práce takového kryptografického zařízení, které je vhodné pro běžné aplikace, aplikace bez povědomí o kryptografii. Naopak málo abstraktní rozhraní vyžaduje od aplikace detailní znalost problematiky kryptografie a použitých zařízení. Tím se ovšem také zvyšuje nebezpečí, že dojde k ohrožení bezpečnosti systému způsobenému chybou při vývoji aplikace. Vzato z druhé strany, tato rozhraní nabízejí větší možnosti práce s kryptografickými funkcemi a tedy naopak spolehlivost větší z hlediska útoku zvenčí. Podle [158], v praktickém provozu u většiny aplikací není potřebná příliš vysoká úroveň kryptografického povědomí. Neustálý vývoj aplikací a stále probíhající prudké změny v oblasti kryptografie vyžadují nezbytnost použití standardních kryptografických rozhraní, zvláště u velkých projektů s předpokládanou dlouhou dobou životnosti. Jejich absence či podcenění při vývoji se může po několika letech provozu, například při změně požadavků na bezpečnost, velmi vymstít. Dobré kryptografické rozhraní v rámci bezpečnostní politiky není sice pro fungování většiny systémů nezbytné, ale z hlediska prevence počítačové, resp. informační kriminality je velmi významným nástrojem.

Export kryptografie. Masové rozšíření Internetu a potřeba řídit bezpečné elektronické obchodování s sebou přinesly potřebu větší dostupnosti *kryptologie*. Dodnes je ale s exportem

šifrovacích produktů mnohde zacházeno jako s exportem zbraní. „Silná“ kryptografie často představuje významnou zbraň, schopnost dešifrování komunikace může rozhodnout výsledek konfliktu. Jak uvádějí autoři studie [73], vládní zájmy se zde převážně soustřeďují

-na jistoty, že používání kryptografických systémů nesníží schopnost stíhání a dopadnutí nežádoucí osoby či skupiny osob,

-na zajištění toho, aby používání kryptografických systémů nepůsobilo proti národním zájmům dané země.

Podle [73] dění v oblasti informačních technologií většinou znamená dění v USA, o kryptografii ani nemluvě. Americká vláda považuje šifrování za stejně nebezpečnou technologii jako zbraně. Často se uvádí, že si americká vláda prostě nepřeje uvolnit mimo zemi technologie, které by jí mohly ztížit sběr zpráv, či stíhání organizovaného zločinu. Informace posílané Internetem nebo jinými otevřenými sítěmi lze velmi jednoduše filtrovat a analyzovat, týká se samozřejmě i zpravodajských aktivit. Některé firmy reagují tak, že ze svých produktů šifrování úplně odstraní. Nebo mají dvě verze a do zahraničí prodávají tu bez šifrování. Mohou mít také jednu verzi s klíčem, která není určena pro export a druhou exportní, s klíčem efektivně omezeným. Účastníci mohou použít také specifického klíče jen k podpisu a nikoliv k šifrování. Podpis zprávy je pak bezpečný dokonce i před protivníkem, kterému se podaří prolomit i ostatní tajné klíče používané pro zašifrování zprávy. Podle [73] exportní omezení ze strany USA stojí americké prodejce miliardy dolarů. A omezení exportu americkou vládou stále komplikuje bezpečnou mezinárodní komunikaci mnohým firmám, protože asi 60% kryptografických produktů se vyrábí v USA, nehledě k množství dalšího užitečného softwaru, který je dnes často kryptografií přímo přeplněn. Někteří prodejci, aby obešli exportní omezení, vyvíjejí šifrovací algoritmy mimo USA. Kolem exportu kryptografie v USA vznikly dokonce soudní pře, vedoucí např. k možnostem volného vývozu zdrojových kódů programů.

Export kryptografie ve většině vyspělých zemí je kontrolován. Všeobecně jsou z takové kontroly vyňata kryptografická zařízení, která umožňují pouze kontrolu integrity. Mezi země, kde není kontrola exportu aplikována, patří Belgie, Dánsko, Finsko, Maďarsko, Irsko a Španělsko. Např. z Británie lze vyvážet kryptografická zařízení pro nekomerční účely bez omezení, ale v případě komerčních produktů vývoz podléhá pravidlům kontroly exportu. Do Kanady lze produkty z USA vyvážet bez omezení, ale z Kanady nelze jednoduše reexportovat americké produkty se silným šifrováním, kdežto obdobné kanadské produkty do zahraničí dodávat lze. Mnozí počítačoví odborníci pamatují působení mezinárodní organizace pro vzájemnou kontrolu exportu strategických produktů a technických dat z členských zemí *COCOM (Coordinating Committee for Multilateral Export Controls).* Ta měla mimo jiné bránit tomu, aby citlivé technologie, včetně silné kryptografie, byly dodávány do zemí východního bloku. Udržovala mezinárodní seznam vybraných citlivých produktů, které této exportní kontrole podléhaly. V roce 1994 byla rozpuštěna s tím, že Rada Evropy připraví podrobné exportní směrnice pro Evropskou unii, obsahující rovněž seznam zboží „dvojího užití“. V tomto seznamu jsou zahrnuty i kryptografické produkty a jejich vývoz proto podléhá zvláštní autorizaci. Vybraným zemím, které nejsou členy EU, může být uděleno generální

oprávnění k exportu. Jedná se o Austrálii, Kanadu, Japonsko, Norsko, Švýcarsko a USA. První diskuse o nahrazení *COCOM* se uskutečnila ještě v roce 1994. Kromě členů NATO a tří nových členů EU byli přítomni zástupci Ruska, České republiky, Maďarska, Polska a Slovenska. Navržený nový orgán byl neformálně nazván *Nové fórum,* a bylo odsouhlaseno ustanovení tzv. *Wassenaarské dohody* o exportních kontrolách konvenčních zbraní a zboží a technologií „dvojího užití". *Nové fórum* se následně sešlo ve Wassenaaru a v dubnu 1996 se uskutečnila jeho první plenární schůze ve Vídni. Nový režim kontroly exportu má dvě větve, týkající se konvenčních zbraní a zboží dvojího užití. Díky Wassenaaru lze dnes stahovat z Internetu např. kanadské produkty se silným šifrováním. Nutno však říci, že přetrvávající nejednotnost zákonných ustanovení a předpisů v jednotlivých zemích, přispívá ještě stále k možnostem páchání specifických deliktů v této oblasti. Je sporné nakolik tyto činy patří do oblasti počítačové kriminality, či do sféry obchodního práva.

Incidenty v oblasti počítačové bezpečnosti. Významnou možnost zvýšení bezpečnosti produktů s kontrolou exportu ukazuje příklad *WWW* serverů a prohlížečů *Netscape.* Systém *Netscape* je v současné době distribuován po celém světě a je předmětem kontroly exportu USA, co se týče kryptografie a délky klíčů. Všechny verze *Netscape* mají zabudovanou podporu *SSL (Secure Sockets Layer)*. Koncem roku 1995 byla zpochybňována bezpečnost exportní verze *SSL* s ohledem na tři incidenty, ke kterým došlo. Při prvním incidentu se podařilo jednomu francouzskému studentovi prolomit během pěti dnů klíč relace, používaný v mezinárodně dostupné verzi *Netscape*. Další incidenty měly za následek snížení pětidenního limitu prolomení. Ten se podařilo několika členům skupiny *„Cyberpunks"* zkrátit až na pouhých 31 hodin. Vysvětlení těchto incidentů spočívá ve vyjasnění závěru, že příslušné klíče nejsou dosti silné. Možné řešení v těchto případech spočívá v úpravě klíčů, případně síly šifrování. Blíže k tomu viz [73].

Vývoj situace v expertu kryptografie. K určitému uvolnění amerických exportních zákonů týkajících se amerických občanů došlo v roce 1996. Institut *ITAR (International Traffic in Arms Regulations)*, který řídí používání kryptografie, povolil dočasný osobní export silné kryptografie americkým občanům cestujícím do ciziny. V následujícím roce 1997 vešla v platnost nová politika kontroly exportu šifrovacích produktů a služeb, označovaná jako *EAR (Export Administration Regulations).* Jedním z důvodů bylo rozhodnutí kalifornského soudu, pozastavující dosavadní omezení řízená institucí *ITAR,* jako omezení odporující duchu prvního dodatku americké ústavy o svobodě projevu. Rozhodnutí soudu platilo pouze pro Severní Kalifornii, jinde závazné nebylo. Do platnosti *EAR* bylo u komerčních šifrovacích produktů společnostem zakázáno prodávat mimo Severní Ameriku produkty s konkrétně definovanými vlastnostmi klíčů. Předpokládalo se, že uvolnění kontrol potrvá dva roky. Po této době nebude povolen export produktů, které nebudou podporovat obnovu klíčů. Obnova klíčů má nahradit americkou administrativou navržené řešení, které vyžadovalo úschovu klíče vládou. Leckteré americké firmy ale nečekají a řeší problém např. akvizicí firem v zahraničí (Sun v Rusku), jiné zase zakládáním zahraničních poboček (RSA v Japonsku). Pokud jde o současnou situaci, *Evropská unie* byla koncem roku pod silným tlakem USA na zavedení společných (rozuměj velmi restriktivních) opatření nejen pro export, ale i pro vnitrostátní

použití šifrovacích produktů. Záměry USA našly oporu jen u Velké Británie. Proto *Evropská unie* tyto návrhy USA odmítla. Především Německo, Belgie, Finsko, Dánsko a Irsko stojí za názorem, že důvody, jako např. sledování kriminálních živlů, neospravedlňují vládní úředníky sledovat privátní komunikaci občanů. Celkově je jasné, že ukrajinská mafie nezačne používat vládou předepsané slabé šifrování jen proto, že se zalekne možného trestního postihu za používání příliš silného šifrování. *Kongresový výbor USA* rozhodl, že software, který chrání soukromí, je předmětem kontroly a nesmí být dále prodáván. Schůze zpravodajského výboru Sněmovny pak hlasovala pro zcela přepracovaný návrh „*Bezpečnost a svoboda pomocí šifrování" (SAFE - Security and Freedom through Encryption).* Ten zahrnuje ustanovení

-o kontrole exportu, kterou budou realizovat ministerstva obrany a obchodu;

-o sledování software, ten může být exportován pouze v případě, že návrh obsahuje pojistku ohledně úschovy klíčů a je nejprve předložen vládě,

-o tom, že exportní rozhodnutí nejsou předmětem soudní kontroly a *„prezident může výkonným příkazem nepřihlédnout k jakémukoliv ustanovení zákona, domnívá-li se, že je ohrožena národní bezpečnost"*.

Zatímco dříve se v USA diskutovalo o kontrole exportu, bojuje se nyní o to, jak přísné budou domácí kontroly. Software bez ohledu na sílu šifry může být tedy exportován pouze v případě, že obsahuje zadní vrátka úschovy klíče a je nejprve předložen vládě.

Některé speciální produkty dostupné na Internetu. Z dobrých dostupných produktů autoři [73] uvádějí

-*systém PGP,* jako asi nejznámější a nejpoužívanější produkt se silným šifrováním, dostupný zdarma pro nekomerční použití; jeho nové verze podporují obnovu klíčů, na síti jsou dostupné jak vlastní *PGP* programy, tak klíče desetitisíců jednotlivců, ale i grafická rozhraní pro náročné;

-*Entrust Solo,* jako nejnižší z řady produktů špičkové ottawské firmy, je dostupný zdarma pro nekomerční účely a na dobu 30 dnů také firmám pro ohodnocení; umožňuje šifrování a dešifrování souborů, vytváření a verifikaci digitálního podpisu, bezpečné mazání souborů a jednoduchou správu klíčů, je velmi dobře integrovatelný s prostředím MS Windows a aplikacemi jako MS Word, doposud byl dostupný pouze pro Windows NT/95;

-*Fortify,* systém pro opravy šifrování u *SSL* ve webových prohlížečích *Netscape*, je zcela zdarma a také volně redistribuovatelný, pouze s určitým omezením proti komerčnímu zneužití.

**

Kryptoanalýza. Úlohou kryptoanalýzy je studium metod luštění šifer, tj. zašifrovaných textů, které vzniknou aplikací šifrovacího algoritmu na otevřený text (zprávu). Podle studie [153], kryptoanalýza v počítačové bezpečnostní politice má v podstatě dvojí účel - slouží pachateli k prolomení šifry nebo naopak k dokázání míry spolehlivosti použitého šifrovacího algoritmu. Proto je potřeba před vlastní kryptoanalýzou stanovit její výchozí podmínky a cíle. Za předpokladu, že kryptoanalytik je obeznámen s použitým šifrovacím algoritmem, můžeme rozlišovat tyto případy:

1)*Znalost pouze šifrovacího textu*, tj. vlastní kryptoanalýzu lze uskutečnit pouze na základě znalosti šifrovacího textu. Přitom v jednoduchých systémech, jako jsou např. substituční šifry, lze z celkem krátkého zašifrovaného textu dešifrovat původní zprávu pomocí statistických informací o předpokládaném jazyku, ve kterém byl napsán otevřený text. Rozhodující v tomto případě je četnost výskytu určitých samohlásek a souhlásek, dvojic či trojic písmen atp.

2)*Znalost otevřeného textu*, kdy kryptoanalytik zná před vlastním dešifrováním určité otevřené texty spolu s jejich zašifrováním.

3)*Možnost výběru otevřeného textu*; kryptoanalytik má možnost selekce určitých otevřených textů, včetně jejich zašifrované podoby. Případ může nastat, pokud dotyčná osoba je schopna předstírat oprávněného uživatele šifrovacího systému. Tento typ útoku je obzvlášť účinný u asymetrických (tj. oboustranně nesdílených klíčů) šifrovacích systémů, jestliže je počet možných zašifrovaných zpráv relativné malý. I informace, že šifrovací text nepatří k určitému otevřenému textu, může být velmi užitečná.

4)*Znalost šifrovacího klíče*; kryptoanalytik zná šifrovací algoritmus parametrizovaný určitým klíčem a pokouší se najít odpovídající dešifrovací algoritmus, aniž by obdržel nějakou zašifrovanou zprávu. Tento přístup je typický pro šifrovací systémy s veřejným klíčem, kde jsou tyto údaje známé. Kryptoanalytik má tedy dostatek času, aby si připravil různé výpočty na dobu vlastního luštění zachyceného zašifrovaného textu. V některých systémech lze totiž při obzvlášť velkém štěstí najít přímo dešifrovací algoritmus, pokud umíme „uhádnout“ rozklad určujícího přirozeného čísla na prvočinitele.

5)*Kryptoanalýza s pomoci násilí či podplacení* je jedním z nejúčinnějších způsobů útoků, kdy kryptoanalytik použije hrubé násilí, případně i poněkud jemnější metody pro získání klíče. Zkušený kryptoanalytik totiž útočí proti nejslabšímu místu, což zpravidla není šifra, ale způsoby nevhodné správy klíčů, jako např. prohřešky zaměstnanců, kteří nedbají na zachovávání pravidel utajení.

Základní metody kryptoanalýzy. Při znalosti pouze šifrovacího textu bývá používáno s úspěchem tzv. polyabecední šifry *Vigenerova* typu, která podle [153] patří k základním moderním metodám kryptoanalýzy. Polyabecední šifry na rozdíl od monoabecedních šifer mají tu vlastnost, že zašifrování písmen (posloupnosti písmen) závisí na jejich poloze v otevřeném textu. *Vigenerova šifra* je vůbec nejstarším a nejznámějším polyabecedním šifrovacím systémem. Ukázku práce s touto šifrou pomocí testů *Kasiského - Friedmanova* podává již citovaná studie [153]. *Kasiského* test je založen na tom, že si všímáme výskytu dvou stejných slov v šifrovém textu (čím delší slovo, tím lépe). Můžeme pak předpokládat, že rozdíl vzdálenosti těchto slov by mohl být násobkem našeho klíče. Jde samozřejmě o hypotézu, protože táž slova nám mohou v šifrovém textu vzniknout i zcela náhodně. *Friedmanův test* nám zase umožňuje odhadnout délku klíče. V tomto testu se ptáme, s jakou pravděpodobností náhodně vybraný pár písmen ze zprávy sestává ze stejných znaků. Máme-li pevně zadán počet písmen zkoumaného textu, lze jednoduchou úvahou spočítat tuto pravděpodobnost, kterou označujeme jako *Friedmanův index koincidence.* Podrobnější použití tohoto ukazatele popisuje opět [153]. Vigenerova šifra se vzhledem k potřebné délce klíče používá hlavně pro diplomatické kanály. Bezpečnost této metody je založena na vytvoření co

možná nejvíce náhodné posloupnosti dat. Nutno si však uvědomit, že cokoliv je vytvořeno počítačem, nemůže být nikdy zcela náhodné. Další známou polyabecední šifrou použitou ve druhé světové válce byla rotorová šifra *ENIGMA*, první šifra dešifrovaná pomocí jednoduchých obrovských elektromechanických počítacích strojů velikosti šatníkových skříní. Přitom zadními vrátky byla mimo jiné znalost způsobu zápisu stručných meteorologických kódů německého ponorkového námořnictva.

Perfektně bezpečné šifry představují pro kryptoanalýzu tvrdý oříšek. Jedná se o takové šifry, kdy z tvaru zašifrovaného textu nelze nic usoudit o původním otevřeném textu. Perfektní bezpečnost je ovšem v praxi obtížné dosažitelná, buď tím, že i pro jedno použití je nutno někde uchovávat dlouhý klíč (což nese s sebou určitá nemalá rizika), nebo je nutno ho předat před vlastním přenosem bezpečně příjemci (ale to bychom mohli udělat i se zprávou samotnou). Kryptoanalýza současných šifer se podstatně liší od kryptoanalýzy historických šifer. Zmiňme v krátkosti některé základní postupy. Prvním je podrobné prohledání prostoru možných klíčů (útok s použitím hrubé síly) a jejich ověření, což v případě nejčastěji používané speciální šifry *DES* vedlo k jejímu prolomení pomocí Internetu. Dále je možné využít některých vad šifrovacích algoritmů, které umožní podstatně zmenšit prostor klíčů. Další používanou variantou je zjištění závislosti počtu znaků (bitů) zašifrované zprávy na klíči.

Diferenciální kryptoanalýza. Podle [153], specialisté Biham a Shamir nalezli útok s možností výběru otevřeného textu pomocí metody *diferenciální kryptoanalýzy*, který je efektivnější než obvyklý útok s použitím hrubé síly. Přitom diferenciální analýza, zjednodušeně řečeno, je založená na tom, že cíleně zkoumáme určité páry šifrovacích textů a to těch, jejichž otevřené protějšky vykazují určité diference (rozdíly). Pak se postupně zkoumá, jakým způsobem se tyto diference v průběhu šifrovacího algoritmu mění a na tomto zjištění se různým klíčům přiřadí různé pravděpodobnosti. Pokud analyzujeme dostatečně velký počet dvojic typu *„otevřený text - šifrovací text“*, obdržíme jeden klíč jako nejpravděpodobnější. Tento klíč je pak považován za hledaný správný klíč.

Lineární kryptoanalýza, časový útok. Dalším kryptoanalytickým útokem je metoda lineární kryptoanalýzy, kdy šifrovací text aproximujeme vhodnou lineární funkcí otevřeného textu. Tuto analýzu lze kombinovat s předchozím přístupem, což bývá označováno jako metoda *diferenciálně-lineární kryptoanalýzy*. Pro úspěšnou realizaci útoků tohoto druhu stačí podstatně menší počet dvojic typu *„otevřený text - šifrovací text“*. Výhody a nevýhody daného přístupu rozebírá podrobněji opět studie [153]. Jiným typem útoku je tzv. *časový útok (timing attack)* založený na přesném změření času potřebném pro operace se soukromým klíčem. Šifrovací systémy často potřebují podstatně různý rozsah výpočetní doby pro různé vstupy. Při jeho komparaci může kryptoanalytik najít potřebné markanty algoritmu, faktorizovat klíče a prolomit i další jiné šifrovací systémy. Přitom v případě zranitelných šifrovacích systémů je tento způsob útoku výpočetně nenáročný a často vyžaduje pouze známý šifrovací text.

Kryptoanalýza a počítačová bezpečnost. Všechny uvedené metody podstatně závisí na šifrovacím algoritmu, který byl použit pro zašifrování zprávy. Neexistuje univerzální postup dešifrování. Vlastní kryptoanalýza není jen suchou matematikou, ale využívá odhadů, apriorních informací, hypotetických aproximací, intuitivních zkušeností operativních pracovníků, chyb protivníka i aktivních postupů k vyvolání takových chyb. V podstatě každý šifrovací systém je prolomitelný, rozhodují o tom systémové zdroje, vyspělost výpočetní techniky, peníze, čas a lidé. Pokud náklady na tyto zdroje převáží podstatnou měrou cenu utajovaných a dobře chráněných dat, lze hovořit o relativním bezpečí daných informací.

**

Elektronický podpis. Transformace informačního systému s papírovými dokumenty na informační počítačový systém indukuje problém konverze klasických papírových dokumentů na záznamy elektronické. Při této konverzi ztrácí dokument jednu z důležitých vlastností, totiž aby mohl být podepsán člověkem, který je za obsah tohoto dokumentu zodpovědný. Jednou ze stěžejních úloh bezpečnostní počítačové politiky je hledání elektronického ekvivalentu manuálního podpisu, jenž poskytne požadované vlastnosti. Tento ekvivalent je nazýván *elektronickým podpisem*, nebo někdy také *podpisem digitálním*. Blíže k tomu viz např. studii [64].

Kryptografie a elektronický podpis. Jak uvádí autor studie [64], proces podepsání zprávy (dokumentu) elektronickým podpisem typicky probíhá tak, že se nejdříve vytvoří kontrolní součet zprávy, tzv. *haš*, který je vlastně charakteristikou zprávy. Tento *haš* se spočte vhodnou, kryptograficky bezpečnou jednocestnou *hašovací funkcí.* Poté se zašifruje asymetrickým šifrovacím algoritmem pomocí soukromého klíče odesílatele a tím se získá elektronický podpis zprávy, který se připojí ke zprávě. Kdokoli, kdo zná odpovídající veřejný klíč odesílatele, si může ověřit platnost elektronického podpisu dešifrováním pomocí veřejného klíče. Pokud je elektronický podpis v pořádku, příjemce má jistotu, že zpráva byla podepsána vlastníkem soukromého klíče a po podepsání nebyla modifikována.

Spolehlivost elektronického podpisu. Pro elektronický podpis se používají asymetrické kryptografické algoritmy, tj. algoritmy s veřejným klíčem. Důvodem je požadavek na efektivní implementaci *autenticity,* kterou lze symetrickými kryptografickými algoritmy splnit jen velmi obtížně. Nejvíce se podle [64] používají algoritmy *RSA (Rivest Shamir Adleman), DSS (Digital Signature Standard)* a algoritmy založené na eliptických křivkách *EC (Eliptic Curves)*. Pro pořízení *haše,* tedy *hašování,* se v případě různých algoritmů používá i různých speciálních funkcí. Někteří uživatelé čelí zneužití tím, že předkládají nezávislé třetí straně zprávu, její elektronický podpis a nepadělatelný doklad o platnosti veřejného klíče odesílatele. Považují to za důkaz o tom, že odesílatel tuto zprávu odeslal a odesílatel tuto skutečnost nemůže popřít. Tato vlastnost se nazývá *nepopiratelností původu.* Elektronický podpis na druhé straně nezajišťuje *důvěrnost (utajení)* zprávy. Pokud si odesilatel přeje zprávu při přenosu utajit, musí ji ještě navíc zašifrovat některým jiným šifrovacím algoritmem, případně pro její přenos použít implicitně důvěrný přenosový kanál, např. v Internetu využitím vlastností virtuálních privátních sítí na bázi speciálních protokolů. Znalost správného postupu

při používání elektronického podpisu je jedním z předpokladů prevence počítačové kriminality.

Fáze elektronického podpisu. Proces elektronického podpisu má tři fáze. V první fázi odesilatel zprávy vygeneruje svůj veřejný a soukromý klíč. Svůj soukromý klíč si bezpečně uschová a chrání jej proti prozrazení. Svůj veřejný klíč si zaregistruje u potenciálního příjemce. Při registraci veřejného klíče odesílatel manuálně podepíše „*prohlášení o registraci veřejného klíče"*, které obsahuje text prohlášení, registrovaný veřejný klíč a dobu jeho platnosti. Druhou fází je podepsání dokumentu odesílatelem. V této fázi odesílatel vytvoří dokument a podepíše jej svým soukromým klíčem. Tento podepsaný dokument odešle příjemci. Třetí fáze spočívá v ověření elektronického podpisu příjemcem, které se uskuteční pomocí veřejného klíče odesílatele. Pokud je ověření elektronického podpisu úspěšné, příjemce má jistotu,

-že zprávu mohl podepsat pouze ten, kdo zná k veřejnému klíči odpovídající soukromý klíč (tedy pouze odesílatel) a nikdo jiný, což je autentizace odesílatele;

-že zpráva nebyla během přenosu ani během archivace modifikována (integrita zprávy);

-že odesílatel nemůže později popřít vytvoření této zprávy (nepopiratelnost původu).

Aplikace elektronického podpisu. Jelikož elektronický podpis zajišťuje jak identitu autora, tak i integritu podepsané zprávy, může být použit v nejrůznějších aplikacích. Může být použit například v systému elektronické pošty. Elektronický podpis může figurovat také v systémech pro elektronické provádění plateb. Autor [64] uvádí příklad zfalšování elektronického převodu určité finanční částky, která byla neoprávněně zdesateronásobena. Při komunikaci po nechráněné datové síti zpráva může být útočníkem poměrně snadno libovolně pozměněna. Pokud je však zpráva před odesláním podepsána elektronickým podpisem, příjemce bezpečně pozná, že byla modifikována a odmítne ji akceptovat. Elektronický podpis může být také zabudován do velkého množství obchodních aplikací vyžadujících elektronickou náhradu manuálního podpisu. Jedním z příkladů v tomto směru je elektronická výměna dat (informací) mezi počítači, kdy přenášené informace představují obchodní dokumenty (doklady). Systému lze použít například pro bezhotovostní platební styk nebo pro elektronický styk s finančními ústavy. Přitom je elektronického podpisu využíváno jako přímé náhrady manuálního podpisu přenášených dokladů. Ve studii [64] je uveden příklad uzavření kontraktu mezi státní správou a dodavatelem. Orgán státní správy vytvoří poptávkový dokument, podepsaný elektronickým podpisem, jehož ověřením se potenciální dodavatel ubezpečí o věrohodnosti dokumentu. Sám potom vytvoří vlastní nabídku a také ji opatří elektronickým podpisem. Jakmile orgán státní správy přijme nabídku, realizuje stejným způsobem její ověření. Je-li nabídka přijata, orgán státní správy s dodavatelem sjedná smlouvu, která je oběma účastníky podepsána elektronickým podpisem a archivována. Pokud by později došlo ke sporu, obsah smlouvy a elektronické podpisy mohou být prověřeny nezávislou třetí stranou, například soudem. Elektronický podpis může být také užitečný při distribuci software. Programové vybavení může být po schválení pro distribuci podepsáno elektronickým podpisem. Před instalací software na počítači může být elektronický podpis

zkontrolován aby se zajistilo, že se softwarem nebyla provedena žádná změna, jako je například infekce virem nebo úmyslná modifikace. Elektronický podpis může být později periodicky kontrolován a tím se zajistí, že ani později během činnosti nebyl software modifikován. V databázových aplikacích je často velmi důležitá integrita informací a jednou z možností jejího zajištění může být také elektronický podpis. Dokument může být například podepsán před jeho vložením do databáze. Při jeho pozdějším vyhledání lze elektronický podpis zkontrolovat. Je-li správný, uživatel má jistotu, že dokument nebyl modifikován ani podvržen neautorizovaným subjektem. Systém také může ukládat podpisy do auditního záznamu, čímž se získá přehled o uživatelích, kteří informaci v databázi modifikovali. To vše přispívá ke ztížení práce případným zneuživatelům a tedy k omezení počítačové kriminality, zejména pak v oblasti finančního styku.

Správa veřejných klíčů. Dalším základním problémem, který se objeví při použití elektronického podpisu, je otázka autenticity veřejných klíčů. V okamžiku ověřování elektronického podpisu si musí být ověřovatel jist, že veřejný klíč, který používá k ověřování daného podpisu, náleží autorovi zprávy, tzn. potřebuje spolehlivou vazbu mezi klíčem a jménem. Registrace veřejného klíče, popsaná v předcházejících odstavcích, je použitelná pouze v prostředí, kde je poměrně malý počet uživatelů, kteří se mohou snadno osobně setkat. V praxi ale chtějí elektronický podpis používat komunity obsahující velký počet uživatelů, kteří se navzájem nemusí ani znát. Zde by tento způsob registrace, vyžadující předchozí osobní setkání odesílatele a příjemce, byl prakticky nepoužitelný. Složitost tohoto problému může být zmenšena *certifikací* veřejných klíčů prostřednictvím někoho jiného, komu jak odesílatel, tak příjemce důvěřují. Tento prostředník, takzvaná *certifikační autorita*, elektronicky podepíše veřejný klíč uživatele a jeho jméno, případně i další údaje, jako například dobu platnosti, svým vlastním soukromým klíčem. Tyto údaje, podepsané certifikační autoritou, nazýváme *certifikátem*. Certifikát může být ověřen veřejným klíčem certifikační autority; oba partneři však musí klíč znát a mít k němu důvěru. Veřejný klíč certifikační autority musí být distribuován vhodným bezpečným kanálem. Ve velkých skupinách (doménách) uživatelů zahrnujících třeba milióny partnerů, však nestačí jediná společná certifikační autorita. Veřejné klíče certifikačních autorit mohou být opět certifikovány jinými certifikačními autoritami. Je možno brát v úvahu *stromové (hierachické) struktury* certifikačních autorit nebo *síťové struktury*, v nichž se jednotlivé autority, náležící do různých stromů (hierarchií, domén), navzájem křížově certifikují. To vytváří *cesty certifikace* nebo *řetězce důvěry* mezi jednotlivými partnery. Řetězce však nemohou být nekonečné a veřejný klíč poslední autority potom zůstává necertifikovaný. To je kořenový veřejný klíč a uživateli nezbývá, než mu věřit. Autenticita tohoto klíče musí být zajištěna nějakým jiným způsobem. Klíč může být zveřejněn například v čitelné podobě a daný software může uživateli umožňovat porovnání s klíčem uloženým v počítači.

Právní aspekty elektronického podpisu. Pro úspěšnou implementaci elektronického podpisu je však třeba zvládnout i některé systémové, organizační a právní otázky. Např. může být nezbytné též zajišťování centrální registrace veřejných klíčů uživatelů. Zde musí být vzaty v úvahu právní náležitosti, jako zodpovědnost certifikační autority, přijímání elektronicky

podepsaných dokumentů orgány státní správy a *důkazní síla elektronického podpisu u soudu.* V konkrétní aplikaci je rovněž třeba vyřešit některé technické detaily, jako mechanismy generování a distribuce certifikátů, mechanismy rušení jejich platnosti aj. Zejména právním aspektům je třeba v našem prostředí věnovat daleko větší pozornost než tomu bylo doposud.

Z uvedeného je vidět, že překonání bariér elektronického podpisu může být pro pachatele informační kriminality velmi obtížné. Aby narušitel mohl být úspěšný, musí být velmi dobře znalý nejen lokálních poměrů komunikace, ale také techniky jištění, včetně kryptografických metod. Prolamuje zpravidla vždy jen nejslabší místo systému nebo využije tzv. hrubé síly, v tomto případě spíše nedbalosti zúčastněných uživatelů. Bohužel studie [64] se nezabývá možnostmi narušení takto jištěné komunikace uživatelů. Rovněž o právních otázkách „de lege lata" elektronického podpisu u nás připravovaného zde není blíže pojednáno.

Akceptování elektronického podpisu ve světě. Jak uvádí studie [64], ve státní správě mnoha zemí je elektronický podpis běžně používán. Všechny federální orgány USA, včetně orgánů ministerstva obrany, mohou používat elektronický podpis, implementovaný na základě speciálních standardů pro podepisování neklasifikovaných informací. Ministerstvo obrany ve vybraných aplikacích používá jednoho z nich i pro podepisování klasifikovaných dat. V USA bylo vydáno rozhodnutí, že elektronického podpisu může být použito pro vytváření platných hospodářských smluv a závazků, přičemž tímto způsobem opatřené dokumenty budou chápány jako platné důkazní materiály. Určité výjimky platí v některých státech USA, jako např. v Utahu. Ten se stal prvním státem na světě, který má ve svém právním řádu uzákoněna pravidla pro používání elektronického podpisu. Podobný zákon je už delší dobu připravován v Německu, ale s jeho přípravou jsou spojeny jisté problémy. Není jasné, zda podobné zákony budou v dohledné době vznikat i v jiných státech, neboť ve většině zemí s anglosaským právem se soudí, že pro používání elektronického podpisu není zvláštní legislativní úpravy zapotřebí.

6.5. Informační a počítačový terorismus

Počítačový terorismus - nejde o nadnesený či jinak nepřiměřený pojem. Podle [164] se pro jeho akceptování můžeme opřít o různé studie renomovaných odborníků - informatiků a o některé scénáře, které ze studií vyplývají. Jde prozatím jen o podobu chmurných vizí. Experti je zpracovávají ve Spojených státech, v rámci *Výboru pro studium systémové bezpečnosti*, na základě návrhu *Darpa, Agentury Pentagonu pro pokročilé výzkumné projekty obrany* a *Národní rady výzkumu* pod vedením Davida Clarka ze špičkového amerického a světového vědeckého pracoviště *Massachusetts Institute of Technology (MIT)*. Clarkův zobecněný závěr zní: *„Terorista zítřka způsobí klíčovým slovem neporovnatelně více škod než dnes bombou."* Neudivuje proto vyslovení takovýchto obav, jako např. Petera Neumanna, informačního experta technologicko-konzultační firmy *SRI International* z kalifornského Menlo Park: *„Pomocník nějakého diktátora zvedne telefon, propracuje se prostřednictvím světových*

komunikačních sítí do počítače dopravní centrály v Dallasu nebo Chicagu a během několika minut již budou světové agentury vyťukávat zprávy o katastrofách." Podle tohoto specialisty se některých ošklivých překvapení dožijeme již velmi brzy. Ještě pesimističtější je viceprezident *Institutu pro aplikované systémy* ve Washingtonu, který říká, že teroristé snadno zjistí, že technická sabotáž prostřednictvím počítačové sítě je atraktivní i vzhledem k malému osobnímu riziku a nákladům, a budou se tudíž pokoušet na úkor maxima lidského utrpení vykonávat nátlak na USA, nebo je dokonce vydírat. Již počátkem roku 1991 na téma *počítač v nebezpečí* bylo hovořeno o velice brizantním tématu rostoucího terorismu, a sice o rizika sabotáží a teroru v sektoru informatiky. Varování zde vyslovená nejsou v žádném případě předčasná. Jejich autoři mimo jiné říkají, že jsme doposud měli štěstí, když zatím nedošlo ke katastrofálním následkům z manipulování počítačovými systémy zvenčí. Zároveň ale zdůrazňují, že existují důvody pro oprávněnost domněnky o tom, že toto štěstí již končí. Šéf počítačové bezpečnosti *JSC - Johnsonova vesmírného centra NASA* v Houstonu, správně odhaduje, že teroristům nejde ani tak o špičkové technické údaje, jako o zaplavování společnosti traumatickými šokovými zprávami.

Směrování konkrétních hrozeb. V ohrožení tedy jsou nejen citlivé informační a řídící systémy amerického ministerstva obrany, *NASA,* nebo kteréhokoliv špičkového výzkumného střediska. V ohnisku zájmu pravděpodobných, politicky motivovaných teroristických útoků jsou i letecká a kolejová doprava, zásobování energií a zdravotnictví, nevylučují se ani počítače a programové systémy používané při volbách apod. V některých případech již neblahá budoucnost začala, jako např. v letecké dopravě, kde v organizaci na zemi i ve vzduchu hrají počítače hlavní roli. Vyskytla se již první hlášení o pokusech manipulace a infiltrování virů narušujících systémy. Největší obavy však nejsou z nedodržování letových časů, ale z dálkově řízených srážek plně obsazených letadel. Toto nebezpečí se přirozeně týká i evropské dopravy. Neméně riskantní oblastí je zdravotnictví, kde rovněž došlo k aplikační explozi počítačů. Podle [164], zfalšování dat a nasazení virů již způsobilo předávkování i smrt pacientů. Stejně mohou vnější vlivy zmanipulovat řídící centra jaderných elektráren, zejména mají-li uvnitř „svého člověka". Tento druh potenciálního i již počínajícího terorismu pochopitelně využívá i virových manipulací a státní hranice nebo civilní či vojenská odlišení nejsou žádnými významnými překážkami. Nebezpečí se v USA považuje již za tak vážné, že jsou na jeho potírání zainteresovány takové instituce jako *NSA - Agentura pro národní bezpečnost* - prostřednictvím svého národního ústředí počítačové bezpečnosti (*NCSC*), dále *Národní institut norem a technologií (Nist),* a zejména *Afosi - Úřad leteckých sil pro zvláštní vyšetřování*, se svým oddělením pro počítačové zločiny. Jsou to jedny z prvních amerických míst kompetentních pro počítačovou bezpečnost. Od doby infekce sítě Internet se 60 000 postiženými počítači po celém světě, spolupracují s *Afosi* v krizových případech tzv. *počítačové záchranné týmy Cert.*

Záruky bezpečnosti vůči počítačovému terorismu spatřují tvůrci katastrofických studií v personální politice, která by měla maximálně zajišťovat nezávadnost osob v okruhu počítačových sítí. Při tom je třeba najít správný kompromis, aby přehnaná nařízení nebrzdila

vědecký a technologický pokrok, ale aby zároveň bylo zajištěno hardwarem, softwarem i uživatelskými předpisy více bezpečnosti zejména tam, kde jde o lidské životy. Navrhuje se vytvoření ústavu pro informační bezpečnost, jehož úkolem by byl výzkum počítačové bezpečnosti, sledování vývoje počítačové kriminality a hledání protiopatření; dále efektivní kontrola software, hesel a jiných způsobů vstupu do systémů, kódování dat pro uživatele, urychlení postupů proti zjištěným proniknutím do sítě atd. Je zřejmé, že čistě národní řešení problémů počítačového terorismu nebudou postačující. Je to i stanovisko amerických expertů, kteří pokusy jednotlivých evropských států o vytvoření vlastního systému počítačové bezpečnosti sledují většinou s despektem. Za úzkoprsé a krátkozraké považují zejména prvořadé snahy evropských výrobců zachovat pro své výrobky výhody evropského trhu.

**

Nové koncepty informační války. S postupným propojením vojenských, civilních a zpravodajských komunikačních systémů se tyto systémy stávají neoddělitelné. Bezpečnostní architektura těchto sítí, která byla vybudována na principu propojení přes přístupový počítač, který vyžadoval vstupní hesla, se ukázala jako značně neefektivní. Moderní sítě jsou složité, rozsáhlé a rostou tak rychle, že nelze vytvořit účinný ochranný systém za použití statických bezpečnostních prvků, jako je oddělení sítě od okolního světa přístupovým počítačem (tzv. firewall). Dokonce zbraňové systémy, které stále více používají komerční software a další zařízení dostupná na trhu, nelze z bezpečnostního hlediska považovat za spolehlivé.

V Bruselu proběhla v roce 1997 evropská konference o informační válce, kterou organizoval *Národní svaz počítačové bezpečnosti (National Computer Security Association - NCSA)*. Jen některé z příspěvků, přednesené renomovanými světovými osobnostmi, objasnily v čem spočívá hlavní riziko tzv. strategického zvratu. Zástupce Ministerstva obrany USA uvedl, že podle jeho názoru přístupy k zabezpečení informací pomocí metod „vyhýbání se riziku“ a „řízeného rizika“ selhaly. Poznamenal, že počítače Pentagonu byly neustále cílem pokusů o průnik, přičemž instalované bezpečnostní systémy s konvenční architekturou vyvolávaly falešný pocit bezpečí. Tento expert předložil operační model vybudovaný na dynamickém chování ve třech základních bodech - *chránit, detekovat, reagovat*. V tomto směru ho podpořili bývalí manažeři speciálních sítí *UUNet*. Jimi bylo konstatováno, že bezpečnost založená na systému přístupového počítače v praxi neexistuje. Tyto systémy jsou pomalé a drahé z hlediska instalace i údržby a navíc jsou nespolehlivé. Při spolupráci se *Střediskem letectva pro informační válku* vyvinula *Wheel Group Corp.* metody a nástroje, které mohou objevovat zranitelná místa sítí, odstraňovat je a sledovat nepřetržitě síť pomocí programů typu *Net Ranger*. Dokonce ještě před vlastním útokem může tento program sledovat síť a odhalit hackerův pokus o přiblížení se k síti. Někteří z účastníků diskuse pracují v divizi informačního boje společnosti *Northrop Grumman.* Úkolem divize je detekce virů, logických bomb a trojských koní, které mohou proniknout do zbraňových systémů. Toto nebezpečí značně vzrostlo, protože do těchto systémů se stále častěji zabudovávají zařízení a programová vybavení od různých výrobců. Výsledkem práce tohoto oddělení jsou testovací programy, které mají za úkol vytvořit databázi průniků. Většina průniků však není došetřena. Databáze proto vytváří „profily“ možných útoků a tak může sama připravit protiakci v

předstihu. *Northrop Grumman* nabídl tento systém Ministerstvu obrany USA. I když se zdůrazňuje obranný účel celého systému, je zjevné, že systém může stejně dobře sloužit i k útočným záměrům americké armády.

Ochrana počítačových dat proti zničení a poškození. Vývoj národní politiky ochrany informační infrastruktury je celosvětově v současné době velmi aktuální. Člen národního bezpečnostního úřadu viceprezidenta USA prohlásil, že je nutno vytvořit zákonný rámec pro tuto oblast. Podle materiálu [235] měl být tento rámec vytvořen a předložen k politické diskusi Kongresu USA již koncem roku 1997. Zákonodárci, podle nichž je však za tuto záležitost zodpovědná vláda USA, požadují na ministerstvu obrany a zpravodajských službách zpracování srovnávací zprávy, která by obsahovala rizika hrozící počítačům a informačním systémům v USA a uvedení způsobů eliminace těchto rizik. Z tohoto důvodu bude *DARPA (Defense Advanced Research Projects Agency- Agentura pro moderní výzkumné obranné projekty)*, která je hlavním vývojovým pracovištěm ministerstva obrany v oblasti informačních technologií, krátce testovat nový bezpečnostní systém z hlediska schopnosti informačního přežití a pokračování operací v nepřátelském prostředí. Technologie použitá v projektu zahrnuje metody a nástroje k detekování průniků, stanovení škod a téměř okamžité obnovení činnosti poškozených systémů s cílem minimalizovat vliv nepřátelských operací. Zkušenosti získané z této činnosti budou po dohodě s odpovědnými orgány USA doporučeny k uplatňování v boji s počítačovým terorismem i v dalších zemích.

7. Porušování autorských práv

Sestaveno převážně z pramenů: [6], [34], [36], [40], [50], [51], [54], [57], [59], [68], [81], [98], [101], [110], [179], [194], [199], [203], [210], [214], [219], [220], [223], [234], [237], [241], [243], [245], [249], [250].

7.1. Autorskoprávní ochrana software

Deklarováním programátorství jako tvůrčí duševní činnosti byl dán popud k přiznání statutu tzv. duševního vlastnictví pro výsledky této činnosti, tedy pro počítačové programy. Pokud počítačový program splňuje požadavek původnosti a jedinečnosti, je na něho pohlíženo jako na autorské dílo se všemi právními důsledky. Dne 22.4.1996 byla uveřejněna *Sbírka zákonů, částka 29*, ve které je obsažen i *zákon č.86/96 Sb.*, kterým se mění a doplňuje *zákon č.35/65 Sb. o dílech literárních, vědeckých a uměleckých (autorský zákon)*, ve znění *zákona č.89/90 Sb., zákona č.468/91 Sb., zákona č.318/93 Sb.* a *zákona č.237/95 Sb.*

Programy jako díla autorská byly tedy výslovně pojaty novelou č.89/90 Sb. autorského zákona č.35/65 Sb. (viz [245]) od poloviny roku 1990. Za předmět autorskoprávní ochrany se považují jen ty programy, při jejichž tvorbě byl uplatněn originální přístup, nápad, myšlenka nebo systémový přístup, který by pravděpodobně nebyl použit jiným tvůrčím subjektem při řešení téhož úkolu. Jak uvádí autor studie [241], samo autorství je v českém právním systému postaveno vysloveně na osobním principu. Což znamená, že autorem se všemi jeho právy může být kdokoliv, dokonce i osoba bez patřičného vzdělání v daném oboru.

Programátor jako autor programu, může tento program poskytovat k užívání další osobě, fyzické či právnické, na základě autorské smlouvy o užití díla, ve které se specifikuje o jaký program jde. Zde se stanoví přesně rozsah jeho užívání a určí se i výše autorské odměny. Totéž platí i ve vztahu k nějaké firmě pro distribuci programu. Vlastnictví autorských práv je nepřevoditelné a zůstává vždy autorovi, který pouze postupuje právo na užívání jeho díla v jím stanoveném rozsahu. Podle autorského zákona, do něhož tedy byly počítačové programy a jejich systémy zahrnuty jako jeden z druhů autorských děl, lze s nimi nakládat jen se souhlasem autora. Programátorovi též přísluší za užívání programu či systému programů jím vytvořených autorská odměna.

Podle studie [199], současný český autorský zákon [249] z roku 1990 ve znění pozdějších předpisů definuje poměrně rigorózní ochranu počítačových programů. Podle tohoto zákona, o dílech literárních, vědeckých a uměleckých jsou předmětem autorského práva díla literární, vědecká a umělecká, která jsou výsledkem tvůrčí činnosti autora, zejména díla slovesná, divadelní, hudební, výtvarná včetně děl umění architektonického a děl umění užitého, díla filmová, fotografická a kartografická. Za předmět ochrany se považují i programy počítačů, pokud splňují pojmové znaky děl podle tohoto zákona.

Podle [199], nejvíce sporů - i mezi policisty, vyšetřovateli a znalci - se týká výkladu ustanovení § 17 o programech vytvořených v rámci pracovního poměru. V poslední době se můžeme setkat ze strany tvůrců programů s vehementní snahou o uzavírání

dalších smluv - tj. autorských, kromě již uzavřených zaměstnaneckých. Několikrát došlo k vymazání zdrojových textů nebo dokonce ke znepřístupnění báze dat zaměstnavatele, a to jednostranným úkonem programátora, když zaměstnavatel odmítl autorskou smlouvu uzavřít. V jednom případě dokonce zaměstnanec požadoval na zaměstnavateli zaplacení dosti vysoké částky za zpřístupnění těchto dat.

Jak uvádí dále [199], nutno především zdůraznit, že takové postupy programátorů, i kdyby se o autorské dílo jednalo, jsou nezákonné a mohou naplňovat dokonce skutkovou podstatu trestného činu vydírání podle ustanovení §235 trestního zákona. Kromě toho by se zaměstnavatelé pravděpodobně úspěšně mohli domáhat náhrady škody podle ustanovení §420 a násl. občanského zákoníku. S tím souvisí i otázka, zda u konkrétního programu jde vůbec o autorské dílo, kdo je jeho autorem a v jakém právním režimu. Pokud programy počítačů splňují pojmové znaky děl podle autorského zákona, považují se za předmět ochrany. Ne všechny počítačové programy lze označit za autorská díla, tedy neplatí, že by automaticky každý program podléhal ochraně podle autorského zákona. Pokud není mezi programátorem a zaměstnavatelem uzavřena autorská smlouva, kde by obě strany shodně označily vytvořený program za autorské dílo, nelze automaticky přisoudit každému programu autorskou ochranu. Dokud tak nebude učiněno (vzájemnou dohodou nebo pravomocným rozsudkem soudu), nelze jednostranným aktem, např. nevydáním zdrojových textů nebo dokumentace, omezit zaměstnavatele v možnosti plně užívat daného programu. Pokud by bylo prokázáno, například posudkem soudního znalce, že se jedná o dílo chráněné podle autorského zákona, platí zde ustanovení §17 autorského zákona a předpoklady pro užívání tohoto díla. Potom ovšem přímo sám programátor, který omezuje zaměstnavatele znepřístupněním zdrojových textů, se dopouští protizákonného jednání.

Podle ustanovení § 17 autorského zákona, může zaměstnavatel užívat k plnění úkolů náležejících do předmětu jeho činnosti díla vytvořená jeho pracovníkem v rámci povinností vyplývajících z pracovního poměru bez dalšího autorova svolení. Zaměstnavatel, do jehož předmětu činnosti náleží vydávat nebo jinak uveřejňovat díla, může vydat nebo jinak uveřejnit dílo svého pracovníka vytvořené ke splnění povinností vyplývajících z pracovního poměru jen se svolením autora. Odpírá-li autor udělit mu svolení bez závažných důvodů, může se zaměstnavatel domáhat tohoto svolení u soudu. Autor díla, jež bylo vytvořeno ke splnění povinností vyplývajících z pracovního poměru k zaměstnavateli, může udělit svolení k vydání nebo jinému uveřejnění díla jen se souhlasem zaměstnavatele. Přitom, aby mohl být program řádně a bez omezení užíván, do pojmu „dílo jako programové vybavení“ je nutno zahrnout zdrojový text, dokumentaci a nakonec i binární program, který lze získat odvozením ze zdrojového textu. Zde dochází často k jednostranným aktům pracovníka nebo zaměstnavatele, vedoucím až k následným občanskoprávním i trestněprávním sporům.

Autorské právo trvá, pokud není stanoveno jinak, po dobu života autorova a 50 let po jeho smrti, u děl spoluautorů a u spojených děl vytvořených pro účely užívání v tomto spojení, 50 let po smrti toho z nich, který ostatní přežil. Pro software je podle autora [199] tato ochrana dosti nadměrná.

Dokazování autorství počítačových programů je důležité z hlediska praktického uplatňování autorského zákona. Po stránce teoretické i praktické se otázkami tohoto typu zabývá softwarová forenzní disciplina. Podle [237] byly v této oblasti experimentálně ověřeny možnosti určení autorství zejména v případech, kdy jsou k dispozici zdrojové texty programů, napsané v konkrétním (vyšším) programovacím jazyce. Otázka zachovaní, resp. odhalení charakteristického stylu programování konkrétného programátora při přechodu na jiný programovací jazyk je sice nepochybně zajímavá, v daném případě však přesahovala rámec experimentálního projektu. Zkušenosti byly tedy získány pouze při analýze zdrojových textů programů, napsaných v jednom programovacím jazyce, konkrétně v široce používaném systémovém jazyce C. Ve studiích [101], [203] jsou naznačeny některé faktory, které by mohly vytvářet charakteristický „rukopis" programátora. V rámci zmíněného projektu se brala v úvahu množina různých metrik týkajících se grafické úpravy programu, stylu programování, pojmenovávání proměnných, preferencí v řadící struktuře programu, cyklení programu, stylu komentování či vůbec nekomentování programu ap. Pro výběr množiny metrik, použitých při konečném experimentu, bylo použito úvodního experimentu malého rozsahu, následovaného pilotním projektem. Pilotní projekt sestával z analýzy práce několika programátorů, kteří dostali za úkol napsat programy pro řešení tří problémů různého charakteru. Na základě pilotního projektu bylo vybráno 23 metrik pro konečný experiment. Ten spočíval v analýze 88 programů od 29 autorů-aspirantů, pedagogů a zkušených programátorů - systémových pracovníků obsluhujících počítačové systémy. Zhruba polovina programů od pedagogů byla orientována na problémy numerické analýzy, druhá polovina byla z oblasti konstrukcí kompilátorů a softwarového inženýrství. Programy aspirantů variovali od řešení projektů počítačových sítí, až po projekty v oblasti databázových systémů, numerické analýzy a operačních systémů. Cílem experimentu bylo správné přiřazení autorů jednotlivým programům. Za povšimnutí stojí skutečnost, že ačkoliv v rámci projektu se shromáždila též kolekce několika set programů od studentů-amatérů, nebyly použitelné pro jejich přílišnou jednoduchost. *Výsledky experimentu* jsou zajímavé. Celkem 73 % všech analyzovaných programů bylo správně přiřazeno jejich autorům. U 17 z 29 autorů bylo dosaženo 100% úspěšnosti přiřazení. U pěti dalších tato úspěšnost klesla na 70%. Nulová úspěšnost v přiřazení programu jeho autorovi byla zaznamenaná u dvou programátorů. Ti podstatně měnili svůj styl programování program od programu v časovém rozpětí dvou měsíců. V programech jednoho z nich se však podařilo dodatečně objevit některé charakteristiky, které zůstávaly neměnné ve všech jeho analyzovaných výtvorech. Tyto charakteristiky však nebyly postihnutelné zvolenými metrikami. Určování autorství počítačových programů je nepochybně zatím v začátcích. Práce [101] však už nyní potvrzuje, že za jistých předpokladů lze dosáhnout v této oblasti zajímavých výsledků. Na vhodné aplikace v praxi si však budeme muset asi ještě počkat. Nicméně dostatečně teoreticky i aplikačně rozvinutá softwarová forenzní disciplina by jistě usnadnila a zkvalitnila rozhodování soudů v obtížných případech dokazování programového autorství.

7.2. Systém právní ochrany počítačových programů a dat

V České republice jsou počítačové programy jako moderní forma nehmotných statků právně chráněny zejména v rámci autorského zákona, obchodního zákoníku a v rámci trestního zákona.

Ochrana v rámci autorského zákona. Novela autorského zákona s účinností od roku 1990 pamatuje ve výčtu druhů autorských děl též na počítačové programy. V té době ČSFR se tím přizpůsobila rozhodujícímu vývoji ve světě. V počítačově vyspělých zemích je ochrana autorským právem základní formou ochrany počítačových programů. Jak uvádí studie [241], autorské právo poskytuje počítačovým programům ochranu absolutní, působící proti všem osobám. Ke vzniku autorskoprávní ochrany není třeba žádných formalit. Systém autorskoprávní ochrany je podrobně rozpracován v teorii i praxi nejen u nás, ale i jinde ve světě. Podle autorského zákona je ke každému užití autorského díla nutný souhlas autora. Užitím se rozumí zejména zhotovování rozmnoženin díla, šíření, provedení překladu, úpravy a provozování díla. U počítačových programů zahrnují tyto případy realizaci rozmnoženiny nebo úpravy programu nutné pro provoz programu na počítači a pro archivní a zajišťovací účely oprávněným vlastníkem rozmnoženiny. Dále pak užití v rámci osobní potřeby, tedy nikoliv pro komerční účely a v omezené míře i pro účely vyučování a vzdělávání. Později byly podrobněji upraveny též případy, kdy uživatel počítačového programu není povinen získat autorovo svolení, ani poskytnout zvláštní odměnu k pořízení rozmnoženiny. Např. podle novely autorského zákona z roku 1966 došlo k velmi významnému ustanovení, které spočívá v tom, že není-li vysloveně sjednáno jinak, autorské právo k počítačovému programu vytvořeného zaměstnancem ke splnění povinnosti vyplývající z jeho pracovního poměru vykonává zaměstnavatel. Zaměstnavatel tak mohl šířit program, aniž by k tomu musel žádat o souhlas programátora, který program sestavil. Podrobněji k tomu viz [243]. Autor, jehož právo bylo porušeno, může žádat, aby bylo neoprávněné užití zakázáno, aby byly odstraněny pirátské kopie a poskytnuto mu přiměřené zadostiučinění, náhrady škody. Úmyslné a hrubé porušení autorských práv k počítačovým programům je trestným činem podle §152 trest. zák. s odpovídajícími trestními sankcemi.

Ochrana v rámci obchodního zákoníku. Obchodní zákoník, jak uvádí autor [241], poskytuje počítačovým programům ochranu v rámci obecné úprava *ochrany obchodního tajemství.* Takto však mohou být chráněny pouze programy, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou běžně přístupné, mají být podle podnikatele utajeny a podnikatel jejich utajení zajišťuje. Uvedené podmínky zužují možnosti efektivního uplatnění této formy ochrany pouze na omezený počet případů, kdy jsou splněny. Ochrana proti zneužívání informací v obchodním styku je podpořena též trestním zákonem (§128 trest. zák.) s příslušnými sankcemi za zneužití obchodního tajemství.

Ochrana v rámci ustanovení o počítačové kriminalitě. Od roku 1992 bylo přijato novelou trestního zákona zvláštní ustanovení o trestných činech poškození a zneužití záznamu na nosiči informací. Tyto činy tvoří podstatnou část počítačové kriminality. Úprav lze užít i

v případech softwarového pirátství, zejména při naplnění skutkových podstat neoprávněného užití informací, neoprávněného zásahu do technického nebo programového vybavení počítače. Rovněž za tyto trestné činy jsou stanoveny sankce odnětí svobody, peněžité tresty či trest propadnutí věci.

Základem systému právní ochrany počítačových programů u nás, podobně jako v jiných zemích, je ochrana autorským právem. Ochrana v rámci úpravy obchodního tajemství, případně dalších forem, týkajících se například nekalé soutěže, patentů, topografie polovodičových výrobků (čipů) apod., tvoří společně se smluvními prostředky doplňkové formy ochrany.

Licenční politika. Pro legálního výrobce software jsou velmi důležité licenční smlouvy uzavírané s uživatelem, který si software regulérně zakoupí. Pokud uživatel souhlasí s podmínkami licenční smlouvy, smí softwarový produkt používat a získává zpravidla ještě další práva. Licenční smlouva nesmí být v žádném případě ve sporu s předpisy a zákony nadřazenými, tedy s ustanoveními větší právní síly. Problematika uzavírání licenčních smluv bývá nazývána *licenční politikou,* která může být specificky orientovaná podle zaměření, obchodní zdatnosti či jiných parametrů softwarové firmy. Velmi dobrou politiku má např. gigant *Microsoft*. Licenční smlouvy Microsoftu začínají částí *Grant of License,* která popisuje, jak uživatel smí software používat. Ve smlouvě jsou i omezení týkající se půjčování nebo pronajímání software, jeho případného dekódování nebo úprav a další omezení týkající se konkrétního produktu. Licenční smlouva také stanoví pravidla, za kterých lze pořídit záložní nebo archivní kopii produktu a obsahuje rovněž omezené záruky za software. Nová licenční politika firmy Microsoft vyhovuje organizacím všech rozměrů a je navržena tak, aby byla konzistentní s tím, že organizace zákazníků se postupně rozšiřují i do větších a geograficky rozsáhlejších sítí. Podle nové politiky jsou licence pro klienty a servery (tj. řídící síťové počítače, jakési centrály sítí) od sebe odděleny. Klienti s licencí mají přístup k neomezenému množství licencovaných serverů určitého typu; existuje malý, pevně stanovený poplatek za jeden typ serveru, který není závislý ani na množství uživatelů v síti, ani na typu počítače, který je používán. S touto koncepcí „plať postupně, tak jak se zvětšuješ“ mohou klienti získávat přístup ke službám libovolného serveru.

Odborné diskuse k problematice právních aspektů ochrany software přerostly u nás v mnoha případech k obecným rozborům počítačového práva, což se projevilo v řadě připomínek [210], [219], [234] k některým publikovaným pracem, jako např. k určitým statím v dílech [50], [51], [194], [199]. V této diskusi nešlo jen o terminologické problémy. Byly rozebírány a podrobeny určité kritice všeobecné povahové a právní otázky nehmotných statků ve vztahu k počítačům, aspekty postavení a účinnosti novel autorského zákona, pracovněprávní poměry programátorů a jiných pracovníků kolem počítačů, trestněprávní aspekty počítačového práva, metodicko-taktické přístupy z hlediska vyšetřovatelských hledisek, otázky daňové, účetní a celní politiky, problémy obchodního práva a podnikání s počítači, aspekty ochrany informací obecně i ochrany osobních informací a soukromí občanů atp. Cílem diskuse bylo vyjasnit a precizovat situaci kolem počítačového práva i počítačové

kriminality především z hlediska legislativních úprav, méně již z pohledu kriminologa. I když některé otázky zůstávají nedořešené, lze celkové aktivity v tomto směru považovat za přínosné.

Jak uvádí autor [179], přes doporučení *Světové organizace duševního vlastnictví,* které se týká vytvoření zvláštní ochrany pro software s možností podpůrného využití zavedeného institutu autorskoprávní ochrany, je až s podivem, že i když byly od té doby zahrnuty pod pojem duševního vlastnictví další jeho formy, často mnohem méně významné něž oblast software a poskytnuta jim zvláštní ochrana, pro software převládla ochrana autorskoprávní. Nevyjasněnost koncepce právní ochrany software lze demonstrovat i na praxi ve státech udávající tón ve vývoji softwarového průmyslu, kde zavedení autorskoprávní ochrany předcházely dlouhé spory o právní charakter software. V USA se tak stalo v roce 1980, v Anglii, Francii a Japonsku až v roce 1985. Programy jsou v těchto státech považovány za díla literární a jako k takovým je k nim přistupováno. Situace u nás je ve srovnání s vyspělými státy v této oblasti horší díky opožděním, spojeným se zaváděním a hlavně smysluplným využíváním výpočetní techniky. Rozvoj dostupnosti personálních počítačů u nás nastal s opožděním odhadovaným zhruba na deset let. V současnosti lze podle [179] zpoždění za vyspělým světem odhadovat asi na pět let a totéž je možné říci o právní regulaci v této oblasti. Názorů na řešení dané problematiky je celá řada a často diametrálně odlišných. Nejde přitom jen o spory o právní podstatu software, ale také často o obtížnost komunikace mezi autory a distributory software na jedné straně a právníky na straně druhé, plynoucí z diametrální odlišnosti logiky těchto oborů, a někdy i nechuti pouštět se do něčeho nového, dynamického a tudíž i rizikového. Zde však jde jen o přechodný jev, do jisté míry v současné době již řešený. Příčinou sváru ve sporu, zda je počítačový program možné považovat za autorské dílo, je skutečnost, že program má s klasickým autorským dílem velmi málo společného. Odlišuje se v řadě specifik. Autorské právo nebylo vybaveno na ochranu takového druhu díla - v době svého vzniku s něčím takovým ani počítat nemohlo. Přesto mu byla přisouzena tato role. S ohledem na praxi v ostatních státech nemá smysl na této skutečnosti mnoho měnit. Otázkou zůstává, zda se s tím náš právní řád vyrovnává, aby nebyla naplněna chmurná vize, že počítačové programy se stanou „počítačovým virem - trojským koněm“ autorského práva, který nahlodá a rozdrolí tento úctyhodný institut zevnitř. Nedostatečná praxe správních a soudních orgánů v této oblasti vedla autora studie [179] k tomu, že se začal více zabývat podněty ze zahraničí, nehledě na mezinárodní charakter software jako takového. Protože měl možnost nahlédnout na tuto problematiku i z druhé strany, tedy z pozice analytiků, programátorů či kvalifikovaných uživatelů výpočetní techniky, přihlížel i k jejich pozici.

Právní povaha počítačového programu. Počítačový program je souborem instrukcí řídící vlastní činnost počítače. Jak uvádí [179], procesor počítače může být řízen programem ve formě binárního nebo objektového kódu. Protože tvorba programů v této formě je velmi obtížná, je využíváno vyšších programovacích jazyků a následné kompilace do objektového tvaru. Dostáváme tak další formu vyjádření programu, jeho zdrojový tvar. Samotný program tak lze vyjádřit v různých formách, přičemž všechny požívají stejné právní ochrany. Užitná

hodnota software je úměrná hodnotě informace v něm uložené. Jedná se především o vnitřní strukturu a organizaci informace, což tvoří „invenční náboj“ software (obsahující též i základní algoritmus řešení) a jehož formulování je často nejnákladnější fází tvorby. Programy jsou produktem intelektuální činnosti programátora nebo častěji kolektivu specializovaných odborníků. Jde o složitý proces, jenž lze rozložit na jednotlivé fáze, které provádějí specializovaní pracovníci. Obecně lze rozlišit

-*zadání úkolu*, které spočívá v přesném vymezení rozsahu řešeného úkolu a formulace požadavků zákazníka; zanedbání tohoto kroku může později způsobit neřešitelnost právní situace mezi zadavatelem a řešitelem úkolu;

-*analýzu úkolu* - realizuje ji programátor-analytik, odborník znalý řešeného problému; úkolem analýzy je zjistit, zda je úkol řešitelný, navrhnout algoritmus a postup řešení, stanovit rozsah prací a tím i předpokládané náklady atd.; jde většinou o nákladnou část projektu, jejíž výsledek nemusí vždy zákazníka uspokojit;

-*vlastní tvorbu programu,* kdy na základě provedené analýzy je vytvořen zdrojový text programu a ten je přeložen do provozní, spustitelné verze;

-*testování programu*, jako nezbytnou fázi tvorby software, při níž je testováno chování programu v předpokládaných i nahodilých stavech s cílem odstranit případné nedostatky menšího charakteru.

Realizace programu jako předmětu směny závisí na jeho užitné hodnotě. Ta je mimo jiné závislá na kvalitě a množství informace v něm obsažené, analýze problému a algoritmu řešení, množství a způsobu interpretace výstupních informací, ale také způsobu komunikace s uživatelem, determinovanosti chování za provozních i nahodilých podmínek. Vhodný *design* programu, přehledná presentace výsledků při komunikaci s uživatelem a uživatelsky přístupné rozhraní je podmínkou úspěšnosti programu. Uvedené atributy jsou komerčně důležité. Podle [179] nejsou však předmětem ochrany na základě autorského práva. Tato skutečnost je tak jedním z argumentů zastánců vytvoření zvláštního druhu ochrany. Jak již bylo uvedeno, počítačový program sám má povahu nehmotného statku. Hmotnou formu mu propůjčuje až médium na němž je uložen, např. magnetické disky, diskety, pásky, optické disky, což jsou nosiče nejčastěji používané při jeho směně. Může však být zachycen i na papíře ve formě textu, obvykle v tzv. zdrojovém tvaru. Součástí software je pak nejen vlastní počítačový program a médium na němž je zachycen, ale i jiné podpůrné programy, data, programová dokumentace či uživatelské manuály, licenční podmínky, popř. další smluvní ujednání spolu s poskytovanými službami atp. Při určitém zjednodušení lze říci, uvádí autor [179], že způsobem svého vzniku naplňuje software znaky nehmotného statku, ale způsobem svého využití je přímo použitelným výrobkem, když toto využití samo o sobě může vést ke vzniku dalších nehmotných statků. Další zvláštností programů je technicky neomezená možnost výroby kopií a jejich nekontrolovatelné šíření. Aby program mohl být spuštěn, musí být nejdříve obsažen v paměti počítače ať již v operační - RAM nebo stálé - ROM, a poté musí převzít řízení. Tato skutečnost je uváděna jako další z důkazů dostatečnosti autorskoprávní ochrany pro počítačové programy. Autor [179] však považuje za nutné předeslat, že jde o zjednodušující pohled, nepostihující vždy přesně pravý stav věci.

Programové vybavení z hlediska funkce lze rozlišit na

-*systémové programy* - základní software bez něhož není provoz počítače možný; vzhledem k těsné vazbě na konkrétní hardware a složitost je dodáván často výrobcem hardware spolu se systémem;

-*obslužné programy* - programy sloužící k tvorbě uživatelských programů;

-*pomocné systémové programy* s odlišnou obchodní politikou, určené pro užší okruh uživatelů - programátorů;

-*aplikační programové vybavení* - uživatelské programy vytvořené k řešení konkrétních úkolů většinou specializovanými firmami;

-*programovací jazyky* -programy vytvářející vhodné vývojové prostředí a překladač pro tvorbu uživatelských programů.

Další formou nehmotného statku patřící pod pojem software, jsou data a informace, ať již ve formě databáze s určitou strukturou nebo v jiné formě. Právní ochrana vycházející z autorského práva je zde podle [179] problematičtější vzhledem k tomu, že jsou obtížněji naplněny pojmové znaky autorského díla dle autorského zákona. Je však možné použít i ochranu z jiného titulu.

K autorskoprávní ochraně počítačových programů z pohledu historického vývoje říká autor [179] v podstatě toto: Náš autorský zákon (viz [249]) vychází z Bernské úmluvy o ochraně děl literárních a uměleckých z roku 1886 ve znění pozdějších revizí (tzv. *„Revidovaná úmluva Bernská“*, jejíž je Česká republika smluvní stranou - členem *Bernské unie*). V těchto úmluvách samozřejmě nemůže být ani zmínka o software. Rozšíření autorskoprávní ochrany na software a jeho specifika oproti klasickým autorským dílům si zřejmě vynutí připojení dodatku k těmto úmluvám přihlížejícího k těmto odlišnostem, aby se tak vneslo jasno i do mezinárodní praxe. Přípravné práce na tomto kroku již začaly. V podkladovém materiálu *Mezinárodního úřadu,* jak uvádí [223], se navrhuje, aby programy byly chráněny podle Bernské úmluvy jako díla literární a umělecká, avšak s těmito hlavními výjimkami:

-ochrana programů může být vykonávána buď ve prospěch autora, jak je stanoveno v článku 2 odst. 6 *Bernské úmluvy*, nebo ve prospěch jiné osoby, podobně jako je tomu u děl kinematografických;

-aplikujeme-li definici publikace podle článku 3, odst. 3 na programy, je třeba konstatovat, že zpravidla nejsou zveřejněny a je s nimi proto třeba zacházet jako s díly neuveřejněnými;

-ustanovení o morálních právech (článek 6 bis) bude ve většině případů prakticky neaplikovatelné, neboť mnohdy nelze skutečného autora programu identifikovat,

-délka ochrany by měla být stanovena jako pro díla slovesná, případně jako pro díla kinematografická, podle toho, jak určí autor;

-výlučné právo autora nebo jinak určené osoby týkající se povolení dalšího zpracování díla by se mohlo aplikovat na programy s tím, že za zpracování je třeba považovat převedení programu z jedné formy do druhé, např. z programovacího (zdrojového) jazyku do cílového jazyku; zde ovšem nejde o překlad v klasickém slova smyslu, totéž platí o tzv. dekompilaci programu, tj. o jeho převedení do formy, v níž je patrná jeho struktura;

-dále bude třeba vypracovat pravidla o kopírování programů bez souhlasu autora, neboť pravidla týkající se literárních a uměleckých děl jsou nepoužitelná.

Jestliže vyjdeme z charakteru díla a způsobu vzniku díla podle [249], musí pojetí software jako autorského díla splňovat následující znaky:

-musí být výsledkem tvůrčí činnosti autora, jde zejména o naplnění znaku autorské individuality a původnosti díla,

-musí se jednat o dílo literární, vědecké či umělecké, přičemž důraz je kladen na formu vyjádření díla,

-dílo ve smyslu [249] vzniká vyjádřením myšlenky formou, která zprostředkuje její objektivní vnímatelnost.

Jak uvádí [179], diskuse zda přiznat počítačovým programům charakter autorského díla se soustřeďovala zejména na problém, nakolik je naplněn znak autorskoprávní individuality díla. Byly pochybnosti o tom, zda autor-programátor, pokud vychází z daných a stejných výchozích podmínek, matematických postupů a vědeckých metod, možností a determinovanosti prostředí výpočetního systému, může natolik uplatnit svou individualitu a vlastní tvůrčí myšlení, aby vniklo nové původní dílo nesoucí autorskoprávní rysy. Novelou autorského zákona v roce 1990 byly mezi díla chráněná z titulu autorskoprávní ochrany zařazeny výslovně počítačové programy. Byly tak oficiálně ukončeny spory o tom, zda je vůbec možné považovat programy za autorské dílo. Ovšem plné objasnění této problematiky to nepřineslo a ani přinést nemohlo. Právní charakter programů však tím byl konsolidován a jelikož zároveň nedošlo k modifikaci pojmových znaků autorského díla, byl de facto programům přiznán i znak individuality. Pravděpodobnost, že naprosto totožný program bude nezávisle na sobě vytvořen několika programátory je srovnatelná se situací u jiných autorských děl. Každý programátor však s výhodou využívá rutinní programy, tj. programy řešící natolik jednoduchý problém či natolik známé a často řešené postupy, že v nich znaky individuality lze nalézt jen stěží. Některé programy, obsahující často řešenou problematiku, pak obtížně dokazují svoji původnost a mohou být považovány za rutinní. Kritérium, kdy se tak již stane, v zákoně výslovně zmíněno není a bude se spíše řídit soudní praxí. V současnosti jsou např. hojně nabízeny programy pro vedení účetnictví ať již jednoduchého či podvojného. Jelikož výrobci vycházejí ze stejného zadání a podmínek daných zvyklostmi v tomto oboru, ze zákona o účetnictví a z požadavků praxe, jsou logika a principy, na kterých je program založen, v převážné míře determinovány. I zde však podle názoru [179] zůstává prostor pro uplatnění tvůrčí individuality, pokud se výsledný produkt nějakým způsobem prokazatelně odlišuje či výrazně převyšuje ostatní průměr.

Informace obsažené v databázových systémech, pokud nejsou výsledkem tvůrčí činnosti autora, není možné zahrnout pod autorskoprávní ochranu. Avšak i na jejich sesbírání, setřídění, vyhodnocení či ověření, bylo nutné často vynaložit značné úsilí či dokonce tvůrčí invence, a proto by bylo třeba i k tomu přihlédnout při hodnocení podle výše zmíněného kritéria. Protože význam zpracování dat pomocí počítače spočívá především v rychlosti s jakou jsou zvládnuty velké objemy informací, jsou tyto aplikace časté a přinášejí uživateli

značné výhody a zisk. Výhrada, kterou zákonodárce užil v demonstrativním výčtu děl spadajících do působnosti autorského zákona podle §2, odst.1 *„... pokud splňují pojmové znaky děl podle tohoto zákona...“*, má zřejmě podle [179] za cíl přihlédnout k výše uvedené skutečnosti. Zároveň však může být chápána jako restriktivní, s nepříznivým vlivem na právní jistotu autorů programů. Snad proto někteří tento jinak velmi pozitivní krok hodnotili jako přechod od bezprávního stavu k právním zmatkům.

Argumentem mluvícím ve prospěch autorskoprávní ochrany software je skutečnost, že každý program může být vyjádřen i ve formě textu - např. ve zdrojovém tvaru, kdy může připomínat i literární dílo. Podle [179] výklad znaku objektivní vnímatelnosti sice nezahrnuje požadavek obecné srozumitelnosti, ale pokud chceme počítačové programy chránit a přesně dodržet analogii s literárním dílem, museli bychom chránit až projev programu po spuštění na počítači. Teprve tehdy můžeme pozorovat to, co nám autor díla - programátor chtěl sdělit. Podobnost zdrojového textu programu s dílem literárním je čistě náhodná. Tento text musíme chápat v konečné fázi jako posloupnost řídících instrukcí procesoru počítače. Číst zdrojový program ve smyslu čtení literárního díla je i pro specializovaného odborníka obtížné a jde spíše o myšlenkovou simulaci činnosti počítače. Jde o odhad, jaký výsledný efekt instrukce po spuštění na počítači vytvoří. Vzhledem k tomu, že hlavním prostředkem komunikace s počítačem je ve většině případů monitor počítače - obrazovka, vyvstává zde dokonce možnost chránit software snad formou děl kinematografických či uměleckých. Autor studie [179] však zdůrazňuje, že si stěží lze představit dopad pro právní praxi, včetně všech obtíží při dokazování porušení práv k takto pojatým dílům.

Příliš rozsáhlá ochrana programů, by však (a to nejen podle názorů presentovaných ve studii [179]) mohla být i na škodu věci. Programy na rozdíl od ostatních děl podléhají neustálému vývoji a příliš striktní ochrana by takový vývoj mohla ohrozit. Vezměme si jako příklad velmi známý systém programů *Windows* firmy Microsoft, jehož úspěch je z velké části založen na lákavém designu a v principu velmi jednoduchém způsobu komunikace uživatele s počítačem. Na podobném myšlenkovém základě byly již založeny i jiné programy. V programech Windows však byly dotaženy k poměrné dokonalosti a úspěšnosti. Pokud by v dané situaci bylo možné chránit tyto myšlenky jako tzv. *user interface*, tj. specifický způsob komunikace s uživatelem, mohla by tato firma získat monopolní postavení na trhu, což by se jistě nepříznivě projevilo na rozvoji softwarového průmyslu. Uživatel by pak jednoznačně dával přednost programům s jednoduchým a hlavně jemu známým prostředím, před nutností učit se ovládat nový, i když třeba funkčně lepší program.

Význam monopolizace uživatelského rozhraní. Aby program mohl vykonávat své funkce musí spolupracovat s hardware, operačním systémem, obslužnými programy, periferiemi atd. Tato spolupráce probíhá také prostřednictvím přesně definovaných rozhraní. Neznalost těchto definicí by znemožnila programátorům tvorbu dalšího software. Zde platí, že kdo monopolizuje rozhraní, může ovládnout celou příslušnou část trhu. Opatření, kdy zákon ukládá výrobcům (zejména výrobcům hardware) zveřejňovat údaje o rozhraní, nemusí být vždy dostatečná, jak podle [179] ukazují zkušenosti z USA.

Problémy dekompilace - zpětné analýzy programu, označované také jako *reversní inženýrství*. Podle [179] si představme situaci, kdy programátor - analytik vytvořil původní řešení problému, navíc v něm uplatnil řadu nových myšlenek, ale řešení některých atributů programu není na odpovídající výši. Práva k užívání poskytne jisté firmě, která se na základě zjištěných nedostatků programu rozhodne provést zpětnou analýzu. Technika, která ji to umožňuje, je běžně dostupná a v určitých případech je možné získat tímto způsobem i zdrojový text programu. Na základě původní analýzy pak napíše nový program, jemuž původní software nemůže konkurovat. Jde o příklad zneužití a porušení autorských práv autora programu. Situaci však nelze vyřešit jednoduchým zákazem dekompilace. Ta tak patří k nejsložitějším otázkám právní ochrany software, úzce souvisí s protikartelovými zákony a s ochranou volného trhu. Autorský zákon tuto problematiku výslovně neupravuje. Významným počinem je v tomto směru směrnice *ES* [54]. V článku 6 se touto problematikou speciálně zabývá. Výslovně zakazuje dekompilaci pro vytvoření konkurenčních programů, což by ve svém důsledku znamenalo porušení autorského práva. Z důvodů výše uvedených ji však umožňuje, vyžaduje-li to zajištění vzájemného funkčního propojení mezi systémy. Tuto možnost však váže na přesně vymezené podmínky a zároveň s tím ukládá určité povinnosti.

Pro zajištění účinnosti právní ochrany software je nezbytné využívat i *mimoprávní prostředky ochrany*. Ty spočívají v zabezpečení a vytvoření takových technických a organizačních opatření, umožňujících efektivní využití právních prostředků. Ve většině případů by jinak uplatnění právní ochrany nebylo dostatečně účinné. Technických opatření je mnoho, [179] uvádí jen některé příklady. Lze např. zabránit pořízení neoprávněné kopie počítačového programu fyzicky - vhodnými technickými opatřeními. Principy bývají různé a stále se vyvíjejí. Jak však vyplývá z údajů o počtu pirátských kopií, pro specializované pirátské firmy nepředstavují nepřekonatelný problém. Navíc oprávněným uživatelům komplikují někdy již tak dost složitou instalaci programu a tím odrazují budoucího uživatele. V našem prostředí máme např. neblahé zkušenosti s legálně provozovaným programem analýzy dotazníkových schémat *PCSASD*, u něhož vlivem firemních pojistek nelze pořídit ani zákonem povolenou zálohu instalačního programu. Od podobných způsobů ochrany většina firem nyní ustupuje. U drahého software jsou často používané tzv. *„hardlock“ ochrany*. Jde o „černou skříňku“, jejíž přítomnost na určeném portu počítače je nutná pro chod programu. Dodává se spolu s programem v počtu zakoupených licencí. Mezi technické prostředky, které by mohly pomoci při dokazování porušení autorských práv lze také zařadit tzv. *„fingerprints“*. V principu jde o zahrnutí jedinečné posloupnosti znaků do těla programu a tím umožnění pozdější identifikace v případě zneužití programu. Další možností ochrany software jsou různá organizační opatření a interní směrnice organizací. Tato oblast by se mohla stát velmi silným způsobem ochrany software. Člověk, na jehož chování závisí účinnost této ochrany nejvíce, však může být v komplexu opatření jak nejsilnějším, tak i nejslabším článkem. To ostatně platí nejen pro tuto oblast.

Jak je uvedeno v závěru studie [179], absolutní ochrana je tedy počítačovým programům poskytována z titulu ochrany autorskoprávní s výše uvedenými specifiky. V

konkrétních případech lze však současně s autorskoprávní ochranou využít i dalších právních institutů a mimoprávních opatření a vytvořit tak vzájemně provázaný, tedy i účinnější systém ochrany. To se jeví v případě dat a databází většinou nezbytné, vzhledem k problematičnosti ochrany dat na základě autorského zákona. Výkon práv k software s sebou nutně nese omezení soutěže. V některých případech se firmy snaží zneužitím těchto práv zajistit si dominantní postavení v určité oblasti a narušují tak pravidla hospodářské soutěže. Ovšem podle [179] jen takové uplatnění a výkon práv je legitimní, které jim skutečně podle práva náleží.

**

Český „informační zákon“. Jak uvádí autor studie [214], v podmínkách našeho státu vznikla za posledních několik desítek let řádově stovka právních norem různé právní síly, které více či méně podrobně a komplexně upravovaly vznik, existenci a fungování nejrůznějších informačních systémů o občanech, počínaje matrikami, přes evidenci motorových vozidel, rejstřík trestů, obchodní rejstřík až třeba po evidenci osob závislých na alkoholu a jiných návykových látkách. Velká část těchto předpisů však ochranu informací neupravuje vůbec, nanejvýš využívá obecných norem platících pro státní, služební či obchodní tajemství, ochranu osobnosti, ochranu průmyslových práv apod. Těm zbývajícím zpravidla chybí jednotící linie. Normou nejvyšší právní síly v této oblasti je v současné době *Listina základních práv a svobod,* která v kapitole základních práv přiznává občanům mimo jiné práva

-na nedotknutelnost osoby a jejího soukromí,

-na ochranu lidské důstojnosti, osobní cti, dobré pověsti a jména, soukromého a rodinného života,

-na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Konkrétní ucelenou obecnou normou, která upravuje práva a povinnosti provozovatelů, resp. dalších zúčastněných osob, při provozování informačních systémů s osobními údaji, tedy českým „informačním zákonem“, je *zákon č. 256/1992 Sb., o ochraně osobních dat v informačních systémech*, viz [250]. Ten směřuje k důsledné ochraně osobních informací a v našem zákonodárství poprvé právně definuje některé zásadní pojmy z informatiky, dále pak ustanovuje pravidla nakládání s informacemi. Tato pravidla jsou pochopitelně chápána obecně jako minimální program pro veškeré informační systémy bez ohledu na to, kdo je jejich provozovatelem. Zejména se však týká i těch informačních systémů, které vznikly již dříve na základě jiných zákonů. Zdůrazněme, píše autor [214], že zákon se týká osobních údajů, které charakterizuje pouze jako informace vztahující se k určité osobě. V této podobě je to formulace natolik široká, že bez problémů zahrne v podstatě cokoliv, co se konkrétního člověka osobně týká. Rovněž pojem informačního systému je definován tak obecně, že by bylo možné při troše fantazie si pod ním představit papírovou kartotéku nebo snad i diář za předpokladu, že slouží cílevědomému a systematickému shromažďování, zpracování, uchovávání a zpřístupňování informací. Zákon zdůrazňuje i zvláštní ochranu informacím, které vypovídají o osobnosti a soukromí dotčené osoby, jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích,

vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech. Tyto „citlivé“ informace lze shromažďovat pouze tehdy, stanoví-li tak zvláštní zákon nebo se souhlasem dotčené osoby. Poněkud problematický se zde zdá termín „osobnost a soukromí“, který není nijak blíže definován a může být tedy pojímán v podstatě v jakékoliv šíři. Jistě by si proto zasloužil bližší konkretizaci, nejlépe v rámci případné novely tohoto zákona nebo alespoň v soudní praxi. Podle tohoto zákona však navíc vznik a existence informačního systému obsahujícího taková speciální data podléhá registraci u zvláštního státního orgánu, pro tento účel zřízeného. Jádrem tohoto zákona je stanovení povinností provozovatele informačních systémů, mezi něž patří dost zásadní omezení případné libovůle těchto subjektů, byť třeba dobře a racionálně míněné. Ve stručnosti odpovídající účelu tohoto textu jde o povinnost

-provozovat informační systém v souladu s účelem, pro který je zřízen,

-získávat informace rozsahem přiměřené účelu, pro který je informační systém zřízen, zejména se vystříhat shromažďování nadbytečných údajů,

-ověřovat přesnost používaných informací a podle potřeby je aktualizovat,

-náležitým způsobem v informačním systému označovat nepřesné a neověřené informace,

-neuchovávat v informačním systému nepravdivé informace,

-zamezit sdružování informací a informačních systémů sloužících k rozdílným účelům, pokud zvláštní zákon nestanoví jinak,

-získávat informace náležitým způsobem, získávat je pod krytím jiným účelem nebo jinou činností lze pouze tehdy, stanoví-li to zvláštní zákon,

-uchovávat informace umožňující identifikaci konkrétní osoby pouze po dobu přiměřenou účelu informačního systému, pokud zvláštní zákon nestanoví jinak,

-zajistit ochranu informací i celého systému před náhodným nebo neoprávněným zničením, náhodným poškozením a neoprávněným přístupem nebo zpracováním,

-stanovit práva a povinnosti všech, kdo mají k informačnímu systému přístup,

-učinit opatření, aby po skončení pracovního nebo obdobného poměru mezi fyzickou osobou a provozovatelem nemohly být informace, s nimiž nakládá příslušný informační systém, touto osobou využity; obdobně se to týká i všech ostatních, kdo mohou s těmito informacemi přijít do styku,

-poskytnout jednou do roka bezplatně, nebo za přiměřenou úhradu kdykoliv, dotčené osobě na požádání zprávu o informacích o ní uchovávaných, pokud to zvláštní zákon explicitně nevylučuje.

Poměrně důsledně je v tomto zákoně stanoveno, co se stane, když příslušné subjekty nesplní své povinnosti, resp. čeho se může občan domáhat, když s informacemi o něm se nenakládá odpovídajícím způsobem. Zpravidla se tyto nároky pohybují (podle charakteru porušené povinnosti) v kategoriích zdržení se takového jednání, odstranění závadného stavu, vydání bezdůvodného obohacení, poskytnutí zadostiučinění (omluvy, opravy), likvidace či doplnění informace a zaplacení přiměřené peněžní náhrady. A aby mozaika nepříjemných následků byla úplná, autor [214] doplňuje, že i v jiném zákoně, a to v zákoně trestním, se v posledních letech objevil §178, upravující skutkovou podstatu trestného činu *„neoprávněného*

nakládání s osobními údaji", za jehož spáchání lze uložit i nepodmíněný trest odnětí svobody. Závěrem k této problematice konstatujme, že zmíněný zákon není ideální, což má za důsledek řadu nejasností, které vznikají při jeho aplikaci. Podle [214] se dá dokonce říci, že ignorování těchto pravidel je poměrně dosti rozšířeným jevem. Nicméně právě znalost a běžné užívání zmíněných norem všemi potenciálně zúčastněnými, včetně domáhání se práv soudní cestou, může výrazně pomoci v boji s negativními jevy, včetně počítačové kriminality, týkající se ochrany osobních práv.

7.3. Softwarové pirátství a jeho formy

Podle autora příspěvku [241], *softwarové pirátství* je neoprávněné nakládání s počítačovými programy, s dokumentací a dalšími součástmi softwarových produktů chráněných především autorským právem, přičemž toto nakládání je v rozporu s platnými právními předpisy. Softwarové pirátství je pouze jednou formou protiprávních jednání, která jsou páchána v souvislosti s využitím, respektive se zneužitím výpočetní techniky. Jde však o natolik charakteristické útoky na právem chráněné zájmy, že je lze řadit k závažné počítačové kriminalitě.

Obdobně vymezuje softwarové pirátství autor studie [40], jako všechny útoky na právo autora a další práva k počítačovým programům, uvedená v autorském zákoně. *Softwarový pirát* je užívané označení osoby porušující autorský a trestní zákon.

Nyní se zmíníme stručně o jednotlivých formách softwarového pirátství.

1.Výroba software, padělatelství. Spočívá v rozmnožování a prodeji kopií počítačových programů bez souhlasu původního autora. Kopírovány jsou nejen diskety, ale i celé sady, obalové krabice, manuály a různé instrukční materiály, prostě vše, aby byl zákazník oklamán a domníval se, že získal pravý software. Tento typ trestné činnosti se vyskytuje nejen ve světě, ale i u nás. Dopouštějí se jí jak fyzické osoby, tak i firmy. Konkrétně lze uvést případ tiskárny *Median a.s.* z Karlových Varů, která přijala zakázku v hodnotě 100 mil. Kč na výrobu počítačových programů bez toho, aniž by zkoumala, zda k jejich replikování dal souhlas autor. Ve věci bylo sděleno obvinění odpovědné osobě pro trestný čin porušování autorských práv podle §152 trest. zákona.

2.Distribuce a prodej hardware. Obchodníci s hardwarem velmi často distribuují nelegálně software, instalovaný na počítačích, které prodávají. Cíl, který tímto sledují spočívá v získání konkurenční výhody nad jiným prodejcem hardware. Software však instalují na prodávané počítače bez řádné smlouvy s autorem. I tento případ je již zjištěn na našem území, firma *VT Data* ve Vysokém Mýtě prodávala počítače s instalovanými programy, aniž by k tomu měla souhlas autora. I zde již bylo sděleno obvinění odpovědné osobě z firmy, opět pro trestný čin podle §152 trest. zákona.

3.Užívání software. Neoprávněné užívání software je pravděpodobně nejrozšířenějším druhem počítačové kriminality. Spočívá v užívání nelegálně získaných nebo rozmnožených kopií programů. Kopie jsou získávány bez souhlasu autora a umožňují tak jedinečným

způsobem šetřit pachatelům peníze. V zemích, kde byl tento způsob užívání software rozšířen, a Česká republika mezi ně bohužel patří, mají i velcí výrobci software potíže s udržením na trhu. Policie v Praze na základě oznámení provedla již několik akcí proti uživatelům, kteří byli podezřelí z nelegálního užívání software. Na základě prohlídek počítačů lze mnohdy snadno pojmout podezření na nekalý původ používaných produktů. Avšak ověřování a důkazní činnost nebývá vždy snadná, hrozí zde dokonce osočování ze strany pachatelů na nelegální postupy orgánů činných v trestním řízení.

4.Sítě BBS. Jedná se o *„Electronic Bulletin Board System“*, kde po telefonních linkách se lze propojit na centrální počítač, na kterém je software, řídící práci sítě *BBS*. Síť *BBS* má sloužit k využívání za určitých podmínek volně šiřitelných programů, tzv. *shareware* nebo bezplatně šiřitelných programů tzv. *freeware*. Bohužel, velmi často dochází k tomu, že prostřednictvím sítě *BBS* jsou šířeny programy označené copyrightem, jejichž autoři si ponechali autorská práva. Pirátem je ten, kdo programy chráněné označením „copyright“ ze sítě *BBS* kopíruje na vlastní počítač, ale i ten, kdo do takové sítě jinak legálně získané programy posílá, protože vlastně vytváří nelegální kopie.

5.Půjčovny software. Tento způsob softwarového pirátství, který je pravděpodobně českou originalitou, spočívá v tom, že uživatel si řádně zakoupí software, vytvoří jeho nelegální kopie, které jsou potom předmětem půjčování. Takový případ byl zjištěn v Praze, kde *PC klub Dundy* kromě jiného půjčoval počítačové programy, chráněné autorským zákonem. Věc je v současné době u vyšetřovatele, který zkoumá trestní odpovědnost majitelů této půjčovny.

6.Počítačové herny. Počítačové herny jsou zvláštní formou užívání software. Je to dáno typem půjčovaného sortimentu, který je svým určením odlišný od např. kancelářského programového vybavení. Počítačové hry jsou v podstatě specifickým artiklem. Jejich prodej či distribuce jsou odlišné od ostatního software. Navíc obvykle není v této oblasti tak nepřehledná paleta autorských práv jako u „normálního“ software. V hernách je obvyklé, že na jeden technicky kvalitní počítač užívaný jako server je instalována hra, kterou je možno hrát na několika připojených počítačích. Pokud příslušná firma, legálně zastupující výrobce počítačových her, nedá souhlas ke komerčnímu užívání příslušné hry, jde vlastně provozováním takové hry o porušení autorských práv. Je tedy i na policii, aby se k tomuto problému postavila a následně byl schopen reagovat celý trestní systém. Výmluvy na nedostatečnou legislativu jsou v tomto případě liché.

Morální aspekty softwarového pirátství. Morální stránka trestné počítačové činnosti a především softwarového pirátství představuje zajímavý problém. Nabízí se ona věčná otázka, co nutí některé občany, aby páchali trestnou činnost. V České republice se používá velmi mnoho softwarových produktů nelegálně. Autor článku [36] uvádí, že v některých případech se hovoří až o 70% nelegálního software. Kdo se dostal do kontaktu s výpočetní technikou před rokem 1989, pamatuje, jak těžce bylo možno sehnat kvalitní počítačový program. Příčinami bylo i embargo na dovoz špičkové technologie, do níž byl zahrnut i software. Potřeba software byla velká, proto se k nám dostával různými cestami a byl v naší zemi všemožně šířen i nelegálním způsobem. Této činnosti přihlížel stát jen z povzdálí přesto, že platila ustanovení §152 trestního zákona v podobném znění jako dnes.

Stíhání za tento trestný čin bylo velmi neobvyklé a kuriózní. Zajímavou úlohu zde sehrálo vzdělání a právní informovanost občanů. Generace dnešních třicátníků nebyla po celou dobu povinného i dalšího, včetně postgraduálního vzdělávání seznámena s ustanoveními trestního zákona, jako základního vodítka v orientaci lidského chování, pokud jde o nedovolenou činnost společností postihovanou. Každý, kdo není profesionálně nucen znát trestní nebo i přestupkový zákon, se řídí intuitivně přirozeným citem ke spravedlnosti, právu a morálce. Mnohdy je pak pro takového jedince překvapením, co všechno může být trestným činem a naopak; že existuje jednání, které je sice morálně odsouzeníhodné, nicméně však nikoliv trestné. Každý občan by měl mít jakési právní minimum, na kterém postaví své každodenní chování. I svůj postoj k nelegálnímu software. Nelze říci, že základním důvodem odmítání softwarového pirátství musí být strach z trestního postihu. Na první místo lze položit úctu k duševnímu vlastnictví. Někteří jedinci však nezdůvodňují porušování autorských práv zištnými cíli, nýbrž odmítáním principů kapitalistické společnosti, světové globalizace a extrémních zisků softwarových gigantů. Duševní vlastnictví považují za universální hodnoty lidstva a jakékoliv omezování jejich šíření a aplikací za nemravné.

Ovšem pouze jednoznačně záporný postoj k softwarovému pirátství, reprezentovaný společenským odsudkem a respektováním duševního vlastnictví, je v daných podmínkách jedinou cestou k omezení tohoto nežádoucího fenoménu.

Postih počítačového pirátství podle [110] je možný, když pachatel úmyslně, bez svolení autora (tj. bez řádného oprávnění) kopíruje programové vybavení a dále je prodává za účelem zisku, nebo prací na tomto nelegálně získaném programovém vybavení dosahuje zisku pro sebe nebo jinou osobu. Základní trestní odpovědnost za tuto činnost zakládá §152 trestního zákona - porušování autorských práv. Při postihu softwarového pirátství přicházejí v úvahu i uplatnění dalších ustanovení trestního zákona:

-§150 trestního zákona - porušováni práv k ochranné známce, obchodnímu jménu a chráněnému označení původu,

-§149 trestního zákona - nekalá soutěž, neboť vyrobený a distribuovaný plagiát parazituje na dobré pověsti oficiálního výrobce.

V praxi jde o činy, kdy pachatel

-užívá programy zaměstnavatele ke svým soukromým účelům; obvykle se tak děje přehráním na jím obsluhovaný služební nebo vlastní počítač,

-užívá nelegálně získané programy, které pořídil na počítačích zaměstnavatele,

-provozuje program na větším počtu počítačů, než bylo smluvně dojednáno,

-zasahuje do programu, provádí změny a úpravy programu,

-prodá nebo poskytne program další osobě,

-brání zaměstnavateli užívat program vytvořený zaměstnancem ke splnění povinností vyplývajících z pracovního poměru.

Orgány činné v trestním řízení by měly akceptovat skutečnost, že vznikne-li porušením práva závažná újma nemajetkové povahy, má autor právo na zadostiučinění v peněžní částce. Jestliže autorovi porušením jeho práv vznikla škoda, má právo domáhat se její náhrady

v občanskoprávním řízení. Pokud ovšem někdo s předmětem autorského práva neoprávněně nakládá způsobem, který přísluší autoru nebo jinému nositeli autorského práva, může být jeho jednání kvalifikováno jako trestný čin porušování autorského práva podle §152 trest.zákona. Pro vznesení obvinění postačí, jestliže některá osoba nahrála programy nebo je poskytla jiné osobě. Není-li např. osoba, která odpovídala za provoz programů v organizaci zjištěna, případně neexistuje-li tato osoba, připadá v úvahu trestní stíhání statutárního zástupce, který odpovídá za organizaci.

Vývoj počítačového pirátství. V současné době počítačoví piráti přecházejí na nejmodernější metody, obrazně řečeno přezbrojují, viz např. [57]. Často se objevují pirátské CD-disky, mnohdy holé, bez jediného označeni či etikety, takže není možné určit, kdo je jejich „výrobcem“ , ani jaký je jejich obsah. Jindy sice označení mají, ale falešné. Nechybí na nich zpravidla žádné z atraktivních novinek počítačového trhu – počínaje nejnovějšími verzemi *Windows,* produkty *Microsoft Office* a konče nejnovější verzí *AutoCAD*. Autor článku [57] zjistil, že na jednom pirátském CD-disku měly programy hodnotu asi půl milionu Kč, kdyby byly pořízeny legálně. Tento nenápadný stříbrný disk se však na černém trhu nabízel za cenu 2000 Kč. Počítačoví piráti mají tradici jdoucí ruku v ruce s rozvojem světa počítačů a programů. Ovšem největšího rozmachu zaznamenalo pirátské řemeslo až s nástupem osobních počítačů. První generaci počítačových pirátů představovali hackeři a crackeři. Tehdy se specializovali především na počítačové hry, které v počátcích éry domácích a osobních počítačů představovaly převážnou část jejich programového vybavení. Majitelé těchto malých počítačů příliš nedbali na autorská práva a měnili si své oblíbené programy mezi sebou. Burzy programů, kde se v podstatě pirátským způsobem šířily programy mezi veřejnost, známe i z doby normalizačního vývoje předlistopadového Československa. Až na výjimky šlo o šíření nezištné a vlastníky autorských práv více či méně trpěné. Pokud chtěl autor programu zajistit, aby se jeho výtvor nedal lehce kopírovat, vytvořil pro to nějakou speciální ochranu. Za všechny lze uvést nestandardní záznam dat na pásek nebo na disketu, které tak nešly běžným způsobem zkopírovat, nebo nutnost zadání hesla při spuštění programu. Heslem bylo přitom obvykle náhodně vybrané slovo z originální příručky k programu. Takže kdo neměl originální balení, do programu se nedostal. A to byla právě příležitost pro hackery a crackery. Přes evidentně protizákonnou činnost je třeba se před jejich „tvůrčí činností“ (o seriózní práci lze hovořit obtížně) sklonit, neboť tito piráti se museli naučit velmi dobře detailnímu ovládání strojového kódu počítače a v něm pak hbitému programování. Ochranu programu odstraňovali tím, že příslušnou pasáž prostě přeprogramovali. Na rozdíl od těchto tvůrčích typů se však stále více objevovali piráti, kteří za úplatu zkopírovali libovolný program. Stačilo si jen vybrat. Ovšem tato činnost se už výrobcům programů příliš nelíbila - vždyť ceny dnešních profesionálních programů, zejména některých specializovaných, dosahují částek několika desítek až stovek tisíc korun. Pokud tedy někdo takový program prodá třeba za „pouhých“ pět tisíc, způsobí tím držiteli autorských práv výraznou ztrátu. O neoprávněném obohacování piráta, který za půl hodiny sezení u počítače vydělá totéž co dělník za měsíc, ani nemluvě. A tak se začali výrobci programů více starat o osud svých produktů. Autorská práva získala na vážnosti, vznikly specializované organizace na ochranu počítačových programů a dat, jako je například BSA, počítačová

kriminalita se stala součástí trestního kodexu mnoha vyspělých zemí světa. Noviny přestaly přijímat inzeráty typu *„prodám levně programy“*, změnila se i obchodní politika v oblasti prodeje programů. Koupíme-li si dnes program od některé renomované firmy (jako je například Microsoft) a zaregistrujeme se jako řádný uživatel tohoto programu, začne o nás tato firma pečovat. Například budeme po určitou dobu bezplatně dostávat informační časopis této firmy, získáme výrazné slevy při nákupu dalších programů stejného výrobce apod. Oproti minulosti také výrazně vzrostla kvalita i kvantita manuálů a příruček, které se s programy dodávají. Často tak dochází k paradoxní situaci, že kdybychom tyto knihy kupovali samostatně, vyšlo by nás to dráž než celý program. I to je forma ochrany proti počítačovým pirátům.

Organizované počítačové pirátství. Drobní piráti, živící se nelegálním kopírováním programů, však na počítačovém trhu parazitují i nadále. Jak uvádí [57], navíc se objevil nový fenomén - organizované počítačové pirátství, které často dosahuje téměř průmyslového formátu. V některých rozvojových zemích, ale i v hospodářsky vyspělých státech není příliš obtížné založit továrničku, která by vytvářela dokonalé kopie originálních programů - od disket s programy přes příručky až k barevným obalům, k nerozeznání od originálu. Pak už pouze stačí tyto pirátské duplikáty různými „nelegálními kanály“ podvrhnout na počítačový trh - a dílo zkázy je hotovo. Že jsme si koupili pirátskou kopii a nikoliv skutečný originál zjistíme až ve chvíli, kdy se jako slušní a poctiví uživatelé snažíme zaregistrovat u původního výrobce. Ten pochopitelně odhalí nepravost naší kopie, ale jako seriózní firma nás (většinou) přesto zaregistruje, i když tím výrazně tratí. Takové organizované pirátství dokáže napáchat nemalé škody, takže se na jeho odhalení a prevenci stále větší měrou podílejí samotní výrobci programů. Metody ochrany originálního software přitom nemalou měrou připomínají způsoby ochrany bankovek proti padělání, takže se dnes běžně setkáme s registrační kartou, která je vybavená vodotiskem, hologramem nebo jinými ochrannými znaky známými z peněžnictví.

Zdánlivě bezpečné CD-disky. Když se na počítačovém trhu začaly objevovat cenově dostupné mechaniky CD-ROM na snímání CD-disků, spatřovali mnozí výrobci programů řešení svých potíží právě v přechodu na tento fenomén, viz [57]. Stříbrný CD-disk je oproti disketám skutečně výhodnějším médiem - je mnohem odolnější proti poruchám a poškozením, jeho výroba je jednodušší, vejde se na něj velké množství dat a hlavně se nedá (tedy alespoň do nedávné doby) v amatérských podmínkách kopírovat. V době, kdy fenomén CD-ROM zdomácněl v našich počítačích, stála čtecí mechanika CD řádově několik tisíc Kč, takže byla srovnatelná s cenou pevného disku. Zapisovací neboli „vypalovací“ zařízení bylo možné pořídit za částku šesticifernou, což je položka pro řadového piráta přece jen za hranicí možností. A tak není divu, že mnozí výrobci programů rychle přešli na nový typ nosiče. Poměr mezi programy na disketách a CD stále více vyznával ve prospěch magneto-optických kotoučků. I uživatelé rychle pochopili, jaké výhody s sebou přináší technika CD-ROM. Stačí si porovnat instalaci Windows 95 z disket nebo z CD-disků. V prvním případě strávíme u počítače minimálně hodinu a celou dobu musíme být ve střehu, připraveni vyměňovat diskety v mechanice. Ve druhém případě vložíme CD-disk do mechaniky a můžeme na chvíli i odejít od počítače. Po návratu nás již přivítá vstupní obrazovka nových Windows. Velká kapacita

CD-disků rovněž uvolnila ruce programátorům, kteří již nebyli limitováni malou kapacitou pevných disků našich počítačů a mohli začít vytvářet projekty v rozsahu několika set megabytů. Nemluvě o možnostech kombinovat klasická programová data s digitálním zvukem nebo obrazem. Na platformě CD se totiž výrobci různých optických disků vzácně shodli nejen na stejné velikosti, ale i na jednotném formátu dat, takže na počítači nemusíme přehrávat pouze programové a datové CD-ROM disky, ale i „klasické" zvukové Audio CD, obrazové Video CD a dokonce i fotografické disky Kodak CD. A když to všechno spojíme dohromady na jeden disk dostaneme *multimédia*. Nejen tyto velké projekty velikosti několika set megabytů zaplňují CD disky. Výrobci začínají na CD-disky přenášet i programy, které by se bez problémů vešly na několik klasických disket. Podle [57] jsou totiž obě média cenově srovnatelná, takže není většího rozdílu, koupíme-li si program na disketách nebo CD-disku. I když je takový CD-disk často z větší části prázdný, pro výrobce má takové řešení značnou výhodu - disk se nedá v amatérských podmínkách zkopírovat. Kdo je ochoten investovat do dnes již celkově dostupného vypalovacího zařízení pro CD-disky, mívá zpravidla dobře prozkoumaný trh a zajištěný odbyt, aby se mu tato transakce co nejvíce vyplatila.

Jak uvádí [57], *v současné době již ani CD-disky nejsou bezpečné.* Miniaturizace a výrazný pokles cen zapisovacích mechanik CD-ROM i dostupnost prázdných CD-disků na trhu způsobily, že jedna z největších výhod tohoto média - totiž nemožnost amatérského pirátského kopírování - již patří nenávratně minulosti. Vypalovací mechaniky CD nejsou cenově nedostupné pro širší okruh nadšenců, zdá se, že pokles cen v této oblasti bude ještě pokračovat. Existují již i interní zapisovací CD mechaniky – tedy vestavitelné přímo do personálních počítačů. Přijatelné cenové relace samozřejmě nemohli nechat programoví piráti bez povšimnutí - a tak se mnozí z nich rychle přeorientovali na nový datový nosič. Médium, ve které výrobci software vkládali své naděje v souvislosti s ochranou svých produktů proti černému šíření, se tak paradoxně obrátilo proti nim. Vezměme si například datový *Microsoft Office for Windows* - vytvořit kopii 40 disket dá i zručnému pirátu hodně práce; jenom hodinu bude tyto diskety formátovat, další hodinu až dvě bude kopírovat. Vypálit CD-ROM se stejným programovým balíkem trvá několik desítek minut - a to ještě většina disku bude prázdná! Takže tímto způsobem vznikají neuvěřitelné „megabalíky" programů, jejichž skutečná katalogová hodnota nezřídka dosahuje několika set tisíc korun. Vytvořit takové CD z připravených dat na pevném disku nebo jiném CD-disku je záležitost nejvýše hodiny - a navíc téměř bez potřeby lidské asistence. V poslední době se objevily na trhu zapisovací mechaniky s výrazně zrychleným režimem vypalování, takže uvedené časy je možné ještě výrazně snížit. Není potom divu, že takovému pirátu stačí za podobné CD provize kolem 2000 Kč. Počítačoví piráti způsobili přechodem na CD-disky výrobcům programů ještě i další problémy. Výrobci programů budou muset vymýšlet nové metody ochrany svých produktů. Nekalé aktivity byly navíc rozšířeny nad rámec počítačového světa, neboť piráti na svých „vypalovačkách" jsou schopni vytvářet nejen disky datové, ale i hudební nebo filmové. A protože přehrávač CD-audio disků již v našich domácnostech zcela nahradil historický gramofon s magnetodynamicknu přenosovkou a rychlostí 33 otáček za minutu, mohou začít uspokojovat i zájemce v této oblasti. Pokud oficiální zahraniční hudební CD stojí asi 500 Kč, kdo by nedal přednost pirátské kopii za polovinu této částky? Podle studie [57], nové pirátské

vlny by se tedy neměli obávat pouze prodejci programů pro počítače, kteří již její účinek pociťují jako výrazný pokles prodeje software, a1e také prodejci hudebnin, které může zasáhnout v nejbližších dnech.

V roce 1999 odhalili na Chebsku naši kriminalisté dvě domácí dílny, kde počítačoví piráti tajně kopírovali programy za stovky tisíc korun. Oba případy jsou výjimečné tím, že zatímco softwarové pirátství je v tuzemsku hojně rozšířené, stále se daří odhalovat jen zlomek nelegálních uživatelů, natožpak výrobců nelegálních programů. První z dopadených pachatelů byl pětadvacetiletý muž z Mariánských Lázní, který více než půl roku vyráběl nelegální kopie počítačových programů různých firem. Ty nabízel prostřednictvím inzerátů v *Annonci* a více než sto osmdesáti odběratelům jich prodal za sto šedesát tisíc korun. Vyšetřovatel muže obvinil z porušování autorského práva a neoprávněného podnikání. Totéž čeká i druhého pachatele z Mariánských Lázní, který má na svědomí tutéž činnost. Prodal programy nahrané na třech stovkách CD-disků za více než dvě stě tisíc korun. Policisté zjišťovali, jaká byla mezi oběma případy souvislost. Při domovních prohlídkách zajistili zařízení, s jehož pomocí muži vypalovali programy na čisté kompaktní disky. Za což může být udělen trest až dva roky odnětí svobody. Statisícové škody, které dopadení piráti způsobili firmám, jejichž programy prodávali, jsou jen určitým zlomkem celkových ztrát. Z noticky [220] vyplývá, že každý rok způsobí počítačoví piráti v tuzemsku nositelům autorských práv škody za osm miliard korun. Podle *Agentury na ochranu softwaru*, která se zabývá bojem proti počítačovému pirátství, se odhaduje, že asi šedesát procent všech počítačových programů v České republice je nelegálního původu. V roce 1999 ve sdělovacích prostředcích proběhla zpráva o počítačovém pirátství neobvyklého rozsahu. Dvě osoby byly ve švédském hlavním městě zadrženy pro podezření z padělání a nelegálního prodeje počítačových programů v gigantickém měřítku. Podle stockholmského deníku Metro zřejmě zadržení prodali pomocí Internetu nelegálně kopírované programy v celkové hodnotě přes 100 mil. švédských korun (přes asi 4oo mil. Kč). Padělání se týkalo především programů *Office* a počítačových her. Při domovní prohlídce bylo u zadržených objeveno celkem 12 500 takovýchto programů.

**

Piráti z Internetu porušují práva hudebního průmyslu. Podle posledních zpráv ČTK [81], citelnou hrozbou pro vydavatele hudebních nosičů je jednoduchost se kterou mohou lidé po celém světě získat nahrávky svých oblíbených písní a skladeb zdarma. I to je totiž možné díky Internetu. Na celosvětové internetové síti stačí zadat jakýkoli vyhledávací program na *www* a napsat *MP3* -označení technologie, která umožňuje majitelům počítačů nahrávat hudbu v kvalitě CD nosiče. Občas narazí fanoušek, který hledá hudbu, na písně legálně nabízené hudebními vydavatelstvími k prodeji, které si může nahrát až poté, když zadá číslo kreditní karty. Nejčastěji se ale objeví některá z tisíců *webových* stránek nabízejících pirátské nahrávky známých zpěváků a hudebníků. O jak rozsáhlou záležitost jde? Po slovu *sex* je označení *MP3* nejčastěji vyhledávaným řetězcem na *www*. Obavy kapitánů nahrávacího průmyslu, vzbuzované širokým spektrem lidí, kteří hudbu přes Internet získávají, jsou tak velké, že dochází k dosud nepředstavitelné věci - hudební průmysl zahájil válku proti všem hudebním pirátům. V uplynulých dvou letech se *Asociace amerického nahrávacího průmyslu*

snažila dosáhnout zrušení webových stránek nabízejících pirátské nahrávky zasíláním právních varování a informativních dopisů operátorům a správcům těchto stránek. Zahájila i celonárodní kampaň určenou k odrazení vysokoškoláků od pirátství prostřednictvím *MP3* a snažila se přesvědčit univerzity, aby zaujaly přísnější postoj vůči studentům, kteří na vysokoškolských počítačích stahují nelegálně nahrávky. Kampaň již vedla k vyloučení nejméně tří studentů, tvrdí asociace. „Pokud jde o hudební piráty na Internetu, najdeme je a potrestáme“, říká oficiální představitel asociace. „Děti musí konečně pochopit, že to, co dělají, je nelegální a podle našeho názoru i nemorální.“

Organizované gangy hudebních pirátů. Pro hudební fanoušky, jakým je např. šestnáctiletý mladík, používající na síti přezdívku *Filter*, je sbírání *MP3* muziky posedlostí. *Filter* je členem gangu *Phreemp3,* jednoho z několika, které slídí po síti a pátrají po některé z nejnovějších nahrávek. Tyto gangy mají jednoduchý cíl - shromáždit a předat co nejvíce hudebních nahrávek zdarma co nejvíce lidem. Platí však, že čím více se výrobci snaží zabránit kopírování důmyslnými opatřeními, pro počítačové piráty je tím zábavnější tato opatření obcházet. Mladí nadšenci jsou schopni získat i nahrávky, které jsou speciálně zakódovány - kód má přitom umožňovat vstup jen přes číslo kreditní karty. Zde pak vzniká také určité nebezpečí realizace přes cizí karty se všemi finančními, ale též i právními důsledky.

7.4. Rozsah softwarového pirátství

Odhady rozsahu softwarového pirátství se v průběhu vývoje počítačové techniky u různých autorů poměrně dosti různí. Závisí to zejména na názorech na rozsah latence tohoto jevu. Lze jen těžko hodnotit případné rozdíly, které takto vznikají. Obecně lze říci, že latence kriminality tohoto typu, i přes určitý pozitivní aktuální vývoj podmínek jejího potlačování, je u nás stále ještě vysoká.

Softwarové pirátství je dnes v České republice velmi rozšířené. Jak uvádí autor příspěvku [241], v roce 1993 připadalo u nás a na Slovensku velmi přibližně na jeden prodaný počítač 0,25 prodaného počítačového programu. Efektivní práce s počítačem přitom předpokládá využívání zpravidla několika systémů. U některých známých západních softwarových produktů, ale i u úspěšných domácích se odhaduje, že více než 80% uživatelů provozuje nelegální rozmnoženiny. Hlavními příčinami tohoto stavu je dlouhodobá nemožnost legálně získat kvalitní zahraniční programy, nedostatek prostředků na nákup počítačových programů potřebných pro provoz zakoupené výpočetní techniky, nekvalitní distribuční síť programů, chybějící služby konečným uživatelům a do nedávné doby i neexistence výslovného zakotvení právní ochrany programu v příslušných právních normách.

Je třeba konstatovat, že v nepříliš vzdálené minulosti bylo nelegální kopírování i jiné porušování autorských práv k počítačovým programům bohužel pro většinu tuzemských programátorů nutností. Základní příčinou nelegálního užívání software u nás, na rozdíl od vyspělejších států světa, byla jistá rozvojová zaostalost. Nyní, v době již podstatně lepších

možností, je proto žádoucí postupné omezování pirátských aktivit, zejména pak těch, které vznikají nově v důsledku nekontrolovaného tržního prostředí a svým rozsahem mohou být značně nebezpečné především pro rozvoj českého softwarového průmyslu.

Podle příspěvku [59], celkový podíl ilegálně užívaného software v Evropě přesahuje 60% - což znamená, že tři z každých pěti používaných programů jsou buď ilegálně okopírovány uživateli nebo byly nakoupeny od ilegálních dealerů. Zůstatková hodnota těchto ilegálně zkopírovaných programů v roce 1993 činila 4,9 miliardy dolarů. Dokonce v zemích jako je Velká Británie, kde ochrana software na základě autorských práv byla průmyslem uznána již dříve a osvěta v této oblasti byla široce rozšířena prostřednictvím vzdělávacích kampaní v průmyslu, ilegální kopírování se týká stále téměř jedné z každých dvou kopií používaného komerčního aplikačního software.

K prospěšnosti a zhodnocení propagačních kampaní proti softwarovému pirátství uvedeme několik čísel hovořících o rozsahu softwarového pirátství podle studie [98] v roce 1993. Porovnáme-li situaci se softwarovým pirátstvím v USA uvidíme, že sedm programů z deseti je zákonných. Ve Velké Británii je legálních pět programů z deseti, ve Skandinávii čtyři a půl, ve Francii tři, a přibližně jeden z deseti v zemích střední Evropy. Na příkladu Velké Británie se dá ukázat, že v důsledku kampaně k softwarovému pirátství, uskutečněné v průběhu dvou let, došlo v zemi k výraznému poklesu míry nelegálního kopírování počítačových programů. Společným úsilím policie a složek a softwarového průmyslu se podařilo vysvětlit uživatelům, proč je důležité používat a zakupovat legální výrobky.

V České republice se odhaduje, že v minulých létech bylo ilegálně používáno 86 % softwarových aplikací, což představuje pro vydavatele a distributory software roční ztráty ve výši 185 milionů dolarů nebo 5,5 miliardy českých korun. Jak již bylo řečeno, tyto odhady škod jsou do značné míry fiktivní. Lze totiž pochybovat o tom, že by si uživatelé za uvedené finanční objemy software skutečně legálně pořídili. Odhaduje se, že rozsah softwarového pirátství je ještě větší ve Slovenské republice a že činí 87%, v Maďarsku 94%, v Polsku a v Rusku 98%. Porovnávací metodou byl legitimní český softwarový trh ohodnocen přibližně na 30 miliónů dolarů (zhruba 900 mil. Kč) - což je pouhá jedna šestina objemu ilegálního trhu. Tento ilegální průmysl omezuje růst legálního softwarového průmyslu v České republice i v celé Evropě. Ve společnostech vydávajících a distribuujících software je v České republice zaměstnáno více než 15 000 lidí, což představuje značný nárůst v průběhu posledních let. Ale rozsah nárůstu zaměstnanosti by mohl být mnohem vyšší, kdyby nebylo softwarového pirátství. Ohroženy jsou zejména menší společnosti - jakými jsou například *Software 602* a *APP Systems* nebo maďarská společnost *Graphisoft* - protože jejich schopnosti kompenzovat ztráty zisku způsobené přebujelým softwarovým pirátstvím jsou menší než v případě velkých mezinárodních společností a tyto společnosti jsou méně schopné vynakládat zákonné poplatky na ochranu svých práv.

Podle [40] nejzávažnější počítačovou kriminalitu tvoří trestné činy porušování autorského práva k programovému vybavení - softwarové pirátství. V současnosti je na území

republiky nelegálně užíváno více software než legálně. Odhady se velmi liší, ale je možno počítat asi s 60-70% nelegálně užívaného software. Pro srovnání - ve Spojených státech je to zhruba 30%, v západní Evropě poněkud více - asi 35 až 40%. I zde jsou výjimky, jako situace v Portugalsku a snad i v Řecku. Jsou to země ekonomicky spíše na okraji vyspělé západní Evropy. A s naším „přibližováním" se k západoevropským strukturám se k nim pravděpodobně dříve nebo později přidáme. Při pohledu na odhady uváděné v nejrůznějších pramenech, možno konstatovat, že jednotlivá čísla nejsou ani tak důležitá, jako spíše pohled na naši zemi v souvislosti s množstvím nelegálního software v zemích aspirujících na členství v EU nebo přijatých do NATO. Při porovnání je zřejmé, že Česká republika je na tom lépe než ostatní srovnatelné země. Avšak podstatně hůře, než by bylo přijatelné. Toto postavení není možno zneužít jako argument pro zmírnění tlaku na uživatele a šiřitele nelegálního software. V této oblasti máme před sebou ještě dlouhou cestu osvěty a dalších aktivit prevence, koneckonců stejně jako v řadě dalších oblastí.

V roce 1998 bylo ministrem vnitra konstatováno, že asi 70% všeho software v České republice využívají občané a často i velké a známé společnosti nelegálně, viz [6]. Proti zvyšování počtu krádeží počítačových programů je nutné učinit vše, aby se tento nepříznivý vývoj podařilo zvrátit. V zemích západní Evropy je na černo využíváno pouze asi 30% software, což pro naši republiku není příliš příznivé. Zcizování počítačových programů je také záležitost etiky. Lidé musí pochopit, že když někdo ukradne něčí software, je to rovněž krádež, jako každé jiné movité věci. Za velmi ožehavý tento problém považují i policejní orgány. Ty však často nemají kapacitu na to, aby tento druh kriminality kvalifikovaně postihovali. O nárůstu krádeží svědčí i skutečnost, že v roce 1997 bylo zaznamenáno 650 případů porušení autorského práva. V roce 1998 kriminalisté zaznamenali 1022 těchto případů se škodou 3,2 miliardy Kč. Pokud budeme softwarové pirátství posuzovat geograficky, je jasné, že nejmenší problémy s ním mají západní země. Do skupiny států, kde je Česká republika se 70% nelegálního užívání software, patří také Polsko a Maďarsko. Směrem na východ se situace zhoršuje. Do skupiny států, které mají s počítačovým pirátstvím větší problémy než my lze začlenit Bulharsko, Rumunsko, Bělorusko a Ukrajinu. Nejhorší situace však v tomto směru panuje v Rusku a v Číně, kde kradený software používá údajně téměř každý. České republice před jejím možným vstupem do Evropské unie hrozí, že bude zapsána do seznamu států, které nejsou v oblasti softwarového pirátství spolehlivé.

Pokud jde o *dynamiku rozsahu pirátských aktivit* u nás, již v roce 1994 byl uspořádán speciální seminář s širokou účastí odborníků zaměřených na represní i preventivní otázky softwarového pirátství, viz [68]. Seminář zorganizovalo a materiálně zajistilo známé sdružení softwarových výrobců - *Business Software Alliance CS*. Spolupořadatelem semináře byl i *Kriminalistický ústav, Praha, Policie České republiky*. Významný posun v nazírání na problém porušování autorských práv v té době spočíval v propojení aktivit *BSA CS* a *České protipirátské unie*, která jak známo dohlížela na dodržování práv v oblasti „video-průmyslu". Na semináři zaznělo množství zajímavých statistických údajů. Například, že zatímco v roce 1992 bylo registrováno 85 % pirátství se ztrátou 22 mil. dolarů, v roce 1993 bylo registrováno už jen 55 % pirátství se škodou 14,2 mil dolarů, v roce 1994 je registrován další pokles na

35% pirátství. Problémy byly spatřovány v obtížném důkazním řízení. Jen výjimečně je případ porušování autorských práv odsouzen. To koresponduje s novými formami pirátství, s nimiž orgány činné v trestním řízení nemají ještě žádnou zkušenost. Podle statistiky Ministerstva spravedlnosti lze vývoj v ČR za období 1995-99 charakterizovat počty vyřízených případů proti osobám podle §152 trest.zák. v rozsahu 187;159;256;475;357; počty stíhaných osob 181;159;256;281;325; počty obžalovaných osob 158;125;223;136;265; počty odsouzených osob 121;82;132;62;148. Odhad celkové účinnosti našeho trestněprávního systému vůči porušování §152 trest.řádu činí 5,2%. Tento odhad byl pořízen na základě středních hodnot uvedeného vývoje s přihlédnutím k odhadům podle normálního modelu latence se střední hodnotou příslušného rozpětí činitele deformace.

Podle příspěvku [68], v současné době nutno i nadále s ohledem na dynamiku a latenci počítačových deliktů

-řešit problematiku právních aspektů nejen softwarového pirátství, jako specifické počítačové kriminality, ale je třeba věnovat obecně pozornost podrobnému rozboru trestně právních ustanovení, které se dotýkají výpočetní techniky vůbec, respektive jejího zneužívání,

-zabývat se doposud neuspokojivě řešenou precizací pojmu *počítačová kriminalita*,

-právně zhodnotit problémy oceňováním dat, která byla zcizena spolu s počítačem,

-vyjasňovat otázky zneužívání cílených výběrů z různých (např. policejních) databází pro účely reklamy; např. individuální výběr dat z databáze policejní evidence motorových vozidel za úhradu byl v té době podle autora běžně povolen,

-přijímat fakt, že s řadou možností zneužívání dat, včetně informací z policejních evidencí, zákonodárce nepočítal,

-akceptovat skutečnost, že styl práce zainteresovaných sdružení, jejich tradiční aktivity a přístupy, po počátečních potížích a někdy i chybných krocích, již krystalizují ke korektním a účinným postupům proti softwarovému pirátství,

-přijímat a dále šířit množství praktických poznatků, včetně konkrétních metodických návodů (jako např. postupu domovních prohlídek s prvky výpočetní techniky), které vznikají ve spolupráci s experty zabývajícími se teorií i praxí postihu počítačové kriminality.

7.5. Důsledky softwarového pirátství

Důsledky softwarového pirátství jsou poměrně závažné, jde zejména o

-snížený zájem domácích i západních investorů, softwarových výrobců a obchodníků o pronikání na náš softwarový trh, vzhledem k omezené možnosti návratnosti investic z důvodů určitého zanedbání právní ochrany v praxi,

-omezení prodeje původních českých počítačových programů, které by nižší cenou mohly konkurovat na domácím trhu západním produktům,

-překážky co nejrychlejšího šíření nových počítačových programů,

-záporný vliv dnešní počítačové antimorálky na obecnou morálku, kdy značná část občanů přicházejících do styku s výpočetní technikou neoprávněné užívání programů dnes nepovažuje za jednání zasluhující morální odsouzení, o právním postihu ani nemluvě,

-rozšířené „překupnické“ dodávky západních softwarových produktů neoprávněnými šiřiteli bez doplňkových technických, konzultačních a informačních služeb,

-rozsáhlé používání technické ochrany počítačových programů snižující jejich kvalitu a ztěžující jejich ovládání uživateli,

-rozsáhlé zamoření počítačovými viry, tj. úmyslně vytvářenými instrukcemi, které ničí softwarové systémy provozované na infikovaném počítači spolu se všemi vytvořenými datovými soubory.

Softwarové pirátství v tržně pojímaných ekonomických vztazích ohrožuje zájmy stále většího množství českých softwarových podniků a programátorů, kteří nyní budují a rozšiřují své firmy. Jejich úsilí je podlamováno díky již zmíněné nejistotě návratnosti investic. To by mohlo mít, nezmění-li se situace k lepšímu, velmi nepříznivý dopad na rozvoj programátorství a na zavádění a využívání výpočetní techniky vůbec. Nutnost právní ochrany programů je nesporná. Samostatné zakotvení ochrany v zákoně však nestačí. Je třeba vytvořit příznivější podmínky pro skutečné prosazení příslušných právních norem v běžné praxi, včetně opatření k jejich vynutitelnosti. Podle zprávy ČTK, České republice vážně hrozí, že bude stejně jako dvanáct dalších zemí zapsána Obchodním úřadem vlády Spojených států do seznamu *„Special 301“*, kde jsou zaznamenány státy, které nedostatečně chrání duševní vlastnictví, viz [34]. Na veletrhu informačních technologií *Invex-Computer* to v roce 1998 sdělil odpovědný činitel z policejního prezidia. Dodal, že mezi další státy na seznamu by měly patřit i Rakousko, Německo, Maďarsko, země bývalé Jugoslávie a bývalého Sovětského svazu. Tuto skutečnost lze rovněž považovat za jeden z důsledků softwarového pirátství.

Nezaměstnanost a softwarové pirátství. Podle [98], padělání softwaru nebo jeho nelegální kopírování, vede ke ztrátám práce a pracovních příležitostí. Snižuje-li se míra pirátství, tj. podíl počtu nelegálních produktů vůči počtu výrobků řádně pořízených, počet pracovních příležitostí roste. Především rozvoj pracovních příležitostí v softwarovém průmyslu lze považovat za jeden z významných přínosů pro nově pojímaná demokratická zřízení těch zemí, které se vymanily z totalitní moci. Je to důležité i z hlediska místních zájmů. Pokud nadnárodní firma chce investovat, obchodovat, prosperovat, musí spolupracovat s místními společnostmi a zaměstnávat zdejší lidi. Tato snaha však nemůže být naplněna v prostředí, kde nutno čelit zlodějům, odcizujícím výrobky, často pracně a nákladně vyvíjené. Všeobecně se dá říci, že důsledkem softwarového pirátství došlo v Evropě ke ztrátě velkého počtu pracovních míst. Podle posledních odhadů je ve špičkovém softwarovém průmyslu vytvořeno minimálně 15 tisíc pracovních míst. Nebýt softwarového pirátství, jen na území Evropy by mohlo být v softwarovém průmyslu zaměstnáno zhruba dvakrát tolik lidí. Podle [98] je 17 tisíc pracovních příležitostí v softwarovém průmyslu ztraceno v důsledkem pokračujících problémů se softwarovým pirátstvím.

8. Boj s počítačovou kriminalitou

Sestaveno převážně z pramenů: [3], [11], [21], [25], [39], [40], [85], [88], [90], [98], [104], [106], [107, [110], [118], [120], [127], [129], [136], [137], [138], [167], [199], [203], [208], [209], [221], [236], [237], [242], [247], [249], [250], [252].

8.1. Význam legislativy pro boj s počítačovou kriminalitou

Ze zkušenosti orgánů činných v trestním řízení lze dedukovat, že průměrný občan České republiky má dosud poměrně vágní právní vědomí. Možno říci, že jeho znalost základních zákonů je nepříliš valná a zejména v trestní oblasti se obvykle řídí pouze jakýmsi zjednodušeným desaterem. Vychází z obvyklého chápání rozdílu mezi dobrým a špatným. Každý ví, že krást se nemá, stejně jako podvádět, poškozovat cizí majetek apod. Přes tento obzor však vidí málokdo. Jen velmi málo lidí, kteří k tomu nejsou nuceni, překročilo rámec intuitivního chápání přirozeného práva tím, že prostudovalo alespoň zběžně určitou platnou legislativní úpravu, zákon, předpis či jiný dokument. Přitom bez znalosti příslušné úpravy se mnohdy mohou dopustit protiprávního jednání, kterému by se jinak jistě rádi vyhnuli, a to nejen snad vlivem hrozby postihu. Poměrně masivní a dlouhodobě vedenou kampaní by se samozřejmě daly tyto skutečnosti změnit. To však není příliš schůdná cesta, protože vzniká otázka, zda by vynaložené síly a prostředky dokázaly plošně změnit právní vědomí celé aktivní populace v zemi. A především za jak dlouho.

Orgány činné v trestním řízení, konkrétně i policie, plnící úkoly v trestním řízení, vyšetřovatel a policejní orgán, jsou ve smyslu §158 odst.2 trest. řádu povinni činit nezbytná opatření k předcházení trestné činnosti. Mají tedy povinnost konat preventivní činnost. Vidíme tedy, že legislativa hraje významnou úlohu v boji s kriminalitou jak z hlediska represe, tak i prevence. Platí to pro kriminalitu obecně a kriminalitu počítačovou zvláště. Bez dokonalé legislativy nejen není možné adekvátně pachatele počítačových deliktů postihovat, ale nelze ani budovat systém vhodné prevence, která v oblasti počítačové kriminality má svá určitá specifika.

**

Pokud jde o trestní právo, v novelizovaném znění trestního zákona, viz [247], je zakotvena řada trestných činů postihujících též různé formy počítačové kriminality. Jsou to především

-§124, porušování předpisů o oběhu zboží ve styku s cizinou,
-§151, porušování průmyslových práv,
-§152, porušování autorského práva,
-§178, neoprávněné nakládání s osobními údaji,
-§239, porušování tajemství dopravovaných zpráv,
-§249b, neoprávněné držení platební karty,
-§257a, poškození a zneužití záznamu na nosiči informací.

Poslední z uvedených paragrafů lze, lapidárně řečeno, považovat za „ryze počítačový“ paragraf, který se ocitl v našem trestním právu v důsledku rozvoje informačních technologií a jejich aplikací v každodenním životě společnosti. Zásadním přínosem této úpravy je použití termínu „nosič informací“, umožňující pružný postih útoků na všemožné nosiče dat z hlediska stávající technické úrovně i do budoucnosti. Podle [199] problém praktické aplikace tohoto ustanovení spočívá v požadavku na existující úmysl způsobit jinému škodu již v okamžiku, kdy si pachatel získává přístup k nosiči informací, a zejména v nepostihování nedbalostního jednání, které přitom může mít velmi vážné následky. Z hlediska orgánů činných v trestním řízení je právě prokazování tohoto záměru klíčovým momentem pro úspěšný postih pachatele úmyslného trestného činu. Z hlediska poškozených pak může být větší tragedií výskyt neobratného laika, který může z nedbalosti způsobit škodu daleko větší - a to v současnosti zcela nepostižitelně, než seberafinovanější pachatel.

Ustanovení §178, neoprávněné nakládání s osobními údaji, je zařazeno v návaznosti na zákon č.256/1992 Sb., o ochraně osobních údajů v informačních systémech, viz [250]. Jak uvádí autor článku [199], toto ustanovení bylo motivováno pravděpodobně i pod vlivem dřívějších zkušeností s prodejem dat občanů reklamním agenturám pracovníky bývalého federálního ministerstva vnitra. Úprava se týká ochrany osobních údajů, zejména povinnosti a odpovědnosti související s ochranou informací při provozování jakéhokoliv informačního systému, který nakládá s osobními údaji občanů.

Podobně §151, porušování průmyslových práv, §152, porušování autorského práva, sankcionují porušování zvláštních zájmů sloužících na ochranu děl podle zákona [251] a autorských děl podle autorského zákona, viz [249]. Trestní sankce se zde týkají odnětí svobody nebo peněžitých trestů, či propadnutí věci.

Konečně ustanovení §124, §124a-124c, §124d-124f postihuje porušování předpisů o oběhu zboží ve styku s cizinou, o nakládání s kontrolovaným zbožím a technologiemi a o zahraničním obchodu s vojenským materiálem.

Postupné zostřování boje s počítačovou kriminalitou si vynutí řadu dalších legislativních úprav, bezprostředně nesouvisejících se zločinností páchanou prostřednictvím počítačů. Jako aktuální příklad můžeme uvést vyhlášku Ministerstva financí, viz [236], o podmínkách monitorování a uchovávání záznamů v kasinu, která může přispět nejen k prevenci nekalých praktik v kasinech, ale též k vyjasnění případných deliktů zde páchané počítačové kriminality.

**

Motivace ke speciálním úpravám ve světle nizozemských zkušeností. O významu legislativy pro boj s počítačovou kriminalitou byla v minulosti otevřena diskuse v mnoha

zemích. K postihu tzv. počítačových zločinů byl položen dobrý teoretický základ např. v Nizozemí přijetím speciální zákonné úpravy již v roce 1992, viz [129]. V úvodu citované studie se autoři zabývají otázkou, zda výsledky technického pokroku, jako počítačové programy a data, jsou dostatečně chráněny existující legislativou. Dále pak vymezují pojem počítačového zločinu. Podle nich lze apriori pod tento pojem zařadit podvod, padělání, vniknutí do systému, programové a čipové pirátství, krádež dat, sabotovaní a zavirovaní programů, včetně dat. Všechny tyto činy nemusí být za všech okolností trestnými, čímž vzniká problém precizování počítačového zločinu. Autoři [129] uvádějí pro ilustraci několik konkrétních případů počítačových zločinů. Podle nich je nejobvyklejším podvod. Doposud největší byl v Nizozemí popsán v roce 1987, kdy úředník městské rady převedl během tří let ve svůj prospěch 8 milionů guldenů. Vniknutí do systému je mnohdy realizováno jako důkaz schopností programátora. Může však být motivováno zájmy průmyslové špionáže i nízkými zištnými cíli při podvodech. Některé firmy jsou vydírány pod pohrůžkou umístění virů do jejich systémů. Podle *Platformy pro počítačovou kriminalitu v Nizozemí* tvoří programové pirátství 47 % všech počítačových trestných činů a působí jen v Nizozemí škodu minimálně 24 milionů guldenů ročně. Což představuje asi 10% obratu nizozemského trhu programového vybavení počítačů. Velké počítačové společnosti, sdružené v *Business Software Aliance*, tak přijdou ročně o 400 až 600 milionů guldenů. S těmito škodami jsou srovnatelné škody způsobené viry. Důvody jejich instalace jsou různé, může to být vydírání, sabotáž, upoutání pozornosti, zamaskování podvodu, nebo dokonce odstrašení počítačových pirátů. Výroba viru nebo vniknutí do sítě nemusí být vždy trestným činem. Samo vniknutí může být v extrémním případě stíháno jako porušení úředního tajemství, protože současná nizozemská právní úprava jej nepovažuje za trestný čin a nestíhá jej jako neautorizovaný vstup. Důvodem je absence postihu některých typů chování v trestním řádu. *Organizace pro ekonomickou kooperaci a rozvoj OECD* definuje „zločin za pomoci počítače“ jako „každé ilegální neetické a neautorizované chování, týkající se automatického zpracování a přenosu dat“. Rada Evropy přijala tuto definici v *Hlášení o trestných činech za pomoci počítače.* Ovšem je-li něco ilegální, není to bezpodmínečně trestným činem - tvrzení opaku by bylo v rozporu se čl.7 Evropské konference o lidských právech. Další část definice, určující, které chování se „vztahuje k počítačům“ a které nikoliv, je stejně neuspokojivá. Definice by měla totiž určit národním legislativám směr při rozlišování trestného a legálního chování na tomto poli a orientaci v jejich budoucím vtělení do právních řádů.

Určité klady a zápory speciální legislativní úpravy. Přes všechny výše uvedené problémy jsou legislativní nástroje i nadále považovány za nejúčinnější prostředek v boji s počítačovým zločinem. Proto významná nizozemská lobby, usilující o vydání speciálního zákona, dosáhla svého. A to i přes určitý odpor některých odborníků. Nová opatření týkající se počítačové kriminality byla vtělena v roce 1993 do trestního zákoníku, trestního procesního řádu a částečně i do občanského zákoníku. Již před vydáním nového zákona byly úspěšně souzeny a odsouzeny případy počítačových trestných činů podle existujících právních úprav. Nizozemský trestní zákoník (1886) a trestní procesní řád (1921) jsou koncipovány poměrně široce a postihují spíše výsledky jednání než jednání samo. Proto nebylo důležité, byl-li např. podvod spáchán za pomoci počítače nebo nikoliv. Při studiu výroků nizozemských soudů

zjistíme, že počítačové podvody a padělání spadaly pod úpravu o podvodech a padělání, programové pirátství pod zákony o copyrightu, škody způsobené na programech nebo souborech byly kvalifikovány jako trestné škody a jediným nepostiženým činem zůstal neautorizovaný vstup do systému bez způsobení škody. Podstatným bylo rozhodnutí arnhemského soudu, které označilo software za materiální zboží, čímž mu poskytlo ochranu tak, jako v rozhodnutí o elektřině z roku 1921, kdy tato byla označena za materiální zboží, které může být předmětem krádeže. Zákon o počítačových zločinech byl v Nizozemí přijat koncem roku 1992. Mimo jiné přiznává policii více pravomocí při vyšetřování. Z debat o tomto zákonu vyplývá, že stávající úpravy poskytovaly takovou míru ochrany, že jeho přijetí nebylo nutné. Dalším argumentem proti je nejednotnost právních úprav na tomto poli v rámci ES. Odpůrci zákona tvrdí, že nové zákony povedou ke zbytečným komplikacím, zmatku a výdajům. Podstatně zvětšují pravomoci policie, aniž by současně poskytovaly více ochrany obětím. Prý by stačilo jen nepatrně pozměnit existující zákony ve smyslu postihu neautorizovaného vstupu a uspořit tak veřejné fondy. Smyslem přijatých opatření je spíše vnutit veřejnosti představu, že počítačové zločiny jsou velkým společenským nebezpečím a tak ospravedlnit množství peněz, utracených na tomto poli. Pro stát je to asi rozumné, protože informace a jejich tok budou v budoucnosti znamenat největší zdroj moci – a tu by stát velice rád kontroloval. Autoři studie [129] pracují na Erasmově universitě v Rotterdamu. Oba se podíleli na činnosti zvláštního pracovního výboru *Nizozemské asociace pro počítače a právo*, zabývají kriminologickými i legislativními aspekty počítačových zločinů.

**

Počítačové právo a počítačová kriminalita. Počítačové právo je nově vznikajícím oborem právní a soudně-znalecké teorie a praxe v systému práva České republiky. V současné době se touto problematikou zabývá několik odborníků, jejichž vytíženost je veliká, ale poměrně málo institucí a organizací. Boj proti počítačové kriminalitě si zaslouží podstatně větší a koordinovanější pozornost, protože škody které způsobuje se většinou pohybují v rozmezí větší škody až po škodu velkého rozsahu, přičemž používané metody a prostředky pachatelů jsou na velmi vysoké technické a intelektuální úrovni.

8.2.Formy boje s počítačovou kriminalitou

Z hlediska forem boje s počítačovou kriminalitou je třeba si uvědomit, že fenoménem současnosti je značný nárůst informačních technologií a s tím spojené pronikání nejrůznější výpočetní techniky, nutně vybavené adekvátním software, do celé společnosti a především do každodenního života nás všech. Vývoj je tak rychlý, že je nutné neustále sledovat nové informace, jinak se otevírá značná mezera mezi realitou a znalostmi k jejímu pochycení. To platí nejen o softwarové kriminalitě, o níž jsme se již poměrně podrobněji zmínili, ale o počítačové kriminalitě vcelku. K základním formám boje s kriminalitou se vyjádříme naznačením otázek *výchovy, prevence, softwarového auditu, represe, působnosti policie a dalších orgánů činných v trestním řízení.*

**

Výchovu k adekvátnímu právnímu vědomí občanů v oblasti počítačové kriminality nutno založit především na dobré znalosti vývoje a stavu legislativy u nás. Vzhledem k závažnosti fenoménu porušování autorských práv ve vztahu k programovým systémům, výchovu nutno orientovat především do této oblasti. Po roce 1989 a v létech následujících došlo mimo jiné i k posunům v oficiálním názoru na dodržování autorských práv k počítačovým programům. Ovšem změny postupovaly převážně vertikálně shora dolů. Zatímco rozhodující orgány státní správy začaly řešit tento problém, možná i z popudu vzrůstajícího mezinárodního tlaku, občan své chápání nezměnil. Pro pochopení současné situace v České republice jsou důležité historické kořeny vztahu k duševnímu vlastnictví. Zde dochází mnohdy ke zjednodušenému pohledu na tento problém, a to především ze zahraničí. Řada softwarových společností, které jsou zároveň největšími nositeli autorských práv k počítačovým programům, předpokládá, že rok 1989 představuje předěl k lepšímu, zejména pokud jde o vztah k duševnímu vlastnictví. To ovšem není zcela pravda. Nové podmínky v ekonomické oblasti, změna společenských vztahů a vlastnictví výrobních prostředků přineslo u jistých podnikavců i nové formy nazírání na nekalou činnost, zejména pak morální ospravedlnění snah po rychlém zbohatnutí. Zde je pak široké pole působnosti pro výchovné vlivy nejrůznějších organizací, i těch, co bojují s počítačovou kriminalitou.

Výchova je v pojetí tohoto působení považována za velmi důležitý faktor *prevence*. Je ovšem často problematické, jak čelit pokušení uživatelů zneužívat software, které je živeno různými důvody. Jedním z důvodů v podstatě masového užívání nelegálního software je jeho cena. Je smutnou skutečností, že kupní síla průměrného občana je relativně velmi nízká. Přitom ceny kvalitního software se počítají řádově v tisících, či desetitisících korun. To vede řadu jedinců k rozhodnutí získat a užívat bezplatně a tedy nelegálně potřebný software. Bohužel jim v tom mnohdy nebrání ani vlastní morální přesvědčení. V uplynulých létech byla morálka ve spojení s pirátskými praktikami mnohokrát bezvýsledně proklamována. Ukazuje se, že pro určité osoby neakceptující obecně normativní společenské hodnoty, je morální apel v podstatě bezcenný. Počítačové programy totiž nijak zjevně neukazují svou vyčíslitelnou hodnotu. A proto není u nás výjimkou osoba, která neoprávněně užívá na svém soukromém počítači software za několik set tisíc korun, aniž by to považovala za nemravné. Zde jsme u zdroje snah o jiný způsob boje s takovými prohřešky, či preventivních opatření, tak jak jsme o nich pojednali v souvislosti s počítačovou bezpečností.

**

Prevence. Pro efektivní tlumení počítačové kriminality je prevence podstatně důležitější než represivní postihy. Obecně je prevence důležitějším prvkem v potýkání se s jakýmkoliv problémem, než při odstraňování implikovaných následků. To platí samozřejmě zejména i v oblasti boje s počítačovou kriminalitou, vzhledem k velmi vysoké latenci ve srovnání s jinými typy kriminality. Vysokou latenci je nutno přičíst především technické náročnosti zjišťování nějakého neoprávněného vstupu či zásahu do systému. Rovněž objasňování zjištěné kriminality není jednoduché. Odhalení neoprávněného průniku ještě nemusí znamenat, že bude odhalen i pachatel. Dalším důvodem priority prevence je fakt, že i když dojde k odhalení pachatele, nastane problém s dokazováním jeho prohřešku u soudu. Důkazy většinou neexistují vůbec, nebo existují-li, vznikají další otázky jejich průkaznosti,

protože záznamy na magnetických médiích ve většině zemí nemohou sloužit jako důkaz u soudu. Dalším důvodem je skutečnost, že pokud dojde k narušení systému, a to zvláště při napadení virem nebo při úniku citlivé informace, dojde k nezměrným nenávratným škodám. Prevenci lze v podstatě rozdělit do dvou typů podle směrů, odkud očekáváme útok. Rozdělme ji tedy na prevenci proti útokům vedeným „zvenku“ -např. z globální počítačové sítě- a na prevenci proti útokům vedeným „zevnitř“ -např. od uživatelů počítačů spojených lokální sítí v rámci jedné instituce, tak jak jsme se o těchto otázkách zmínili již v souvislosti s počítačovou bezpečností.

Softwarový audit. Jednou z forem prevence počítačové kriminality je softwarový audit, spočívající v profesionální kontrole legality užívání software u provozovatele. Zde se nebudeme zabývat podrobnostmi a podmínkami za kterých se s příslušnou firmou uzavírá smlouva na realizaci softwarového auditu a jakým způsobem se tato kontrola uskutečňuje. Na základě úspěšně proběhlých auditů lze udělit uživateli tzv. *deklaraci čistoty*. Pro úspěšný audit je vždy rozhodující odhodlání vedení organizace investovat do legalizace mnohdy značné finanční prostředky, ale zároveň i překonání určité neochoty vlastních pracovníků k užívání software jen legálně zakoupeného. To tedy znamená i konec užívání software od „kamaráda na zkoušku“, nebo jen z toho důvodu, aby se operátor s ním seznámil, protože někdy v budoucnu to bude potřebovat. Ze zkušeností organizací, které se auditu podrobily, lze usuzovat na to, že podstatně větším problémem než programy koupit a zaplatit, je uhlídat vlastní zaměstnance, aby sami na užívané počítače nějaký nelegální software neinstalovali, viz např. [242]. Proto je potřeba vyžadovat, aby součástí kontroly bylo i interní memorandum, které zaměstnancům zakazuje užívat jiný než legální software, což lze podpořit i sankcemi podle zákoníku práce. Zároveň v průběhu auditu jsou vytvořeny tzv. *pasporty počítače*, které uvádějí u každého počítače, jaký legální software je na něm instalován. Takový pasport by měl být podepsán konkrétním uživatelem přiděleného počítače, tedy osobou, která by v případě zjištění nelegálního software orgány činnými v trestním řízení za to trestně zodpovídala. Uvedená opatření mají pochopitelně velký význam po skončení auditu ze strany firmy, která jej realizuje, např. u nás je to *organizace BSA CS, Busines Software Alliance.* Každá organizace, u které se audit uskutečňuje, obdrží od *BSA CS* program *Search II* pro kontrolu obsahu počítačů. Organizace jsou tedy schopny samy následně kontrolovat své počítače a zabránit tak tomu, aby zaměstnanci nadále užívali nějaký nelegální software. Nejlépe se tento stav udržuje v organizacích, kde je jmenován zvláštní pracovník, který tyto interní kontroly dělá a přitom spolupracuje s příslušnou firmou pro realizaci auditu. V minulosti byla udělena deklarace čistoty, např. *a. s. Plynoprojekt Praha.* Audit v této organizaci proběhl úspěšně díky úzké spolupráci vedení podniku s *BSA CS*. Vedením organizace byl od počátku kontroly jmenován odpovědný pracovník, který ve styku s *BSA CS* audit zajišťoval. Ten byl přímo odpovědný za tuto činnost generálnímu řediteli organizace. Některé problémy řešil pak s *BSA CS* přímo generální ředitel, který trval důsledně na oboustranném plnění smlouvy o auditu. Jeho snahu o získání jistoty, že je v organizaci užíván pouze legální software, zdůvodňoval velmi jednoduše, ale jasně. Protože podnikání jeho firmy je založené na duševní práci, nemůže si dovolit zneužívat duševní práci jiných. Mnohdy se stává, že softwarový audit využívají společnosti mimo jiné k tomu, aby dokonale zjistily

softwarové potřeby své firmy a získaly dokonalý přehled a evidenci o již zakoupených a užívaných počítačových programech s cílem předejít hospodářským machinacím na tomto poli. Příkladem takového postupu je i firma *Eko & Capital, spol. s r. o.*, která rovněž požádala o softwarový audit. Protože tato společnost nakupuje software i pro své dceřiné společností, od auditu si kromě jiného slibuje i dokonalou evidenci užívaného software i hardware. Samozřejmě, zavedení úplné a průkazné evidence vede jednoznačně i ke zjištění nedostatků v této oblasti. Některé postoje a aktivity evropské BSA jsou v poslední době podrobovány ostré odborné kritice. Jde zejména o moment údajného potlačení některých morálních a právních principů, jako odmítavých postojů k aktům vyhrožování, udavačství, k potlačování presumpce neviny, či zbytečné kriminalizaci ať již mezifiremních nebo i jiných vztahů apod.

**

Policie a další orgány činné v trestním řízení nemají v boji s kriminalitou snadné postavení, protože pachatelé trestných činů tohoto druhu mají obvykle značný náskok před represivním aparátem. Důvodů je několik. Patří mezi ně zejména nutnost kvalitního počítačového vybavení, které je také samozřejmě finančně nákladné. Dalším důvodem může být i nedostatek kvalifikovaných odborníků. Obrazně řečeno, policie nemůže být na stejné metě nebo dokonce před zločinem. Ve skutečnosti bude vždy o něco pozadu. Jejím úkolem však je, udržet minimální odstup. V případě informačních technologií to platí mnohonásobně. Informační technologie velmi rychle expandují i do běžného života a zároveň dochází k jejich velmi rychlému vývoji, technologickému i softwarovému. Současnost klade na policii a další orgány činné v trestním řízení proti počítačové kriminalitě značné nároky a je možno říci, že se tyto nároky budou stále zvyšovat. Lze předpokládat, že s rozvojem informační technologií počítačová kriminalita poroste. Není daleko doba, kdy se, stejně jako dnes, kdy máme obavu z odcizení motorového vozidla nebo vloupání do bytu, budeme obávat neoprávněného získání dat z našeho domácího počítače nebo i jiného znepříjemňování běžného života stále více závislého na výpočetní technice. To se týká samozřejmě i bezpečnosti osobních dat. V mnoha filmech, které se snaží o pohled do budoucna, můžeme vidět, co nás pravděpodobně čeká. Ve spojitosti s informačními technologiemi pro mnohé je již skutečností, co donedávna bylo pouhou málo pravděpodobnou fikcí.

K úloze a možnostem policie v počítačové kriminalitě se v materiálu [110] uvádí, že složitost problematiky výpočetní a organizační techniky, s níž se orgány činné v trestním řízení setkávají, zejména při vyšetřování počítačové kriminality, klade na tyto orgány vysoké nároky pokud jde o použití specifických metod vyhledávání zajišťování, zkoumání a vyhodnocování počítačových stop. U stop policii zajímá nejen jejich technická hodnota, která je potřebná k úspěšné kriminalistické identifikaci, ale předmětem zájmu musí být i taktická hodnota stop, která je významná z hlediska určení způsobu páchání konkrétní kriminalisticky relevantní události. Úspěšnost dopadení pachatele počítačové kriminality závisí nejen na technickém vybavení policie a na důkladném ohledání místa události související s počítačovou kriminalitou, ale i na znalostech a zkušenostech orgánů činných v trestním řízení, soudního znalce nevyjímaje. Policie musí mít neustále na zřeteli, že počítačová kriminalita není jen trestnou činností páchanou proti výpočetní technice, datům a programům. V současnosti je totiž počítačové techniky stále více využíváno jako prostředku páchání mnoha forem dalších závažných deliktů.

**

Obtížnou formou boje s trestnou činností je vyhledávání *nelegální výroby nosičů software* typu CD-disků (CD-ROM). Tato činnost začala ve větším měřítku před několika lety a od té doby se stává stále frekventovanější. Je podmíněna dnes již lepší dostupností zapisovací mechaniky CD-disků, která je k výpočetní technice prodávána jako externí nebo i interní. Důvodem je cena zapisovací mechaniky, která v posledních třech letech klesla zhruba z 80 tisíc Kč asi na osminu. Tím se stala cenově přístupná pro každého. Filozofie prodeje mechanik spočívá v umožnění kvalitního zálohování velkých objemů dat. Výsledkem však je mohutná výroba CD-disků s nelegálním softwarem podle tržních požadavků zákazníka. Důvody této trestné činnosti jsou diktovány požadavky trhu, aby značné množství osob získalo rychle co nejlevnější software a samozřejmě, aby pachatelé dosáhli maximálního zisku. Jde zřejmě o nejjednodušší způsob jak uspět při získávání poměrně slušného, ovšem nelegálního příjmu. Zatím co dříve byl rozsah takové činnosti úměrný počtu právnických nebo fyzických osob, které byly ochotny investovat do této technologie i zvýšené náklady, dnes snad skoro všichni inzerenti nabízející nelegální software mají doma nebo na pracovišti k dispozici vypalovací mechaniku na CD-disky. Sledováním trhu lze vidět, jak s možnostmi rozšíření vypalovacích zařízení mezi uživatele poklesla nabídka různých firem a jednotlivců na zálohování software. Nabídka sice klesla, ale neodezněla. Dodnes se můžeme setkat s velmi ochotnými firmami, které nehledě na autorská práva zazálohují prakticky cokoli. Je ovšem problematické, co je nebezpečnější, zda dovoz tisíců nosičů, nebo výroba stejného nebo i většího množství zde u nás doma. Jde o velmi zajímavou a zatím stále ještě lukrativní trestnou činnost. Každý, kdo investuje do potřebného hardware, tak může vyrábět tolik nosičů, na kolik má odbyt. Nejsou výjimkou čisté příjmy okolo několika desítek tisíc korun za měsíc. Nezdaněné, nekontrolovatelné. Ovšem škoda způsobená na autorských právech je daleko větší. Jistě to není zaviněno jen zištnými domácími „vypalovači“, ale problémem klimatu celé společnosti. Nicméně bez nabídky by byla poptávka neuspokojena a lidé by museli kupovat legální software. V tomto směru tak domácí kutilové způsobují značné škody. A proto nutně musí být jejich činnost cílem přiměřené represe.

Strategii represe možno založit na skutečnosti, že každá osoba, která vyrábí na svém obvykle soukromém počítači v domácnosti nelegální software, je kvůli zajištění zisků nucena na sebe upozornit. Obvykle to provádí cestou inzerce v inzertních periodikách (Annonce, Inzert spoj apod.) a v odborných časopisech (Chip week, Level atd.). Nejjednodušším způsobem odhalení takového výrobce - distributora nelegálního software je rozbor inzerce v regionálním měřítku. Zásobování nejbližšího okolí není komerčně nejúspěšnější strategií. Takový trh je brzy zcela pokryt. Je tedy nutno vystoupit z anonymity, ovšem pokud možno nenápadně. To je však pro pachatele vždy problematické. Pachatel realizuje prodej obvykle dvěma způsoby. Na dobírku, většinou zákazníkům mimo obec bydliště pachatele, a osobně zákazníkům v obci. Osobní prodej pak probíhá buď v bydlišti pachatele, nebo na smluveném místě. Kontakt pachatele se zákazníkem probíhá telefonicky, do bytu nebo na pracoviště. Telefonní číslo bývá obyčejně součástí inzerátu. Podezřelá osoba může software distribuovat pouze mezi prověřenými zákazníky, kteří si jeho nabídku předávají mezi sebou a rozšiřují mezi známými. Místo toho, aby odhalený pachatel přemýšlel nad nezákonností svého

protiprávního jednání, kterým si připravil velké osobní potíže, uvažuje často nad mezerami svého zabezpečení proti prozrazení. Podezřelý inzerát se prozradí zpravidla

-tím, že obsahuje nabídku na různý software na jednom nosiči, např. na systémy Windows 95, Microsoft Office, AutoCad, hry, utility atd.,

-nízkou prodejní cenou produktu, často řádově odlišnou od oficiální nabídky,

-neexistencí informace o originalitě programů,

-chybějícím oprávněním k prodeji software.

Taktika represe. K identifikaci takového inzerátu je nutná jistá elementární orientace ve výpočetní technice. Nejdříve je nutno inzerci úspěšně identifikovat a pak se zaměřit na inzerenty. Při zjišťování rozsahu činnosti a množství nabízeného software lze vycházet z archivu inzerce. Je to samozřejmě náročné na čas a odborné znalosti orgánů činných v trestním řízení.

**

Internet jako světová síť vzájemně propojených počítačů (serverů), které využívají různí uživatelé ke komunikaci, získávání informací a k práci, může být, jak jsme již uvedli, prostředkem páchání nekalé činnosti. *Problémy prevence* jsou v podstatě omezeny na výchovu uživatelů a na otázky technického zabezpečení přístupu k informacím podle typu nebo solventnosti uživatele. Bariéry tohoto druhu nejsou však pro schopného pachatele nepřekonatelné. Pokud jde o *represi,* bývají řešeny zpravidla problémy nedovoleného kopírování určitých systémů. To však přináší určité problémy, o nichž se zmíníme v dalším.

Mnichovská policie společně se dalšími počítačovými odborníky hledá pachatele trestných činů v Internetu. Pátrá od roku 1996 v této síti po osobách, které zásobují Internet zakázanými informacemi. Organizačně tyto aktivity spadají pod pracovní skupinu *EDV (Zajišťování důkazních prostředků)* s perspektivou jejího povýšení na samostatný komisariát. Pátrá se zejména po odesilatelích pornografických snímků, neboť rozšiřování dětské pornografie nebo pornografie se zvířaty je trestné. Dětskou pornografii je dokonce vůbec zakázáno ukládat do počítačů. *EDV* se zajímá především o tzv. *newsgroups*, což jsou diskusní fóra. Tyto newsgroups jsou něco jako veřejné nástěnky, kde může každý zanechat svůj příspěvek nebo obrázek a přečíst si příspěvky ostatních. Diskusní fóra jsou rozdělena do mnoha tematických skupin. Jen několik desítek z více než 20 000 na Internetu existujících newsgroups je zaměřeno výhradně na pornografii. U vybraných obrázků se zjišťují data odesilatele. Pokud nejsou utajena a odesilatel pochází z Německa, je jeho počítač zajištěn a vyhodnocen počítačovými odborníky. Poté je případ předán státnímu zastupitelství. V roce 1996 dopadla *EDV* přibližně 100 pachatelů. Ve skladu kanceláře *EDV* čeká průběžně na expertizu 30 až 40 zajištěných počítačů. U zahraničních pachatelů je však vyšetřování prakticky bez náležitých dopadů. Výsledky jsou sice předávány k dalšímu vyšetřování příslušným úřadům, ale *EDV* dosud neobdržela žádné zpětné hlášení. Pracovník této skupiny se nesmí vydávat za potencionálního zákazníka a není mu povoleno skryté vyšetřování. Používá jen nezáludný pseudonym, neboť v Internetu nemůže vystupovat jako zástupce Policejního prezídia Mnichov. Potencionálnímu zájemci nesmí *EDV* zaslat pornografický

obrázek, který by vyvolal pocit důvěry, ani ho nemůže provokovat k nezákonné činnosti. Musí jen doufat, že zájemce bude aktivní sám. Rovněž spolupráce s dalšími policejními orgány je pro skupinu *EDV* velmi důležitá. Jako příklad lze uvést jistého doktora věd z univerzity v Giessenu, který se chtěl telefonicky přesvědčit, že jeho partnerovi v komunikaci je více než 18 let. Vyšetřovatel *EDV* tedy nejprve zatelefonoval vědci, kterého informoval o svém věku, a poté vyrozuměl policii v Giessenu do jejíž kompetence případ místně náležel.

**

Kriminalistické aspekty a teorie hrají v boji s počítačovou kriminalitou významnou roli. Autor ve sdělení [106] uvádí, že většina u nás publikovaných informací o počítačové kriminalitě se týká obecného popisu způsobu spáchání trestného činu, úvah o motivu nebo porušení bezpečnostních, zatím nezávazných kriterií. V lepším případě bývá popsán postup pachatele při realizaci příslušné počítačové operace, která je chápána jako projev počítačové kriminality. V této souvislosti bývá zpravidla uvedeno, že k usvědčení pachatele byly využity údaje z informačního systému, v jehož rámci byl daný skutek realizován. Jen výjimečně je uvedeno, že se jedná nebo, že by se mohlo jednat o kriminalistické *počítačové stopy*. Autor [106] se dále zamýšlí nad využitím *kriminalistické teorie stop*. Za kriminalistické počítačové stopy nutno považovat stavy nebo změny v informačním obsahu počítačových a obdobných záznamových médiích, ale i stavy nebo změny v celém počítačovém systému tvořeném komplexem hmotných (hardware) a nehmotných (software a data) prostředků, které souvisejí s kriminalisticky relevantní událostí. *Kriminalistickou počítačovou stopu* v užším slova smyslu lze chápat jako digitalizovanou informaci, která je dočasně či trvale uchována na záznamovém mediu, nosiči informace, a kterou je možno zpětně získat zpravidla týmiž nebo obdobnými technickými a programovými prostředky, kterými byla vytvořena. Materiálním nositelem počítačové stopy je příslušné záznamové medium, paměť či jiný nosič informací. Záznamová media mohou být různá - od děrné pásky či štítku až po moderní optický disk, CD-disk či speciální počítačové karty. U děrných štítků a děrné pásky bylo možné, i když velmi pracné, získat obsah kódované informace přímo - tj. vizuálním vnímáním polohy a kombinace otvorů v příslušném sloupci daného media. U magnetických, optických či jiných dalších typů záznamových medií to bez technických prostředků možné není. Kromě technického hlediska, které je dáno výrobcem zařízení pro práci s daným typem záznamového media je též nutno přihlédnout ke způsobu uložení, formě souborového uspořádání a případně ochrany informačního obsahu. Ve většině případů nelze ihned určit, zda dané záznamové medium obsahuje kriminalistickou počítačovou stopu. Tu lze hledat v obsahu pevného disku počítače nebo v obsahu záznamových medií. Tedy počítače nebo záznamová media nejsou zpravidla (vyloučíme-li zcizení nebo fyzické poškození) kriminalistickou stopou, ale z hlediska počítačové kriminality jsou jen potencionálními nosiči případné kriminalistické počítačové stopy. Vlastní kriminalistické počítačové stopy je nutno teprve v zajištěných počítačích, resp. záznamových mediích, vyhledat a následně zkoumat, což realizuje kriminalistický expert nebo soudní znalec. Autor [106] se dále zabývá pravidly pro zjišťování nosičů kriminalistických počítačových stop, problematikou znaleckých nálezů a pojetím kriminalistických počítačových stop z hlediska teorie stop vůbec. Kriminalistická teorie hovoří především o prostorových stopách, kterými jsou zejména změny v poloze

určitých předmětů a zmizení či objevení předmětů. Podle názoru autora [106] lze záznamové médium chápat jako určitý „digitální prostor“ pro uložení informací. Velikost daného prostoru je dána kapacitou konkrétního záznamového média. Tedy v daném „digitálním prostoru“ se mohou vyskytovat kriminalistické stopy, které jsou analogické ke stopám prostorovým. Pracovně jsou proto nazývány jako *počítačové (digitální) prostorové stopy*. Na základě toho lze pak využít poznatků obecné teorie kriminalistických stop též v boji s počítačovou kriminalitou.

**

Významným přínosem pro uplatňování praktických aspektů boje s počítačovou kriminalitou je konstituování metodiky speciálního vyšetřování trestných činů, páchaných v souvislosti s počítači. Metodika [167] byla zpracována kolektivem autorů specialistů. Jak uvádí autor recenze [107] , v dané publikaci jsou shrnuty dosavadní poznatky s projevy počítačové kriminality. Jedná se o učební text, na který je vhodné upozornit nejen kriminalisty, ale i ostatní pracovníky orgánů činných v trestním řízení, kteří přicházejí do kontaktu s počítačovou kriminalitou. Vlastní text je rozdělen do devíti částí s předmluvou a přílohou, která je věnována normalizované terminologii z oblasti výpočetní techniky. Do metodiky vyšetřování počítačové kriminality lze podle [167] zahrnout problematiku

-*kriminalistických charakteristik*, včetně vymezení pojmu počítačové kriminality, což podle [167] je skupina trestných činů, či obecně společensky škodlivých jednání, páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení a databází výpočetní techniky. Jako typický počítačový delikt je chápán trestný čin, jehož skutková podstata je uvedena v ustanovení §257a trest.zák., případně ve speciální formě ustanovení §124c trest.zák., §125 trest.zák. a §250a trest.zák. jako deliktů často páchaných pomocí počítačů. Ostatní trestné činy, které souvisí s výpočetní technikou, počítačovými programy nebo zpracovávanými daty, by měly být posuzovány mimo tento rámec, jako např. porušování autorských práv k počítačovým programům. Dále do této problematiky patří vyjasnění základních pojmů, poznatky ke kriminální situaci, ke způsobům páchání deliktů a k osobě pachatele, včetně rozboru typických motivů;

-*typických stop* s členěním na *stopy materiální a jiné soudní důkazy* a na *stopy paměťové;* mezi první uvedené řadíme *počítačové stopy*, které dále dělíme do tří kategorií

-na stopy na výpočetní technice včetně neoprávněných zásahů do této techniky,

-na stopy na záznamových médiích a informace uložené na nich,

-na stopy na organizační a kancelářské technice umožňující zaznamenání a uchování digitálních informací;

-*typických vyšetřovacích situací*, hodnocených podle počátečních informací;

-*dokazování počítačové trestné činnosti* a zvláštností předmětu vyšetřování, zejména s ohledem na specifika

-neoprávněného užívání počítače a jeho komunikačního zařízení k soukromým účelům,

-zneužívání počítače a jeho komponentů k páchání jiné trestné činnosti,

-počítačových podvodů,

-tvorby a rozšiřování počítačových virů,

-neoprávněných zásahů do programového vybavení, databází a komunikačních zařízení,

-neoprávněných přístupů k datům;

-*zvláštností podnětů k vyšetřování* s nejčastějšími motivacemi a formami;

-*prvotních úkonů a operativně pátracích úkonů*, včetně ohledání místa činu, domovní prohlídky a prohlídky jiných prostor, zajišťovacích úkonů pro počítačovou expertízu a zvláštností cílevědomého vyhledávání elektronických stop a důkazů;

-*vyšetřovacích verzí*, plánování a organizace vyšetřování, včetně vytyčování typických verzí a způsobů páchání, s uvedením zobecněných případů;

-*počítačových expertíz*, následných etap vyšetřování, výslechu obviněného a výslechu svědků;

-*zapojení laické i odborně fundované veřejnosti do možností prevence* v obecné i speciální rovině, bezpečnosti výpočetní techniky, včetně bezpečnosti uchovávaných a přenášených dat.

**

Dokazování autorství programu v boji s počítačovou kriminalitou. Problém určení autorství daného počítačového programu nebo jeho fragmentu, v souladu s příspěvkem [237] nemusí být primárně orientován na řešení sporů týkajících se porušování autorských práv, tedy na softwarové pirátství. Lze ho chápat i jako otázku, do jaké míry je možné z programů nebo jejich zbytků, zanechaných na místě počítačového trestného činu, určit jejich autora (autory). Těmito programy mohou být počítačové viry, ale i různí červíčci, úpravy existujících programů vytvořené někým jiným nebo programy přímo vytvořené s cílem získat neoprávněný přístup do počítačového systému nebo k jeho údajům. Pro vyšetřování trestných činů spáchaných pomocí počítače by nepochybně bylo užitečné vytěžit z programů při tom použitých co nejvíc informací o autorovi programu jako o potenciálním pachateli vyšetřovaného činu. Forma ve které se tyto programy nacházejí, však obvykle není vhodná pro klasické expertízy . Jde zpravidla o změť bitů neumožňujících usuzovat cokoliv o počítači, na němž byl program vytvořen, či o autorovi daného seskupení. Pokud zmíněná změť reprezentuje počítačový program, vyznačuje se jistou strukturou, podle níž lze učinit pokus o úsudek na okolnosti jejího vzniku. Pramen [203], z něhož bylo autorem [237] čerpáno, je pravděpodobně základním kamenem tzv. *software forensics*. Pro další rozvíjení této disciplíny a pro její zdokonalení do použitelné podoby nepochybně bude nutný další výzkum.

Analýza exekutivních programů, tedy programů přeložených do posloupnosti strojových instrukcí, představuje nejnáročnější úlohu pro malou srozumitelnost podkladu, který je k dispozici. Moderní optimalizující překladače (kompilátory) totiž do značné míry stírají některé charakteristické črty původního programu. Navíc platí, že programy, které se na určitých místech odlišují, mohou být přeloženy zcela do téhož exekutivního programu. Některé charakteristické črty však přesto možno zachytit. Jde zejména

-o struktury údajů a algoritmy, jejichž presentace může vypovídat o osobnosti autora programu, jeho kvalifikaci, zručnosti či rutině;

-o opakující se konstantní podúlohy;

-o aplikaci speciálních „červíků“ jako primárních struktur použitých údajů;

-o uspořádání strojových instrukcí;

-o další specifické informace týkající se kompilátoru a systému, jako např. o výskyt speciálních systémových volání, charakteristických jen pro některé operační systémy;

-o výskyt segmentů kódu reprezentujících podpůrné podprogramy;

-o programátorskou zručnost a systémové znalosti, které jsou demonstrovány např. výskytem segmentů programu duplikatur funkcí systémových volání apod.;

-o výběr systémových volání - pokud jsou v systému např. k dispozici dvě či větší počet odlišných pojetí, pak opakovaná volba jednoho z nich může prozradit autora;

-o výskyt chyb - určité chyby jsou u některých programátorů prakticky součástí jejich stylu, např. při cyklickém přechodu přes strukturu údajů někteří programátoři často zapomínají na poslední realizaci, takže počet přechodů je o jednotku menší, což způsobí chybu na výstupech.

Analýza zdrojových textů programů je ve srovnání s předchozím případem schůdnější. Ze zdrojového textu programu, který představuje původní „rukopis“ programátora, je možné vyčíst daleko více charakteristik použitelných k odhalení autora. Tíhnutí autora k určitému stereotypu v jeho chování, respektive projevu, nazýváme *perseverancí*. Jak uvádí autor [237], při rozboru zdrojového programu je třeba hodnotit

-výběr použitého programovacího jazyku - asi by nebylo správné připisovat autorství programu osobě, která neovládá použitý jazyk;

-formátování textu - programátoři jsou obvykle zvyklí na určitý způsob grafické úpravy zdrojového textu, např. dodržují odrazy bloků programu o určitý počet míst, mají specifický styl závorkování výrazů, formátování deklarací proměnných, seskupování příkazů na jednom řádku, rozdělování programu do bloků, modulů, či samostatných souborů s jejich propojením řídícím programem apod.;

-speciální vlastnosti zdrojového textu - některé kompilátory poskytují určitá makra, tj. posloupnosti úkonů komprimované do jednoho globálního úkonu; jejich přítomnost může pak vypovídat o vývojovém prostředí, v němž program vznikal;

-styl komentování programu, zda vůbec autor komentuje a v případě, že ano, jaké je grafické zvýraznění doprovodného textu, jeho umístění, frekvence výskytu, míra detailnosti, obratnost při vyjadřování apod.;

-pojmenování proměnných, které může být významnou markantou mezi ostatními znaky; autora lze typovat podle délky jmen proměnných, originality verbálního výběru, způsobu zápisu, užití malých či velkých písmen, používání standardních jmen pro lokální proměnné určitého stálého charakteru apod.;

-překlepy a gramatické nedostatky - někteří programátoři se dopouštějí opakovaně týchž překlepů v textu, v zápise či výslovnosti některých slov;

-využívání vlastností programovacího jazyku - sem patří např. již dříve uvedený výběr příkazů cyklení, dále pak větvení programu, vytváření hodnot funkcemi, ignorování složitějších typů struktur, funkcí atp.;

-nefunkční části programu - některé programy obsahují nefunkční fragmenty zbývající po jeho ladění či pozdější přestavbě; při spuštění programu jsou ignorovány a jen díky pohodlnosti, nepozornosti nebo snaze po archivaci postupu ladění či jiných úprav, nebyly programátorem vypuštěny;

-chyby - někteří autoři programů setrvávají důsledně v tvorbě chyb, zvláště takových, které se projevují jen v určitých případech, např. při přechodu na jiný hardware; jde např. o kódování bitových operací, které nerespektuje uspořádání na cílovém počítači, o absenci kontroly chyb některých systémových volání, o absenci kontroly na numerické přeplnění atd.;

-softwarovou metriku - v softwarovém inženýrství se používají některé metriky pro hodnocení složitosti programu, např. počet řádků na určitou funkci, podíl počtu příkazů a komentáře apod., za určitých okolností vhodně volené míry lze předpokládat použitelnost dané metriky k odhalení autora.

Všechny uvedené aspekty mohou při dokazování autorství programu přispět ke konkrétní aplikaci *teorie perseverance*, jako nástavbové analýzy osobnosti programátora (event. pachatele počítačové kriminality) a jeho chování. Lze vyčíslit i konkrétně určitou míru perseverance pro charakterizování individuality daného jedince. Hodnota či užitečnost perseverance je v praxi dána možnostmi odlišit chování určitého jedince (pachatele, recidivisty) od chování průměrného representanta určité skupiny lidí (např. systémových programátorů). Výrazná individualita projevu pachatele bývá v literatuře (viz např. [11]) nazývána *signifikancí* chování pachatele. Jedinec, je-li jeho chování výrazně signifikantní, může být snadněji podle typických znaků identifikován. Blíže k tomu v souvislosti s problémy stability chování subjektů i obecných systémů viz [138].

**

Zvyšování důvěryhodnosti informací jako forma boje s počítačovou kriminalitou. Jedním z důležitých prostředků počítačové bezpečnosti je adekvátní užívání šifrovacích a dešifrovacích technik. Podle [118] lze se v této oblasti setkat s problémy, kdy existuje přiměřené řešení za předpokladu, že známe vlastníka určitého kryptografického klíče. Či spíše máme k dispozici popisné informace, které jej identifikují a důvěřujeme spojení těchto informací a daného klíče. Nyní se podíváme podrobněji na tento aspekt důvěry. Připomeňme, že šifrovací algoritmy lze mj. dělit na symetrické, jež pro zašifrování i dešifrování používají stejný klíč, a asymetrické, které používají odlišný klíč pro zašifrování (veřejný klíč) a pro dešifrování (soukromý klíč). Symetrické algoritmy jsou sice rychlejší, ale vyžadují dohodu

mezi partnery ohledně výběru kryptografického klíče a oba uživatelé jej musí pečlivě opatrovat. Pro asymetrické algoritmy obecně platí, že rychlost šifrování je výrazné nižší, ale jinak stačí spolehlivě publikovat svůj veřejný klíč a chránit si jen svůj soukromý klíč. K tomu všemu lze ještě vytvořit a ověřit digitální podpis. Na první pohled se skutečně zdá, že správa klíčů u asymetrické kryptografie je podstatné jednodušší než u symetrické kryptografie. Pro malé systémy je to podle dosavadních zkušeností většinou pravda, ale ukazuje se, že ono spolehlivé publikování či oznámení veřejného klíče není triviální záležitostí, zvláště pro velké systémy. Zásadním aspektem správy veřejných klíčů je jejich integrita a spojení s dalšími informacemi o uživateli. Pro malé skupiny uživatelů vystačíme např. s osobním předáním klíčů na disketě, popřípadě předáním otisku, tzv. *haše,* klíče a zasláním vlastního klíče e-mailem nebo poštou, při nejhorším i přečtením haše po telefonu. Pro velké, snad i celosvětové, zejména dosahem rozsáhlé systémy, jsou určitým řešením tzv. *certifikáty veřejných klíčů*, kde je spolehlivě spojen veřejný klíč s patřičnými informacemi. Spolehlivé vázání je u certifikátů řešeno digitálním podpisem - operací s privátním klíčem entity, která takto vlastně prohlašuje vazbu za důvěryhodnou. V posledních letech slýcháme stále častěji o infrastrukturách veřejných klíčů a o potřebě využití služeb certifikační autority nebo tzv. důvěryhodné třetí strany. Pokud nám někdo zajistí infrastrukturou jen spolehlivou výměnu veřejných klíčů uživatelů a tím nám vlastně umožní navázat bezpečnou komunikaci, označujeme tuto stranu jako *certifikační autoritu*. V podstatě jde o vystavení potvrzení ve smyslu „tento veřejný klíč patří uživateli *XY*“, samozřejmě za využití digitálního podpisu. Uvedení e-mailové adresy a dalších informací nám pak pomůže zjistit ještě přesněji, o kterého *XY* se jedná. Certifikační autorita obvykle nezajišťuje jen vlastní certifikaci klíčů, ale také udržování údajů o platnosti klíčů a to buď odvoláním (revokací) klíčů, nebo opětným potvrzením klíčů (rekonfirmací); což souvisí s liberálním nebo konzervativním přístupem k důvěře vůči klíčům. Naproti tomu důvěryhodné třetí strany poskytují další služby, jako např. spolehlivé služby elektronického notáře, nezvratné označení času u datových položek (tzv. časová razítka) a je také mnohými vládami zvažována pro podporu depozitování soukromých klíčů.

Významnými představiteli norem certifikátů jsou standardy *PGP (Pretty Good Privacy)* a *X.509*. Významným rysem certifikace *PGP* klíčů je to, že ji uskutečňuje každý uživatel sám, na základě vlastních informací a podle vlastního rozhodnutí. Tak je vlastně správa klíčů přímo pod kontrolou uživatele. Velkou nevýhodou obvyklého využití *PGP* klíčů je pak to, že není jasně prosazována homogenní bezpečnostní politika ani uvnitř jedné domény a až příliš často je třeba se spoléhat v mnoha kritických funkcích na korektní a zodpovědný přístup zúčastněných členů. Naopak certifikáty podle standardu *X.509* jsou vždy vytvářeny certifikační autoritou, která je také revokuje. Významným rysem plynoucím z *X.509* je stromová struktura, kdy daný uživatel a jeho klíč spadají pod jednu certifikační autoritu, ta pak může spadat pod další nadřazenou atd., až se dostaneme ke kořenové certifikační autoritě. Problém ale spočívá v tom, že jednoznačné pojmenování existuje snad jen v určité doméně, např. malé firmě. V této doméně lze s určitým úsilím a v závislosti na její velikosti také prosadit jednoznačnou bezpečnostní politiku a zavést nějaké konvence. Jak uvádí [118], daleko závažnějším problémem je skutečnost, že certifikační autorita může

poměrně jednoduše falzifikovat podstatná data v neprospěch strany, jejíž pár kryptografických klíčů je předmětem sporu. Podle *X.509* je totiž certifikační autorita zároveň i revokační autoritou. Navíc je struktura seznamu revokovaných certifikátů certifikační autoritou libovolně modifikovatelná, aniž by modifikace byla bezproblémově a jednoznačně prokazatelná. Pro ověření certifikátu *X.509* je potřeba mít k dispozici také veřejné klíče (certifikáty) všech nadřízených certifikačních autorit až po tu certifikační autoritu, které lze bezmezně důvěřovat a jejíž klíč je zaručeně bezpečný. To obvykle znamená potvrzení nebo dodání certifikovaného klíče nezávislou cestou, nejlépe zveřejněním v tisku, osobním odběrem od důvěryhodného zástupce atp. V žádném případě nelze za spolehlivou metodu považovat zveřejnění klíče na Internetu, jeho dodání v rámci aplikace WWW ap. Jakýkoliv podvod nebo selhání certifikační autority znamená porušení důvěry ve všech větvích stromu certifikačních vztahů pod touto autoritou.

Pokud jde o *ověřování klíčů* ve smyslu jejich aktuální platnosti, lze je podle autora studie [118] dělit na

-*konzervativní*, kdy každý klíč, resp. certifikát považujeme za neplatný až do okamžiku, kdy jsme spolehlivým způsobem zpraveni o opaku - např. potvrzením vydaným certifikační autoritou, spolu se spolehlivým označením času;

-*liberální*, kdy klíče, resp. certifikáty považujeme za platné až do okamžiku, kdy jsme informování o opaku , např. prostřednictvím seznamu revokovaných certifikátů.

Certifikační autority v praxi. Celkový počet certifikačních autorit lze dnes odhadovat řádově na desetitisíce; protože ne všechny nabízejí služby veřejnosti, většinou se jedná o certifikační autority tzv. uzavřených skupin uživatelů. Seznam mnoha významných veřejných certifikačních autorit je dostupný na Internetu. Nešvarem mnoha certifikačních autorit je bohužel jednání hraničící často až s nekompetencí. A to jak v zahraničí, tak i u nás. Důvěřovat, ale prověřovat, tak zní dávná moudrost, která je u nás platná dvojnásobně. Podle [118] byla již učiněna zkušenost s českou certifikační autoritou, jejíž zástupci nebyli schopni aplikovat digitální podpis u vlastních e-mailů a k dovršení všeho e-maily opatřovali elektronickými podpisy (což je řetězec znaků na konci e-mailu) jiných osob, než byli sami odesilatelé v záhlaví e-mailu. Dalším problémem je nespolehlivost cesty, používané k distribuci a ověření veřejného klíče vrcholné (kořenové) certifikační autority. Zahrnutí certifikátů do nové distribuované kopie WWW prohlížeče není příliš spolehlivou metodou, i když je samozřejmě spolehlivější než stažení certifikátu po Internetu. Výzkumný tým oddělení počítačové bezpečnosti na univerzitě v anglické Cambridge navrhl řešení, které spojuje prvky tradiční důvěry s důvěrou potřebnou pro elektronické obchodování. Pro práci s kryptografickými aplikacemi platí, že bezhlavé klikání myší na řadu tlačítek *OK* nebo mačkání *Enter* se jednou vymstí. Akceptováním jednoho klíče nespolehlivé certifikační autority můžeme přijít k mnoha dalším klíčům, které způsobí více škody než užitku. Předtím než můžeme důvěřovat, musíme prověřovat! Na akceptování právě jen dobrých a potřebných klíčů je založeno vybudování systému, kterému můžete s velkou jistotou důvěřovat, a o němž jsme přesvědčeni, že může zvýšit počítačovou bezpečnost a čelit tak případným počítačovým deliktům.

Jak dále uvádí [118], zajímavý je i pohled na důvěru jako takovou, samozřejmě v oblasti boje s počítačovou kriminalitou. V základní rovině lze snad říci, že jde o víru, že systém splňuje dané bezpečnostní požadavky a specifikace. Na věc se však lze také podívat z úplně jiného úhlu. Zde máme na mysli porušení bezpečnostní politiky bez zanechání jakýchkoliv stop v podobě průkazné evidence. Autor [118] říká, že tyto dva pohledy nejsou nutně v protikladu!

8.3. Problémy boje s počítačovou kriminalitou

Běžný občan si představuje preventivní činnost orgánů činných v trestním řízení jako každodenní, jinak však podle okolností příležitostné výchovné působení zejména policejních představitelů na občany. Realita je ovšem poněkud jiná. Po listopadu 1989 došlo k značnému nárůstu trestné činnosti ve všech oblastech. Jak uvádí autor studie [39], při střízlivě prostém hodnocení se často zjednodušeně hovoří o jakési „dani" za demokracii, kterou platíme bez rozdílu všichni. Orgány činné v trestním řízení proto vynakládají obrovské úsilí na potlačování trestné činnosti jako takové. Prostor pro prevenci tak zůstává jen velmi malý. Jednou z účinných forem preventivního působení je rychlé dopadení a potrestání pachatele trestného činu. To platí jak obecně, tak i pro počítačovou kriminalitu a zvláště pro její snad nejnebezpečnější formu, softwarové pirátství.

Systém trestního řízení v naší zemi, kdy policista předá podezřelého vyšetřovateli, který mu sdělí obvinění z trestného činu a po zpracování případu věc předá státnímu zástupci s návrhem na podání obžaloby, státní zástupce pak podá obžalobu soudu, před kterým se koná hlavní líčení, není ani jednoduchý, ani rychlý. Jeho spletitost a nutnost překonávání různých překážek je mnohdy důvodem značného časového odstupu mezi zadržením pachatele a jeho odsouzením. Tím je narušen jeden z velmi účinných způsobů preventivního působení na občany, totiž neodvratnost bezprostředního trestu. Každý již zná situace, kdy obviněný z trestného činu, vyšetřovaný na svobodě, pokračuje dále v trestné činnosti. Navíc značná doba mezi spácháním trestného činu a odsouzením vyvolává v řadě lidí pocit beztrestnosti. Samotný trest udělený někdy i po letech tak ztrácí na své účinnosti. Dalším nemalým problémem je novum stíhání porušování autorského práva. S trestním postihem porušování autorských práv podle §152 trest.zák., se v širším měřítku začalo až po roce 1989. Je tedy jedním z negativních dědictví minulosti, že systém není zcela připraven na trestní stíhání tohoto trestného činu. Jestliže u nás byla učiněna určitá zkušenost s trestním stíháním za pirátské audio a video nosiče, nebo za nelegální hudební produkce, tak softwarové pirátství je zatím stále ještě určitou novinkou. Samozřejmě nelze vidět vinu jen v samotném systému. Ten je postaven na lidech, kteří svou prací musejí naplňovat literu zákona. Z praxe orgánů činných v trestním řízení jsou však známy velké problémy při realizaci boje s trestnými činy spojenými s počítačovou kriminalitou, zejména pak s pirátskými delikty, týkajícími se počítačových programů. Problémy začínají často již na úřadech vyšetřování. Vyšetřovatelé nejsou mnohdy dostatečně připraveni na stíhání této trestné činnosti. Příčiny tkví v minulosti. Již před rokem 1989 tehdejší Československo podepsalo dvě úmluvy. *Bernskou úmluvu o ochraně literárních a uměleckých děl* z roku 1986, ve znění pařížské revize z roku 1971 a *Všeobecnou úmluvu o autorskému právu* z roku 1952 v Ženevě ve znění pařížské revize z roku 1971. Tím jsme se mimo jiné zavázali respektovat autorská práva a v souvislosti s tím byl zařazen do trestního zákona §152, porušování autorského práva. Nelze tedy říci, že před rokem 1989 u nás byla v tomto směru právní libovůle. Problém spočíval a stále trvá v naplňování těchto úmluv a v jejich prosazovaní do života. Na základě politického rozhodnutí bylo plnění úmluv v této oblasti minimalizováno a respektování autorských práv, pokud jde o

software téměř nulové. Tomuto postupu nahrávala i situace ekonomických a jiných sankcí, kdy legálně získat zahraniční programový produkt bylo téměř nemožné. Ale ekonomika a i jiné oblasti počítačové programy stále více vyžadovaly. Proto bylo považováno za naprosto normální, když byl do země různě „pašován“ software ze zahraničních zájezdů, seminářů a i vědeckých konferencí. Je možno říci, že získání kvalitního západního software bylo úspěchem a většinou nikoho nenapadlo, že jde vlastně o trestnou činnost.

**

Domácí uživatelé velmi hřeší na omezené možnosti policejních orgánů. Myšlenka masových kontrol v bytech spojených s „prohledáváním“ počítačů ke zjištění nelegálního software je skutečně nepřijatelná, ať už z jakéhokoli důvodu. Hlavním motivem k ukončení činnosti softwarového piráta tak není strach z trestního postihu. Takový člověk nemá obavu z následků, které by mu reálně hrozily. Vzhledem k minimu realizovaných případů (u nás asi 30-40 ročně) nemají lidé možnost vidět ve svém bezprostředním nebo i vzdálenějším okolí příklad policejní aktivity. Odsouzeno bylo zatím jen několik osob. Lidé si stále myslí, že jsou v podstatě nepostižitelní. Jde o chybný úsudek. Každý takový člověk by si měl uvědomit, že nežije ve vakuu, a že počítačové programy nevznikají samovolně a nelze je jen tak kdekoliv najít a sebrat. Existuje mnoho nekalých aktivit spojených se získáváním nového software - nákup přes inzeráty, od známých a kamarádů apod. Čím více dotyčný uživatel takové aktivity preferuje, tím stále více osob ví, co dělá a jakým software disponuje. Obvykle si totiž prodejci nelegálních počítačových programů vedou evidenci zákazníků a odebraného zboží, podobně jako jiní dobří obchodníci. Navíc bohužel mají v povaze při přistižení ukazovat na ostatní. Jako by to mělo přímý vliv na výši trestu. Z těchto důvodů tak policie nepotřebuje ve všech případech hromadné domovní prohlídky, protože informace získá jinak, a následně přijde udělat prohlídku pouze ke konkrétní osobě. Obvykle s úspěchem. Následky jsou pro pak již obviněného velmi nepříjemné.

Jako příklad uvádí autor článku [40] případ z roku 1997, kdy určitý muž prostřednictvím inzerce nelegálně prodával počítačové programy *Mapa Prahy, DOS, Microsoft Word a Windows*. Byl odsouzen Okresním soudem v Litoměřicích k trestu odnětí svobody v trvání čtyř měsíců s podmínkou na jeden rok, k peněžitému trestu ve výši 10 000 Kč a k propadnutí věci - datových nosičů. Postih jistě citelný, navíc se pochopitelně trest zapsal do rejstříku trestů, kde řadu let bude na požádání upozorňovat, že dotyčná osoba byla odsouzena za úmyslný trestný čin.

Takových případů, odsouzených softwarových pirátů bude zřejmě přibývat. I přes obecně známou pomalost naší justice roste počet podání obžaloby a projednání před soudem. Každý uživatel si tak bude moci zjistit, jaké následky mu jeho činnost přinese.

Výroba nelegálního software již není tak diskusní otázkou jako prosté užívání. Lze opatrně připustit, že uživatel nelegálního software nemusí vždy vědět, že tak činí. Může jít ve výjimečných případech i o neúmyslnou činnost. Kdo ale vyrábí datové nosiče, obvykle

se záměrem je prodat, nikdy se nemůže vymluvit na chybějící úmysl. To platí v největší míře o průmyslové výrobě.

**

Problematika CD-disků. S výrobou CD-disků jsou u nás tradičně spjaty Gramofonové závody Loděnice v okrese Beroun. Patří k našim největším výrobcům takových nosičů, především v audio oblasti. Ale u tohoto výrobce nedocházelo k zadávání objednávek ze strany továrny. Objednavatelem byla jiná osoba, ať již právnická, nebo fyzická. V konkrétním případě podepisoval zadavatel zakázky doklad, kde uvedl, že je nositelem autorských práv. Právní odpovědnost ležela tedy na něm. Jiným případem jsou „lisovny", které jsou od prvopočátku zaměřeny na nelegální produkci. Zde vznikají problémy především v Bulharsku a z našich sousedů v Polsku. Z hlediska průmyslové výroby většina nelegálních CD-disků na našem trhu pochází z dovozu. Dováží se vše, co požaduje „trh". Licencovaný software, jako jsou operační systémy a kancelářské balíky nebo hry. V současné době se nedá říci, že by Česká republika byla masivně zaplavována nelegální produkcí ze zahraničí. Náš trh není tak zajímavý jako západoevropské země nebo třeba Polsko, kde je potenciálních kupců asi pětkrát více než u nás. Pro vlastní odhalení dovozu nebo výroby nelegálních datových nosičů, především CD-disků, je nutno získat vzorek, a ten podrobit zkoumání pro získání informací vedoucích k odhalení výrobce a následně i pachatele. Na nosiči výrobce povinně zaznamenává vlastní identifikaci a některé další znaky. Podle toho lze u produkce legálního výrobce nosiče zjistit, o jakou zakázku šlo a pro koho. Tento stav výrazně ovlivňuje možnosti odhalení trestné činnosti. To je ovšem ten nejjednodušší příklad. Obvykle jsou totiž CD-disky lisovány u výrobce, který nemá nejmenší zájem na vlastní identifikaci. Proto vybaví takový nosič nic neříkajícím označením a neuvede ani vlastní výrobní značku (Gramofonové závody mají značku GZ). Mnohdy jednotliví výrobci (např. v Bulharsku) mají alespoň vžité obvyklé označení, které dovolí získat i když jen minimální základní informace. To ale neplatí vždy. V případě zjištění výskytu průmyslově vyrobených CD-disků je tedy v první řadě nutno zjistit, zda jde o domácí výrobek, nebo dovoz. Podstatně složitější je situace u CD-disků v zahraničí vyrobeného a k nám dovezeného, kdy je ztížena identifikace osob, které nechaly CD-disk vyrobit, a dalších, které nosiče dovezly na naše území. Umístění CD-disku na trh předpokládá existenci distribučního kanálu, který přivede produkt k prodejci, a odtud k zákazníkovi. Tento poněkud složitý model se v praxi realizuje prostřednictvím jen několika osob, které nosič nechaly vyrobit nebo již hotový získaly v zahraničí. Pak už jej vlastními silami, inzercí, případně cestou dalších osob umisťují na trh. Způsob distribuce obvykle přímo ovlivňuje i rychlost odhalení takové činnosti. Aktivity konkrétních osob jsou jejich nejslabším článkem. Z logiky distribuce a z charakteru prodeje je naprosto zřejmé, že tuto činnost nelze nikdy dostatečné utajit a je jisté, že se nedá realizovat naprosto anonymně. To obvykle vede k identifikaci konkrétní osoby a následné aktivitě policie směřující k sdělení obvinění pachateli. Je zřejmé, že veškeré snahy o prodej nosičů s nelegálním softwarem jsou pro pachatele vždy nebezpečnou hrou. Avšak zisky z této činnosti jsou velmi přitažlivé. Není potřeba žádných surovinových zdrojů, výrobky jsou skladné a především nedochází tak zvaně ke „krádeži" hmotné věci. Duševní vlastnictví je právě i z těchto důvodů pro pachatele velmi atraktivní.

Při zachycení podezřelého CD-disku musí policie nechat odborníkovi k posouzení, zda jde o pirátský software. Mnohdy je totiž možno narazit na takto distribuované produkty *shareware* nebo *freeware*. U produktů shareware je v některých případech umožněno autorem jeho distribuování a prodej i způsobem, který může vzbudit podezření z trestné činnosti. To dokresluje spletitost různých možností a práv v oblasti počítačových programů. Naproti tomu freeware, a zvláště *public domain*, umožňuje v podstatě plné šíření, jak vyplývá i z názvu této kategorie programů. Teprve až potvrzení autora, že jde o volně šiřitelný software, odstraní mnohdy podezření z trestné činnosti. Na druhé straně taková tvrzení občas užívají i pachatelé. Při samotném policejním šetření je totiž velmi obtížné na místě anebo ve velmi krátké době identifikovat software. To platí i pro užívání různých utilit pro zlepšení a podporu software, včetně složitějších systémů her. Stává se, že spolu s „ostrými" verzemi software jsou na nosičích též produkty shareware i freeware. Orgány činné v trestním řízení musí proto většinou spoléhat na odbornou pomoc, kterou lze používat podle zákona nebo podle služebních předpisů. Tedy pomoc soudního znalce nebo znalce z kriminalistického ústavu. Mnohé chyby při objasňování již nelze nijak napravit. V případě, že je potvrzeno, že jde o CD-disk s pirátským software, je především nutno dokumentovat výskyt nosičů a zjistit osoby spojené s touto činností. Nelze předpokládat, že s touto formou trestné činnosti budou spojeni jen lidé pracující s počítači nebo odborníci. Často jde o lidi více méně obeznámené s výpočetní technikou, ale jinak s jednoznačnou tendencí k požívání zisku. Trhovci prodávající u svých stánků obuv a oděvy s falešnými výrobními značkami jistě nejsou nijak zběhlí v oděvní problematice. Analogicky je tomu tak i u distributorů software. Dovoz, distribuce a prodej nelegálně vyrobených nosičů s programy pro výpočetní techniku ve velké většině překračuje území okresu, kraje, státu. To následně komplikuje vyšetřování případů a vede k nutné spolupráci všech místně i odborně kompetentních orgánů. S tím souvisí řada dalších organizačních a technických problémů, které však již nebudeme blíže specifikovat.

**

Problémy boje s nelegálními kopírovacími službami. Většina společností a jednotlivců zabývajících nelegálním zálohováním software využívá tvrzení, že provádějí pouze technický úkon a ani nevědí, jaký software kopírují. Vyvrátit toto tvrzení je poměrně jednoduché. Není totiž možno jednoduše akceptovat odmítnutí odpovědnosti daného subjektu za následky jeho činnosti. Krom toho, jak vyplývá z autorského zákona, může kdokoliv disponovat pouze jednou „bezpečnostní" kopií, kterou si tedy může nechat vytvořit jako službu. Ovšem to znamená, že přináší ke kopírování originální nosič. Není možno vyloučit, že oprávněný uživatel této služby legálně využije. V praxi jde ovšem o minimum zákazníků. Zadavatel obvykle přináší na nosiči již nelegálně „vypálený" software. Za těchto podmínek realizovaný technický úkon se stává trestným činem podle §152 trest. zákona. Častý je též opakovaný výskyt zákazníků se stejným požadavkem na vytvoření již několikáté bezpečnostní kopie. Je jasné, že v takovém případě se firma nemůže příliš vymlouvat. Podnikatel, který je rozhodnut respektovat zákon, musí vytvořit takové podmínky, aby předešel možnému trestnímu stíhání. Mezi osvědčené základní předpoklady patří minimálně

-jednoznačná smlouva o vztahu mezi zákazníkem a firmou, včetně seznamu kopírovaného software a důvodu kopírování,

-jasné podmínky poskytování služby, včetně odkazů na legálnost kopírovaného software, případně vlastních dat,

-možnost odmítnutí služby při porušení podmínek.

Jak již bylo uvedeno v souvislosti s problematikou CD-disků, technické bariéry kopírovacích aktivit jsou již překonány. Dnes již v podstatě každý může na svém počítači s „vypalovací" mechanikou vytvářet buď kopie originálu, nebo sbírky všeho možného. Obvyklejší bývá druhý případ. I přes to se stále ještě vyskytují nabídky na kopírování dat. Někteří jedinci pak nabízejí, že přijdou i do soukromí k zákazníkovi. Pravděpodobně disponují přenosnou mechanikou. Nelze ovšem paušálně takovou činnost odsuzovat. Pro řadu i domácích uživatelů má smysl zálohování pevného disku na jiné médium, které umožní bezproblémové a rychlé obnovení ztracených dat. Ale bohužel jen málo uživatelů sleduje tento cíl. Někteří pachatelé na svou obhajobu uvádějí, že když nekalou činnost dělají jiní, proč by to nemohli také oni. Zde jsme opět u aspektů morálky, a to převážně morálky podnikatelské. Je na povážení, že honba za ziskem některých spoluobčanů nebo firem překračuje všechny možné konvence, od norem slušného chování až po ustanovení trestního zákona. Každý trestně odpovědný občan nese plnou odpovědnost za své chování. Platí to i pro majitele firem, kteří umožňují nebo uskutečňují nekalou činnost. Odpovědnost nesou nejen morální, ale především i v trestním řízení. Boj pak nutno vést proti nim nejen po stránce trestního postihu, ale i formou preventivního usměrňování.

Půjčování software. Obecně není půjčování software dovoleno zákonem. Odchylně může tuto činnost upravit smluvní ujednání mezi autorem (nositelem autorských práv) a oprávněným uživatelem. Jedním ze způsobů půjčování je pronajímání výpočetní techniky spolu se softwarem instalovaným podle přání zákazníka. Podle dosavadních zjištění (viz [40]) žádná ze známých softwarových firem, např. *Microsoft, AutoDesk, Software602* atd., půjčování neumožňuje. Pokud se tak děje, jedná se o porušování autorského zákona, a tím o trestný čin podle §152 trest. zákona. Zatím není znám žádný autor, který by umožňoval půjčování svého programu. Totéž platí o společnostech či firmách tvořících software. Důvody jsou pravděpodobně finanční. Je výhodnější software prodávat, než půjčovat. Můžeme si představit určité příklady potřeby zapůjčování počítačových programů, od nutnosti zpracování písemností v nařízeném formátu, až po prepubertální zábavu v hernách. Vše však by mělo být legální. To znamená založené na smlouvě mezi autorem a provozovatelem. Např. firmy pro zahraniční počítačové hry by byly ochotny uzavřít smlouvy s hernami. Avšak provozovatelé heren by museli část svého zisku odevzdat podle autorského zákona autorovi. A to nechtějí. V dohledné době se zvýší tlak na tyto herny a i jiné půjčovny software s cílem upevnit zákonnost v této oblasti. Strategie boje je pak založena opět na vyhledávání příslušných služeb v inzerci nebo na různých místních vývěskách apod. Aktivity tohoto typu bývají regionálně omezeny. Důvodem je pravděpodobně určitá nejistota provozovatelů nebo strach z postihu. Ale nelze hovořit o jakémkoliv schovávání nebo utajování vlastní činnosti. Pro orgány činné v trestním řízení je důležité, že v podstatě není problémem identifikace osoby podezřelé z této trestné činnosti. Hranou naivitu některých takových „podnikatelů" nelze akceptovat. Neznalost zákona neomlouvá. Pro samotnou policejní práci je pak prvořadé kontaktování majitele

autorských práv s cílem získání odpovědi na otázku, zda půjčování umožňuje. V negativním případě je činnost půjčovny jednoznačně porušením trestního zákona.

Prodej nelegálních programů s výpočetní technikou jako jedna z forem šíření nelegálního software, vyžaduje při potírání aplikaci jistého specifického přístupu. Nejčastěji dochází k tomu, že výrobce nebo prodejce s cílem získání většího okruhu zákazníků, do počítače nainstaluje různý software, k jehož šíření (prodeji) není oprávněn. Tyto počítačové programy pak obvykle nejsou uvedeny na faktuře ani jiném nabývacím dokladu k výpočetní technice. K takové činnosti je zneužívána obchodní politika prodeje tzv. *OEM software*, což je prodej počítačových programů za nižší ceny společně s novou výpočetní technikou. Tato forma prodeje je však smluvně vymezena a software je součástí fakturovaného zboží, což se uvádí i na dodacím listu. Represe nelegálních aktivit je pak založena zpravidla na upozornění policie ze strany autora nebo výrobce software, který zjistí, že obchodník prodává jeho počítačové programy bez smluvního ujednání. Vlastní aktivitou je tato činnost obtížně zjistitelná, protože tyto informace jsou známy jen úzkému okruhu osob z relace „prodejce-zákazník". Jsou však známy případy, kdy výše uvedenou nelegální aktivitu oznámil i zákazník. Popsaná protiprávní činnost je v podstatě velmi jednoduchá. Výrobce, obvykle neznačkový montér sestavující počítače z různě sehnaných dílů, přidává jistý bonus. K podezření někdy svádí inzerce výrobců, kteří se předhánějí v lovu na zákazníky různými tvrzeními o množství software dostupného výlučně v jejich počítačích při zachování minimálních cen. V takových případech je nutno vše prověřit u výrobce. Buď předloží doklady o legálnosti jeho postupu, a pak není co řešit, anebo je nepředloží a následuje sdělení obvinění podle platné zákonné úpravy.

**

Problémy Internetu. Získávání informací z Internetu spočívá obvykle ve vyhledávání požadovaných volně dostupných dat a jejich vytřídění nebo zkopírování na pevný disk. K dokreslení celé situace je nutno uvést, že tzv. „informační dálnice", která více či méně začíná fungovat v západní Evropě a velmi dobře již pracuje v USA, je u nás zatím fenoménem budoucnosti. Možná nedaleké. Každý, kdo zkusil získat nějaký objemnější software ze zahraničního serveru, ví, jak je to obtížné. Nejen pomalé linky, ale i chyby při přenosu dělají z takové aktivity na našem území často velmi nepohodlnou činnost. Lze předpokládat, že do budoucna se situace může a zřejmě bude pouze zlepšovat. I přesto nemůžeme vyloučit získávání nelegálního software touto cestou. Jednou z možných legálních aktivit je instalace software nabízeného počítačovými výrobci a dalšími firmami uživatelům Internetu. Variantou toho je zkopírování nelegálního software na pevný disk a jeho užívání. V absolutní většině případů je takový software jednoznačně jako nelegální označen. V podstatě každý, kdo takový software kopíruje a užívá, tento software již vědomě vyhledal jako nelegální. To dává policii velmi dobrou možnost k vyřešení otázky, zda podezřelý konal úmyslně, či nikoli. Obecně platí, že taková činnost je nelegální. Podle autora [40] je na našem území několik míst, kde se masivně „stahuje" nelegální software z Internetu a nabízí dalším uživatelům. Tato činnost vyžaduje neomezené, kvalitní a rychlé připojení k Internetu. Je s podivem, že jsou to převážně vysoké školy, které svým liberálním přístupem dovolují svým studentům to, co by jinde nešlo. Nelze takovou činnost omlouvat akademickou svobodou nebo zlehčovat tvrzením o nutnosti

získání informací studenty. Pochopitelně stahování nelegálního software na Internetu je i záležitostí jednotlivců, kteří na své domácí počítače takto získávají některé programy zdarma k užívání. Dokumentování a objasňování této trestné činnosti je u nás teprve v začátcích, stejně jako v západní Evropě. Pouze v USA jsou ve stíhání podobných deliktů poněkud dále. Proto zatím neexistuje v současné době v naší literatuře dostatek přesných a náležitě konkrétních informací.

**

Obecně k boji s počítačovou kriminalitou. Autor studie [110] uvádí, že vzhledem k náročnosti postupů objasňování deliktů spjatých s počítači, musí policie řešit současně mnoho problémů. Jde však hlavně o správné stanovení obsahu a rozsahu předmětu dokazování, aby byla zabezpečena objektivnost, úplnost a rychlost vyšetřování. Úspěšné vyšetření každého trestného činu totiž závisí na správném určení okolností, které jsou nezbytné pro posouzení věci. Je tedy užitečné vyjasnit, co je třeba dokazovat v trestním řízení. Podle ustanovení §89 odst.1 trest. řádu je třeba dokazovat zejména

-zda se stal skutek, v němž je spatřován trestný čin,

-zda tento skutek spáchal obviněný, případně za jakých pohnutek,

-podstatné okolnosti mající vliv na posouzení nebezpečnosti činu,

-podstatné okolnosti k posouzení osobních poměrů pachatele,

-podstatné okolnosti umožňující stanovení následku a výše škody způsobené trestným činem,

-okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání.

Z ustanovení §89 odst.2 trest. řádu vyplývá, že za důkaz lze považovat vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Současně je třeba mít na zřeteli, že rozsah dokazování je vždy konkrétně determinován nejen jednotlivými znaky skutkové podstaty trestného činu, ale také zvláštnostmi daného případu.

Trestné činy související s výpočetní technikou, s nimiž se můžeme u nás setkat, nemusí být jen čistě „počítačové“, ale obvykle naplňují také skutkovou podstatu dalších, „běžných“ trestných činů. Podle [199] za zvláštní zmínku stojí

-prodej cizích programů firmou, která neměla oprávnění programy prodávat (§152 trest.zák.-porušování autorského práva, v souběhu s neoprávněným podnikáním podle §118 trest.zák.),

-daňové podvody postižitelné podle §125 trest. zák.- zkreslování údajů o stavu hospodaření a jmění,

-případy, kdy programátoři sdělili svému zaměstnavateli, že zpřístupní určitá zakódovaná data (nebo programy) ve firemním počítači pouze tehdy, uzavře-li s nimi autorskou smlouvu a zaplatí-li jim větší finanční částku; tato, dle názoru autora [199], zcela mylná aplikace autorského zákona bezpochyby naplňuje skutkovou podstatu trestného činu podle §235 trest.zák.- vydírání;

-počítačový podvod ve sféře bankovnictví v roce 1992, kdy pachatel zdefraudoval v pobočce České spořitelny postupně částku okolo 35 mil. Kč změnou údajů v souborech platebního styku při převádění mnoha postupně se zvyšujících částek na své účty; odsouzen byl pro trestný čin podvodu podle §250, odst. 4 trest.zák. k odnětí svobody na osm let;

-používání počítačů zaměstnavatele k soukromým účelům, což by mohlo naplňovat skutkovou podstatu neoprávněného užívání cizí věci podle §249 trest.zák.; ovšem ve sféře osobních počítačů je dokazování v tomto případě velmi obtížné, navíc znění tohoto ustanovení míří poněkud jinam, totiž do oblasti jednání, v jejichž důsledku je majitel věci byť krátkodobě omezen v právu s věcí disponovat; může být sporné, zdali lze pod tuto skutkovou podstatu podřadit případ, kdy sice vlastník počítače není nijak omezen v dispozicích s počítačem, neboť umístění počítače se nemění, ale zaměstnanec používá počítač ke své potřebě; vše komplikuje ještě složitější situace při multiuživatelském přístupu k počítači;

-finanční hry typu „letadlo“, vycházející z principu pyramidového efektu, kdy vyhrává vždy jen několik účastníků na prvních místech (z řad organizátorů), zatímco počet neúspěšných hráčů může jít až do desítek tisíc; na enormní výskyt těchto her, provozovaných často s pomocí nejmodernější výpočetní techniky, reagoval zákonodárce vložením ustanovení §250c trest.zák. o provozování nepoctivých her a sázek (s maximální sazbou odnětím svobody až pět let); vyšetřování těchto případů je velice náročné, protože v řadě případů neexistují řádné doklady o průběhu hry a výslechy desítek tisíc poškozených přesahují kapacitní možnosti orgánů činných v trestním řízení.

Zkušenosti softwarových firem s právní problémy při vedení sporů. Autoři studie [98] uvádějí nejčastěji se vyskytující právní problémy při vedení sporů, které se po ukončení policejního vyšetřování dostanou až před soud. Vycházejí ze zkušeností z 10 zemí Evropy a 20 zemí zbytku světa. Autoři shledali, že se určité otázky objevují vždy opakovaně. Patří k nim zejména

-jakým způsobem zjistíme, že se na počítači nachází software a zda se jedná o instalaci legální nebo nelegální kopie;

-je-li konkrétní software chráněn autorským zákonem či nikoliv, v některých zemích tato otázka nebyla ještě rozhodnuta;

-zdali je software původní, což bývá často předmětem častého zkoumání u soudu; všude v podstatě platí, že program je chráněn autorským zákonem pouze tehdy, je-li původním tvůrčím dílem; po určitém období počáteční nejistoty a diskusí v některých zemích (včetně Německa) se nyní již standard původnosti vyjasnil; stručně lze říci, že za původní dílo je považován takový program, který vytvořil programátor samostatně (sám jej vymyslel a vyvinul) svým vlastním přičiněním nebo společně s ostatními pracovníky;

-kdo je vlastníkem programu; většina soudů aplikuje velice jednoduchý test - vychází se z předpokladu, že vlastníkem programu je firma, která program vytvořila a na obžalovaném je, aby vznesl důkazy o opaku; v tomto ohledu se za důležité důkazy považují různé dokumenty a též registrační karty, kterými se vlastník programu zavazuje k dalším závazkům vůči uživateli;

-spory o práce realizované zaměstnanci v počítačových firmách; jde o teoreticky dosti složitou záležitost s různými aspekty náhledu v různých zemích; s vývojem počítačové

problematiky došlo též k podstatné změně zákonů i výkladu stávajících legislativních úprav; většinu software vytvářejí desítky, v některých případech dokonce stovky programátorů a dalších vývojových pracovníků, společně zpravidla v jedné firmě; je jasné, že za takovéto situace je velice důležité vědět, kdo je vlastníkem práva na ochranu software; nemělo by žádný smysl, aby každý jednotlivý zaměstnanec počítačové firmy vlastnil třeba jednu setinu programu, právní praxe se proto vyvíjí v tom smyslu, že nositelem vlastnického práva k programům, které byly vytvořeny zaměstnanci, se stane zaměstnavatelská organizace - počítačová firma;

-problematika soudních příkazů k prohlídce; zjištěné důkazy v oblasti softwarového pirátství bývají velice snadno zničitelné; podobně jako lze něco okopírovat z diskety do počítače během několika málo sekund, stejně tak lze během okamžiku zničit vše, co je nelegálně nahráno na magnetických mediích, tedy zničit důkazy, které jsou pro danou kauzu důležité; pokud se kontrolní akce předem prozradí, pachatel v klidu vše nelegální smaže a zničí tak jednoduše veškeré důkazy a potom, jakmile pomine nebezpečí kontroly, vše znovu nainstaluje; je proto zapotřebí, aby příkazy či povolení k prohlídkám byly vydávány promptně, bez zbytečných průtahů a v naprosté tajnosti, tj. především bez předběžného upozornění podezřelého;

-otázky výpočtu škod nebo pokut; paděláním software se dají vydělat obrovské částky peněz; v některých státech je softwarové pirátství dokonce stejně výnosné (a mnohem bezpečnější), než ilegální obchodování s narkotiky; padělání software se rychle rozšiřuje a současně dochází i k tomu, že obchodníci s hardwarem se uchylují k levným ziskům z prodeje ilegálního software; jediný způsob, jak je možné tyto lidi odstrašit nespočívá ovšem v tvrdých postizích, ale v neodvratnosti trestu za takovéto počínání; na druhé straně je ovšem třeba, aby soudy neváhaly ukládat vysoké pokuty a předepisovat značně vysoké náhrady škod, samozřejmě v souladu se zákony; jedině tehdy lze očekávat obrat k lepšímu; pro padělatele např. v Itálii jsou pokuty řádově desítek tisíc US dolarů zanedbatelné, když ve skutečnosti dochází při nelegální činnosti k milionovým ziskům; zákon by proto měl být přísný a jeho vynucování nesmlouvavé.

Přes všechny problémy s počítačovou kriminalitou, firmy většinou konstatují, že dochází na celém světě k pozitivnímu rozvoji softwarového průmyslu. V Evropě se rozšiřují místní vývojové softwarové firmy, vznikají nové pracovní příležitosti a programové vybavení počítačů se neustále zdokonaluje v přijatelných cenových relacích. Mnohé země a hlavní města střední Evropy jsou plná talentovaných programátorů i jiných specialistů. Lze předpokládat, že určujícím momentem prosperity těchto států pro další období budou podmínky pro uplatnění těchto talentů. K tomu by měl přispět i nesmlouvavý boj s počítačovou kriminalitou.

**

Zkušenosti kriminalistů podle autorů studie [104]. O problémech s počítačovými delikty se v literatuře objevuje stále více informací. Z nich lze odvozovat určitá metodická doporučení, jak postupovat proti počítačové kriminalitě. Vedle vlastních odborných znalostí a zkušeností s výpočetní technikou a vedle poznatků získaných z odborné literatury mají

zásadní význam praktické zkušenosti a poznatky (včetně taktických pochybení), získané v tomto oboru orgány činnými v trestním řízení. Potřebné informace by v tomto směru měly být uloženy v resortních informačních systémech. Zde však nutno předpokládat jistou míru neurčitosti a chyb. Není rozhodující na jaké technice a pod jakým programovým vybavením se ten který informační systém provozuje. Důležitější je, zda lze pomocí něho získat údaje odpovídající původnímu předpokladu, tj. zda lze obdržet informace o všem podstatném v daném oboru, teritoriu a období. Navíc pokud možno ve formě vhodné pro zadavatele a s předpokladem, že podle míry naléhavosti bude následně možné vyžadovat k prostudování i příslušné spisy. To jsou teoretické předpoklady, v praxi zpravidla málo splnitelné. Bohužel v některých resortech se preferuje více forma (např. otázky pořizování hardware a software) před obsahem (co a k čemu se výpočetní technikou zpracovává). Pracovníci, někdy i značně laičtí, zúčastnění na výběrech firem jsou pak zpravidla ceněni organizací daleko více než samotní výkonní specialisté. Mnohdy to může souviset i s úplatky vedoucích činitelů informačních útvarů ze strany zúčastněných firem.V policejní praxi lze pro získání přehledu o páchání trestné činnosti proti výpočetní technice, informačním systémům nebo programům (porušování autorských práv) využívat v podstatě dvou systémů *ESSK* a *NTC* o počítačové kriminalitě.

Systém ESSK (evidenčně statistické sledování kriminality) je uspořádaným souhrnem informací, které jsou do počítače vkládány ze speciálních formulářů vyplňovaných policejními orgány či vyšetřovateli. Nevýhodou systému *ESSK* je jeho nedostatečné programové vybavení pro specifické (nestandardní) dotazy a statistiky. Lze sice uskutečňovat dotazy podle všech položek, ale bez odpovídajícího tiskového výstupu.

Systém NTC (nápad trestné činnosti) je orientován na obecnou kriminalitu. Vstup do systému je realizován informacemi z jednotného formuláře. Skládá se z propojených databází (událostí, poškozených, stop, pachatelů, věcí) se snahou o odstranění dosavadních evidenčních duplicit. Kromě prověřování zaznamenaných případů (přes systém *ESSK)* existuje i možnost přímého zjišťování verbálního popisu případu ze systému *NTC*. Porovnáním s výsledky z *ESSK* jde tak o možnost další kontroly, což je v boji s počítačovou kriminalitou považováno za zvláště významný aspekt, usnadňující orientaci často ve značně složité situaci.

Vypracování metodiky boje s počítačovou kriminalitou by bylo počinem, vítaným všemi orgány činnými v trestním řízení. Nikdo nepochybuje o tom, že problematika objasňování počítačové kriminality má své zvláštnosti. Týká se to odhalování počítačových stop, jejich dokumentování, zajišťování a zkoumání. Své zvláštnosti má i metodika ohledávání a prohlídek, kde je zastoupena výpočetní technika. To však nenaplňuje bezezbytku veškerý boj s počítačovou kriminalitou. Bohužel se ukázalo (alespoň v současné době), že cesta zobecnění dosavadních zkušeností a ponaučení z případných pochybení nevede přes resortní informační systémy. Ne proto, že by byly nevhodně navrženy, budovány nebo provozovány, ale proto, že údaje vkládané do podkladů (tiskopisů, formulářů, statistických listů, speciálních rastrů), ze kterých se zavádějí do počítačových databází, nejsou odpovídající struktury či kvality. Mnohdy v tomto směru jde i o otázky adekvátní teoretické přípravy. Speciálně pak o vhodné volby ukazatelů a o jejich operacionalizaci v souladu

se základními principy kriminologické statistiky, jako metodologie práce s kriminálními statistikami, tj. s konkrétními daty o zločinnosti, viz např. [136], [138]. Počítačová kriminalita je pojem v různých periodikách značně rozebíraný, ale jako jev v kriminálních statistikách zatím nesledovaný. Kriminologická statistika však přesto disponuje přístupy využitelnými i v této oblasti (latence, perseverance, stochastika, testování hypotéz, multivariační přístupy, osobnost pachatele, viz [136], [137], [138]). Jak uvádějí autoři [104], vyhledávání a dokumentování počítačové či informační kriminality, stejně jako její objasňování resp. vyšetřování není jednoduché a dosud se nijak nezviditelnilo. Celkově nutno konstatovat, že teprve kvalifikovaným pokusem o využití informací z resortního informačního systému se zjistí, zda opravdu jde o funkční informační systém. Z pohledu konkrétní počítačové kriminality nemáme však k tomu zatím adekvátní možnosti.

**

Otázky zbytečné kriminalizace aktivit osob a firem. Je zřejmé, že nekalá činnost kolem instalace software do výpočetní techniky může být spíše trestným činem, ale vzato z druhé strany je nutno klást otázku, zda nejde o věc řešitelnou obchodním jednáním. Právě v oblasti aktivit *OEM* může přicházet v úvahu více nekalá soutěž podle obchodního zákoníku než trestná činnost. To je ovšem tvrzení polemické a jak uvádí autor studie [39], někteří odborníci jsou přesvědčeni o opaku. Rozhodně však je nutno proti nekalým praktikám v oblasti počítačové kriminality postupovat legálně v duchu zákonných ustanovení, což v rámci pirátských aktivit lze lapidárně vyjádřit slovy „proti pirátství nelze postupovat pirátsky“.

8.4. Organizace pro boj s kriminalitou

Problematikou autorských práv k softwaru se u nás zabývá několik autorskoprávních agentur, jejichž cílem je všestranné omezování softwarového pirátství. Spolupracují s policií zejména nejrůznějšími formami prevence, jakož i při odhalování, dokumentování a dokazování konkrétní trestné činnosti.

Organizace BSA CS. Busines Software Alliance (BSA) je jednou z největších světových organizací, které se snaží o prosazení legálního užívání software a potlačení softwarového pirátství. Byla založena v roce 1988 v USA z iniciativy nejdůležitějších producentů software pro osobní počítače. V současné době působí ve více než 60 zemích celého světa. V lednu roku 1993 vznikla její odbočka v Praze, jako lokální sdružení pro Čechy a Slovensko. Sdružuje čtyři výrobce software v ČR a SR *Microsoft, Software 602, Autodesk a APP Group*. Sídlo BSA CS bylo zřízeno v Praze. Mělo zřízenou „horkou“ linku pro možnost ohlašování případů nelegálního užívání software a získávání informací, týkajících se užívání software obecně. Působení BSA bylo rozděleno do tří sfér. Podle získaných zkušeností se došlo k závěru, že pouze propojení všech těchto tří sfér vedlo k úspěšnému snížení procenta softwarového pirátství.

První sférou jsou *represivní složky*. Sem spadá uplatňování autorského práva ze strany tvůrců software ve spolupráci s policií, státními zastupitelstvími a soudy. Tato první oblast

souvisí i s druhou, kam směřovalo rovněž nemalé úsilí, a tou je *výchova*. Je třeba osvětově působit tak, aby lidé pochopili, že kopírovat software je protiprávní, že protiprávní je i rozšiřování takto vytvořeného software a, že zde existuje reálné hledisko, že budou přistiženi a také potrestáni ti, kteří tuto činnost provozují. Třetí sférou působnosti BSA byla *legislativa,* tedy činnost veřejná, překračující v jistém smyslu rámec původního poslání. Tvůrci software pro své působení potřebují nekompromisní zákony. V České republice je tato oblast upravována autorským zákonem č.35/65 ve znění novely č.89/90 Sb., viz [249]. Zaměřením na tyto tři oblasti jako celek lze dosáhnout značných úspěchů, jak o tom svědčí výsledky BSA ve světě. Na území Evropy začala BSA působit v roce 1989 ve třech státech, v Itálii, Španělsku a ve Francii. Svou působnost neustále rozšiřuje.

Vedle *Obchodní softwarové aliance BSA* se sídlem v Londýně, jmenujme ještě další světovou organizaci *WIPO, World Intellectual Property Organization* - Světová organizace pro duševní vlastnictví, u nás pak Agentura pro ochranu software.

K úloze BSA autor [110] uvádí, že tato organizace kromě preventivní činnosti, kdy už sama existence takové aliance by měla uživatele software odradit od jeho nelegálních aktivit, se zabývá také praktickými činnostmi. Jsou jimi

-osvětová činnost, odborná konzultační činnost a ochrana zájmů výrobců software,

-vydávání odborných stanovisek na vyžádání k jednotlivým případům nelegálního užívání software,

-realizace auditu u firem, zda je na jejich počítačích užíván legální software,

-podávání občansko-právních žalob pro porušování autorských práv, eventuálně trestních oznámení v případě zjištění nelegálního rozšiřování softwaru.

Nezanedbatelnou stránkou činnosti BSA je také spolupráce s policejními orgány při odhalování softwarového pirátství a poskytování pomoci při jeho dokumentaci. Tento okruh činnosti BSA je z hlediska policejní práce stěžejní a nejvýznamnější.

Podle autorů [98], BSA definuje též *globální problém* krádeží software a prostřednictvím úzké spolupráce se softwarovými společnostmi v zemích celého světa upřesňuje implementace lokálních programů pro každé tržní prostředí zvláště. Přímou komunikací s vládními úřady se BSA snaží o dosažení užší vazby, aby se prosadila ochrana autorských práv k software ve všech zemích. S tím ovšem kontrastuje současná kritika týkající se některých postojů a aktivit této organizace, údajně neslučitelných s jistými morálními i právními aspekty. Pozorovatel zvenčí může jen velmi těžko posoudit tyto výhrady, zda nepramení např. z určité firemní rivality nebo zda se neozývá pouze oprávněně potrefený subjekt.

Mezinárodní provázanost mají též jiné firmy, které vznikly i bez zahraniční kapitálové účasti, jako např. *APP Group, a.s.,* transformovaná z původní firmy *APP Systems.* APP Group, a.s. se zabývala především systémovou integrací se širokým repertoárem špičkových technologií a programových prostředků, včetně databázového systému *Oracle.* Jako jedna z prvních firem přijala nabídku na spolupráci v oblasti boje s počítačovou kriminalitou, i pokud jde o realizaci preventivních akcí.

**

Představy o koncepci specializovaného pracoviště pro potírání počítačové kriminality. Jak uvádějí autoři studie [88], rostoucí využívání výpočetní techniky ve všech oblastech lidských aktivit vytváří předpoklady pro páchání nové, specifické trestné činnosti, při které výpočetní technika představuje jak její předmět, tak i prostředek použitý k páchání této činnosti. Problematika počítačové kriminality se stává jedním z nejvážnějších úkolů, před jehož řešením stojí nejen Policie ČR, ale i další orgány činné v trestním řízení a jiné státní instituce. Je zřejmé, že při používání výpočetní techniky se bude prolínat problematika počítačové kriminality především s problematikou hospodářské trestné činnosti. Dosavadní praxe ale ukazuje, že počítačová kriminalita má úzkou návaznost i na násilnou a majetkovou trestnou činnost. Momentální naprostá nepřipravenost policie čelit této narůstající hrozbě vedla *Kriminalistický ústav Praha* ke zřízení pracoviště orientovaného především na problematiku technického zkoumání prostředků výpočetní techniky a provádění kriminalistických expertíz v nově koncipovaném odvětví znalecké činnosti - v *počítačové expertíze*. Kromě toho však je nutno postupně vytvářet další specializovaná pracoviště, příp. týmy specialistů i v ostatních policejních službách (v kriminální službě, v útvarech vyšetřování) obdobně, jak je tomu v počítačově vyspělejších zemích. Rozsah a složitost problematiky týkající, se trestné činnosti páchané s pomocí výpočetní techniky nebo přímo na ní vyžaduje, aby se touto problematikou zabývali specialisté - kriminologové, právníci, kriminalisté, technici, programátoři, psychologové a další. S problematikou se váže celá řada problémů jednak autorskoprávního charakteru (plagiáty, softwarové pirátství apod.) a jednak trestněprávního charakteru. Techničtí specialisté budou muset obsáhnout v základních rysech velmi široké spektrum technických a programových znalostí a dovedností v závislosti na okamžitém stavu nejpoužívanějších typů počítačů a programového vybavení. Rozvoj a osvojení potřebných znalostí vyžaduje, aby vedle technického vybavení bylo pracoviště průběžně dotováno i novinkami programovými. Růst odborníků specializovaných pracovišť musí korespondovat s vývojem výpočetní techniky; měl by být zabezpečován minimálně

-zajišťováním stáží na různých dalších specializovaných pracovištích policejních, armádních i civilních,

-v kursech u specializovaných školicích firem,

-zajištěním přísunu odborné literatury, nejen tuzemské, ale i zahraniční,

-dodávkami nejnovější výpočetní a periferní techniky, včetně mobilních počítačů s moderním software a jeho posledními aktualizacemi.

Pracoviště by v cílovém stavu mělo být schopno posuzovat a následně i vydávat osvědčení o úrovni nových technických a programových produktů chránících výpočetní techniku a její data. Z toho důvodu musí být proto pravidelně navazován kontakt s nejrůznějšími firmami a ochrannými autorskými organizacemi, které se touto problematikou zabývají. Složitost problémů s rozvojem počítačových sítí i mezinárodní charakter páchání počítačové trestné činnosti vyžaduje i přebírání zahraničních zkušeností a spolupráci se zahraničními odbornými pracovišti.

Bezprostřední náplní specializovaného pracoviště pro potírání počítačové kriminality by měla být

-*praktická činnost,* spočívající

-v dožádání pracovníků orgánů činných v trestním řízení možnosti zúčastňovat se formou konsultativní účasti při kriminalisticko-policejních úkonech, tj. zejména v možnostech posuzovat získané prvotní informace a signály, zda se v konkrétním případě může jednat o trestnou činnost spojenou s výpočetní technikou, případně v možnostech specifikovat předpokládanou formu trestné činnosti,

-ve spolupráci na stanovení dalšího postupu odhalování a dokumentování konkrétních případů,

-v realizaci činnosti expertizního pracoviště v daném oboru se zaměřením na počítačovou expertízu a kybernetiku,

-ve vytvoření databanky počítačových odborníků, resp. institucí a firem, ochotných spolupracovat formou konsultací při expertizní činnosti pracoviště;

-*preventivní činnost* týkající se

-vymezení hlavních úkolů v problematice postihu počítačové kriminality,

-poskytování konsultací a spoluúčasti na odborné přípravě specialistů, vyšetřovatelů, příp. dalších odborníků formou lektorské činnosti v resortních školách, kursech a seminářích;

-*činnost týkající se rozvoje teorie,* zejména

-účast na vymezení pojmu „počítačová kriminalita“ co do formy i obsahu,

-analýza známých a vytváření nových metod a postupů odhalovaní a vyšetřování případů počítačové kriminality,

-shromažďování informací o vývoji počítačové kriminality u nás i v zahraničí a vyvozování závěrů pro kriminalistickou a expertizní praxi,

-průběžné typování převažujícího trendu působení počítačové kriminality,

-předběžné odhadování hlavní orientace boje s počítačovou kriminalitou;

-*realizace profylaxe*, zejména

-kontroly úrovně zabezpečovacích technik a opatření poskytovaných specializovanými firmami,

-ověřování úrovně existujících a provozovaných bezpečnostních prostředků a technik;

-*koncentrace na aktivity v oblasti „informační bezpečnosti“*, jako např. účast

-na konstituování základních směrů vytvářené „informační bezpečnosti“, tj. jasném a pregnantním definování cílů, kterých je nutno postupně dosáhnout,

-na definování kritérií pro různé úrovně zabezpečení počítačově zpracovávaných informací, tj. definování úrovně „citlivosti informací“ a stanovení uceleného souboru bezpečnostních opatření, tzv. „bezpečnostních standardů“,

-na předkládání zásad právních norem týkajících se počítačového zpracování informací a postihujících zejména

-neoprávněné přístupy k informacím a neoprávněné manipulace s nimi,

-ochranu vlastních soukromých informací každého jednotlivce,

-stimulaci zavádění účinných bezpečnostních prostředků (např. formou odpisů z daní, pojištěním dat, pojistných bonusů při používání ověřených bezpečnostních prostředků apod.),

-na vypracovávání pokynů, návodů a metodik ochran před počítačovou kriminalitou

-sebeochranou provozovatele,

-trestněprávní prevencí,

-softwarově-hardwarovou prevencí,

-na určování základních principů a postupů budování, používání, zdokonalování a kontrolování účinnosti bezpečnostních opatření,

-na vypracovávání metod hodnocení účinnosti používaných bezpečnostních opatření,

-na zpracování zásad vytváření týmů analýzy rizik, řešení krizových situací a týmů kontrolních,

-na definování metod a způsobů protivirové prevence a virové detekce,

-na kontrolách zabezpečení proti působení počítačové kriminality v organizacích spadajících do sfér státního zájmu.

Autoři sdělení [88] se bohužel nezmiňují o nutnosti kontroly toků i statického presentování informací ve veřejných počítačových sítích, jako je např. Internet. Do náplně činnosti specializovaného pracoviště popsaného typu by jistě příslušelo též např. na Internetu systematické vyhledávání šiřitelů dětské pornografie, propagátorů rasového násilí, případně dalších projevů xenofobie, ale i nekalé reklamy a jiných protizákonných aktivit.

Podmínky nutné ke splnění uvedených cílů spočívají v přiměřené vybavenosti pracoviště

-odpovídající technikou, včetně její aktualizace, inovace a doplňování náhradních dílů,

-schopným personálním substrátem,

-nákupem odborné literatury,

-možnostmi průběžného získávání poznatků o nových technologiích.

Podle zaměření autorů [88] se uvedené představy týkaly původně koncepce policejního pracoviště, avšak některé z nich jsou přijatelné i pro jiné organizace se zaměřením na prevenci či jiné způsoby boje s počítačovou kriminalitou.

8.5. Mezinárodní aspekty boje s počítačovou kriminalitou

Z hlediska nadnárodních přístupů k boji s kriminalitou zaujímají Spojené státy americké iniciativní pozice. Podle amerického ministerstva spravedlnosti otevírají počítače a mezinárodní počítačové sítě nové cesty zločincům, kteří se nenechají zastavit státními hranicemi. Pro USA to znamená, že i v této oblasti nutno podat iniciativní podněty mezinárodní spolupráci. Státní a vládní představitelé sedmi nejvýznačnějších průmyslových států a Ruska (G8) potvrdili nutnost jednat o této záležitosti již na summitu v červnu 1997

v Denveru. Nyní ministři vnitra a spravedlnosti dotyčných osmi států podepsali ve Washingtonu desetibodový program, který by měl především zabránit náskoku zločinců v používání nejmodernější techniky, včetně počítačové.

„Růst dětské pornografie na Internetu pobouřil celý svět“, zdůraznila kanadská ministryně spravedlnosti. Další problémy souvisí s krádežemi nebo ničením informací v databázích a s nelegálními peněžními transakcemi. Nové problémy vznikají podle poznatků americké protidrogové instituce *DEA* v souvislosti s tím, že obchody s drogami jsou stále častěji dojednávány prostřednictvím Internetu. Státní tajemník německého spolkového ministerstva vnitra řekl: „...nesmíme posuzovat zločiny páchané pomocí moderní techniky izolovaně, ale jako zvláště nebezpečnou součást veškerého dění v oblasti organizovaného zločinu...“.

Ve Washingtonu podepsaný desetibodový program počítá především s potíráním počítačové kriminality. Musí se urychlit výměna dat a kompetentní partneři musí být dosažitelní po celých 24 hodin denně. Elektronické informace mají být předávány ve formě využitelné při trestním stíhání. Odborníci z uvedených osmi států chtějí dosáhnout toho, aby v jejich právních systémech bylo zneužití systémů pro přenos dat stíháno ve srovnatelné míře. Současně má být zajištěno vydávání domnělých pachatelů pro účely soudního jednání do země, v níž byl čin spáchán.

Tento rozsáhlý program má však především charakter výzvy. Podle státního tajemníka německého spolkového ministerstva spravedlnosti představuje dohoda podklad pro možné následné dotazy vlád jednotlivých států k tomu, co již bylo ve smyslu tohoto programu vykonáno.

**

Počítačová kriminalita nebezpečných forem v současné době překračuje rámec jednotlivých zemí a souvisí v nadnárodních měřítcích zpravidla s organizovaným zločinem. Klasickým příkladem toho je případ softwarového pirátství podle zprávy [21], která informuje o konkrétním pašování velké zásilky nelegálních kopií software do SRN a o ekonomických ztrátách souvisejících s těmito aktivitami, jež v poslední době získávají zcela nové rozměry. Na současnou situaci reaguje zvýšenou aktivitou policie ve spolupráci s odborníky firem vyrábějících software. Jako příklad relativně nové metody distribuce nelegálního software je uvedena Internetová síť.

Celníci z Kolína nad Rýnem ve spolupráci s pracovníky německé filiálky americké firmy Microsoft sledovali muže z Texasu, který se pokoušel importovat do Německa přes Velkou Británii a Nizozemsko velké množství nelegálních kopií programového vybavení výpočetní techniky firmy Microsoft. V blízkosti Cách objevili v nákladním voze 38-letého Američana dosud největší množství nelegálních softwarových kopií, které kdy byly v Evropě zabaveny v rámci jednoho případu. V desítkách beden bylo ukryto 300 000 CD-disků, 400 000 příruček, registračních karet, nálepek na diskety a certifikátů potvrzujících pravost. Hodnota zabavených softwarových padělků byla vyčíslena na 105 mil. DEM. Nejen pro softwarového giganta Microsoft, ale pro celé výrobní odvětví se programové pirátství stalo

vážným problémem. Každou vteřinu uniká výrobcům software v důsledku používání nelegálních kopií jejich produktů přibližně 500 USD. Tento výpočet pochází od Business Software Allianz (BSA), celosvětového zájmového sdružení na ochranu před pirátskými kopiemi, jehož hlavní sídlo se nachází v Mnichově. Jen v Německu dosahovaly škody v roce 1997 v souvislosti s touto nelegální činností 891 mil. DEM. Uvedený případ transakce s pirátskými kopiemi však svědčí o zcela novém rozměru softwarových deliktů. Pokud se v minulých letech v této nelegální činnosti angažovali převážně jednotlivci, nyní se tímto lukrativním obchodem s disketami a CD-disky zabývají mezinárodně operující bandy, které doposud pašovaly převážně drogy a zbraně. Většinu nelegálních produktů vyrábějí piráti v zahraničních firmách nebo dokonce ve vlastních podnicích. Tím se stává pro zákazníky i vyšetřovatele stále obtížnější rozlišit originální zboží od padělků. Rovněž zatčený Američan není podle poznatků kolínských celníků izolovaným pachatelem, a proto se intenzivně pátrá po jeho šesti komplicích. Tento muž byl předmětem zájmu vyšetřovatelů již dva a půl roku a pravděpodobně vlastní ve Velké Británii výrobnu CD-disků a tiskárnu, kde jsou zřejmě ilegálně kopírovány programy, tištěny příslušné příručky a padělány etikety Microsoftu. Z Velké Británie také pocházela zajištěná zásilka, která se skládala z 36 palet se softwarovým vybavením, které bylo údajně vyrobeno na zakázku pro německý Microsoft GmbH. a mělo být dodáno přímo do Německa. Na základě upozornění firemní vyšetřovací skupiny zpřísnili celníci hraniční kontroly. Při prohlídce nákladního auta byl nalezen nejen nelegální software, ale také podezřelé doklady, ve kterých byl odkaz na další sklad poblíž Cách, kde celníci zajistili další kopie.

Nejen gangsteři pracují stále profesionálněji, ale také vyšetřovatelé zdokonalují svou činnost. Stále častěji se policisté spojují s výrobci software do pracovních skupin pro boj proti pirátství. Německá filiálka Microsoftu pomáhá policii při rozlišování originálního software od padělků. Odborníci firmy Microsoft realizovali v roce 1998 v SRN šest školení pro celkem 300 pracovníků policie. Týmová práce policie a výrobců software se osvědčuje. Před několika týdny se policii v Meklenbursku - Pomořansku podařilo ve spolupráci s pracovníky firmy Microsoft po několikaměsíčním vyšetřování zajistit 2400 nelegálních kopií software v hodnotě 3,36 mil.DEM. „Tyto úspěchy ukazují, že spolupráce mezi policií a průmyslem funguje," tvrdí přední odbornice firmy Microsoft pro záležitosti pirátského kopírování. „Mnoho případů vyšetřování však dosud ztroskotává na nedostatečném vybavení policie nebo malém pochopení soudů pro hospodářské škody způsobené softwarovými piráty," konstatuje mluvčí BSA a obchodní vedoucí softwarové firmy *Adobe Systems*. Výrobci software se potýkají ještě s dalším problémem. Většina firem si sice koupí originální software, který je však opakovaně kopírován pro větší počet zaměstnanců. S cílem omezit toto zneužívání programů se BSA v Německu začátkem roku 1997 rozhodla použít ofenzívní postup. Zaslala doporučeně jak německým velkým podnikům, tak i malým firmám formulář k „inventarizaci software", ve kterém byly firmy vyzvány k dodatečnému vyžádání licencí pro nelegálně užívané kopie. Mluvčí organizace BSA označil akci za úspěšnou a v jejím důsledku podíl pirátských kopií v Německu prý poklesl z 36% v roce 1996 na 33% v roce 1997. To však zároveň znamená, že stále ještě každá třetí kopie, kterou německé firmy používají, je nelegální.

Následky uvedeného stavu pro trh práce jsou velmi negativní. Podle studie poradenské firmy *Price Waterhouse* došlo v důsledku škod způsobených softwarovým pirátstvím v Německu jen v roce 1996 ke ztrátě více než 25000 pracovních míst. Také v dalších státech vzrůstá obchod s pirátskými kopiemi. Největší podíl na nelegálním software vykazuje v Evropě Bulharsko s 93%, Rusko s 89%, Řecko s 73%, Irsko s 65% a Španělsko s 59%. V Číně dosahuje tento poměr dokonce kolem 96% (pro srovnání v Japonsku 32%). Nejlepší výsledky dosahují USA, kde se podařilo snížit podíl pirátských kopií v roce 1997 na 27%. Lze předpokládat, že úspěchy německé policie v minulých létech alespoň částečně odradí potenciální pachatele od obchodování s ukradeným software. Pokud by se podařilo do roku 2000 snížit podíl pirátských kopií v Německu pod 30%, byl by to poměrně slušný úspěch. Také Internet se stal v posledních letech podle tvrzení BSA velmi využívaným výrobci pirátských kopií. Pokud v roce 1995 bylo možno pod internetovým heslem pro nelegální software „warez" nalézt přibližně 10000 dokumentů, v květnu 1998 se jejich počet zvýšil na 285000. V červnu 1998 identifikovali internetoví vyšetřovatelé BSA v Evropě celkem 50000 webových stránek s nelegálním software, z toho téměř 18000 v Německu. Způsoby činnosti softwarových pirátů jsou mnohostranné. Sahají od bezplatných nabídek přes e-mail až po časově limitovaný nebo ve své funkčnosti omezený uživatelský software. Vedle těchto bezplatných nabídek existuje stále více internetových zločinců, kteří se na nelegálním software obohacují a kteří prostřednictvím speciálních on-line aukcí a on-line katalogů nabízejí široké spektrum služeb. Platby pak následují většinou prostřednictvím kreditních karet. BSA odhaduje, že škody vyplývající ze softwarového pirátství s využitím Internetu dosahují v Německu 1,6 miliard DEM ročně a tak značně převyšují částku 891 mil. DEM, kterou jsou vyčísleny škody způsobené tradičním nelegálním kopírováním.

Škoda, že tak podrobný rozbor situace a následných opatření, jaký byl vypracován v SRN zatím u nás nemáme. Lze však předpokládat, že ani Česká republika se nevyhne problémům s organizovaným zločinem podobného charakteru.

**

Počítačová kriminalita ohrožuje národní bezpečnost. S počítačovou kriminalitou jsou spojena i některá další závažná rizika. Jedním z nich je tzv. *počítačový terorismus*. Tomuto tématu byla věnována v minulosti téměř současně probíhající významná jednání expertů v Moskvě a ve Washingtonu. Vzhledem k tomu, že názory na možné řešení situace mají nadnárodní charakter, je možno uvedené poznatky využít i v práci orgánů činných v trestním řízení České republiky. Účastníci všeruské porady nazvané *„Problémy boje s počítačovou kriminalitou"*, kterou uspořádala v roce 1996 v Moskvě *Rada bezpečnosti Ruské federace,* v přijatém usnesení zdůraznili, že současná etapa informatizace všech sfér života ruské společnosti je charakterizována zvyšováním počtu případů porušení zákonů, při kterých pachatelé využívají jako nástroj technické prostředky informatiky.

Situace v Ruské federaci. Představitel Rady bezpečnosti Ruské federace v průběhu jednání prohlásil, že všechna dosud přijatá opatření, včetně svolání této porady, se opozdila o několik let. Podle analýz amerických specialistů představuje průměrná výše škody každého

trestného činu v této oblasti přibližně 450 000 USD, přičemž roční ztráty všech amerických společností dosahují přibližně 5 miliard USD. Finanční ztráty jsou však jen jednou stránkou problému. Stejně velkým rizikem je zmíněný *počítačový terorismus*, který může vést ke katastrofickým důsledkům v činnosti řídících a průmyslových systémů. V současnosti je podle pracovníka aparátu Rady bezpečnosti Ruské federace nejzávažnějším problémem prokazování této trestné činnosti. Podle amerických statistik je odhaleno asi 5 % počítačových trestných činů a z nich jen 20 % je dotaženo do stadia soudního procesu. Představitel Federální služby bezpečnosti ve svém vystoupení uvedl, že pracovníci FSB a ministerstva vnitra Ruské federace mají zatím velmi nedostatečné zkušenosti s počítačovou kriminalitou, neboť se dosud setkávali s tímto typem trestné činnosti pouze ve finanční sféře. Podobné zločinecké aktivity však mohou vést až ke globálním katastrofám, ekologickým, dopravním a jiným kolapsům. Po zobecnění všech faktů lze současnou úroveň organizace boje s počítačovou kriminalitou v Rusku charakterizovat jako kritickou. Toto konstatování plně sdílejí i specialisté MV a FSB, kteří se zúčastnili vypracování projektu Federálního programu odhalování počítačové kriminality, který má vytvořit nezbytné podmínky pro organizování boje s trestnou činností ve sféře výpočetní techniky. Účastníci porady současně apelovali na ruskou vládu, aby uvedený program urychleně zařadila do registru federálních programů a vyčlenila nezbytné finanční prostředky na jeho realizaci. Podle názorů odborníků je pro zlepšení situace v rámci orgánů činných v trestním řízení na federální a regionální úrovni nezbytné vytvořit organizační struktury schopné vést efektivní boj s počítačovou kriminalitou. Dále je nutné vytvořit systém vzdělání specialistů a zahájit realizaci komplexu vědecko-výzkumných a experimentálně-konstrukčních prací s cílem zabezpečit ruské orgány činné v trestním řízení nezbytným metodickým a vědecko-technickým vybavením pro odhalování, vyšetřování a expertizy takových trestných činů. Dále je nutné organizovat spolupráci ruských institucí a specialistů na mezinárodní úrovni v oblasti boje s počítačovou kriminalitou. Program konkrétně předpokládá

-vytvoření vzájemně propojeného systému opatření právního a administrativního charakteru, určeného pro boj s tímto druhem zločinnosti,

-organizaci spolupráce státních a soukromých struktur,

-praktická opatření k zajištění bezpečnosti a ochrany informací zpracovávaných v elektronické formě,

-informování obyvatelstva, i prostřednictvím hromadných informačních prostředků, o možných důsledcích počítačové kriminality,

-ochranu zájmů a stanovení práv osob, společenských organizací, zařízení a podniků, které se stanou oběťmi počítačové kriminality,

-rozšíření mezinárodní spolupráce a kooperace v boji s počítačovou kriminalitou.

V rámci programu se připraví *Výnos prezidenta Ruské federace „O opatřeních při organizování boje s počítačovou kriminalitou“* a dále má být vytvořena meziresortní koordinační rada pro boj s počítačovou kriminalitou. Rovněž se má komplexně prověřit účinnost ochrany informací v počítačích a informačně-telekomunikačních systémech orgánů činných v trestním řízení, pokud obsahují informace představující předmět služebního,

státního nebo obchodního tajemství či informace o občanech. Navíc se předpokládá vypracování návrhu dohody o základních principech spolupráce států SNS v boji s počítačovou kriminalitou.

**

Svět ohrožují počítačoví piráti. Americkým hackerům, jak jsou někdy nazýváni počítačoví piráti, se jenom za loňský rok podařilo ve 162 500 případech proniknout do počítačové sítě Pentagonu, přičemž dalších asi 90 000 pokusů bylo neúspěšných. Schopnost „útoku“ na počítače Pentagonu však má nebo ji vyvíjí 120 cizích zemí, uvádí zpráva Pentagonu citovaná v pramenu [3]. V extrémním případě se nedá vyloučit, že kontroly informační sítě americké obrany se zmocní teroristé nebo jiní nepřátelé a vážně ohrozí možnost řízení vojenských jednotek. V této souvislosti lze připomenout případ z roku 1994, kdy se dvěma hackerům podařilo proniknout do počítačů výzkumného střediska velitelství vojenského letectva ve městě Rome ve státě New York, ovládnout kontrolu celé sítě a vyřadit ji na několik dnů z provozu. Jeden z nich, 16-letý britský chlapec, byl odhalen, ale druhého se nikdy zjistit nepodařilo. Jak uvádí zpráva [3], počínání tohoto typu může ohrozit celosvětovou bezpečnost.

Softwarové pirátství je rovněž neobyčejně složitý problém. Podle studie [98], i v USA, kde dnes existují tvrdé postihy ze strany policejních orgánů, není zhruba 30 % používaných programů legálního původu. Je třeba říci, že míra softwarového pirátství v USA, což je počet nelegálních kopií používaných na území USA, byla dříve mnohem vyšší. Po letech mohutné kampaně ze stran softwarového průmyslu, tvrdé spolupráce průmyslu a policejních složek a po celé řadě výchovných kampaní bylo dosaženo úspěchu v podobě snižující se uvedené míry.

V zemích ES jako celku je situace o něco horší. Podle [98] pouze čtyři počítačové programy z deseti jsou zakoupeny legálně. Zde však ve srovnání s USA trvá spolupráce mezi průmyslem a policejními složkami kratší dobu. V zemích střední Evropy - v České republice, Slovensku, Polsku a v Maďarsku je situace ještě horší. Převážná část výrobků je stále ještě nelegálně kopírována a návratnost vložených prostředků je pro softwarové společnosti velmi malá. Nárůst nezaměstnanosti v této části Evropy je sice poměrně nízký, ale situaci lze hodnotit jako nejistou. Za „dobrou zprávu“ snad lze považovat fakt, že byl nalezen hned na počátku spolupráce v boji proti softwarovému pirátství společný zájem mnoha institucí na poli respektování práv intelektuálního bohatství.

Všichni výrobci softwaru, včetně firmy *Microsoft*, jsou nuceni čelit padělání software. Existují důkazy o tom, že asijská a italská mafie pracují na padělání výrobků této a samozřejmě i jiných firem, podrobněji k tomu viz opět studii [98]. Pomocí vyšetřovatelů, najatých na Thaiwanu, v Hong-Kongu a v Číně, bylo zjištěno, že více než 20 společností se v těchto zemích - a navíc i na jedné univerzitě v Číně - zabývalo padělaním výrobků Microsoft. Na trh byly uváděny v pěti různých jazycích. Rovněž byly vyráběny nelegální padělky hologramů, používaných na obalech produktů. Těchto hologramů bylo objednáno u specializovaných výrobců asi kolem 3 milionů. Z tohoto příkladu je patrné, o jak závažnou

trestnou činnost šlo. Kdyby byla tato pirátská akce úspěšně dokonána, vznikly by firmě Microsoft ztráty ve výši stovek milionů dolarů. Určit rozdíl mezi originálním hologramem a padělkem z Číny je nesmírně těžké. Padělek byl zjištěn i ve střední Evropě, v Polsku, Maďarsku, Německu, i v České republice. Je zajímavé sledovat cesty padělků z Dálného Východu do Evropy. Před časem byl odhalen padělek putující z Thaiwanu do Austrálie, dále do skladu v Budapešti a odtud byl rozesílán na místa určení ve střední a východní Evropě. Jiný se dostal do zemí Evropského společenství přes Rotterdam a dále pak do střední Evropy. Další padělek cestoval z USA přímo do České republiky. Tím lze doložit, že jde skutečně o velmi závažný problém celosvětového charakteru.

Italská mafie v čele pirátů. Podle [98], na základě dalších důkazů bylo zjištěno, že největším producentem nelegálního počítačového softwaru v Itálii je italská mafie. Stručně řečeno, mafie vyrábí software, který konkuruje nejen Microsoftu, ale i dalším legitimním softwarovým výrobcům. Zde přicházíme do bezprostředního styku s hlavními organizacemi mezinárodního zločinu. Všechny druhy nelegálních softwarových výrobků jsou přichystány též k distribuci nejen na náš trh, ale i do ostatních zemí Evropy. V boji s tímto fenoménem nutno navazovat spolupráci s vládami jednotlivých zemí, s místními agenturami, státními zástupci, prokurátory a s policií. Je třeba objasnit, o jaké výrobky jde, odkud asi pocházejí, a to vše s cílem zastavit tuto produkci, zabavit a zničit nelegální kopie a cestou práva uvalit trest na pachatele.

**

USA se obávají kybernetické války. Jedním z témat jednání senátního podvýboru pro vládní záležitosti USA je nebezpečí *elektronického terorismu* pro svět a speciálně pak pro USA. Jednání se účastní i ředitel CIA, který údajně uvedl, že CIA má spolehlivé informace o tom, že některé státy vyvíjejí doktríny, strategie a prostředky pro realizace útoků v informační oblasti. Mezinárodní teroristické skupiny jsou již dnes schopny negativně působit na informační infrastrukturu USA s použitím poměrně jednoduchých metod. Kybernetická válka se pravděpodobně stane v 21.století jedním z hlavních ohrožení národní bezpečnosti USA, a jistě i dalších zemí, hned po nebezpečí použití jaderných, chemických a biologických zbraní. Podle hodnocení kontrolně-finančního útvaru amerického Kongresu nejméně 120 států světa uskutečňuje v současnosti výzkum možností speciálního programově-matematického působení na informační systémy potencionálního protivníka. Podle názorů amerických expertů, kteří vystoupili před senátním podvýborem, potencionální agresoři již dnes disponují moderní technologií nezbytnou pro vyvolání katastrofických událostí. Dosud však nemají v dostatečné míře ujasněné poznatky o svých cílech či obětech a nejsou schopni získat přímý přístup k počítačovým sítím, které by chtěli paralyzovat. Lze tedy konstatovat, že zbraně pro útok již existují, ale naštěstí zatím není možno cíl vybrat a touto zbraní zasáhnout. Již v minulosti došlo k pokusům o proniknutí do počítačového systému ministerstva obrany USA, počítačových sítí atomových elektráren, středisek kontroly letového provozu, počítačových systémů mezinárodního platebního styku a do dalších oblastí, které představují strategický zájem USA. Nebezpečnost takových pokusů se zvyšuje úměrně se zvyšováním míry závislosti jak vojenských, tak i civilních organizací na stále složitějších počítačových

systémech. Pro zabezpečení nadnárodní ochrany informační strategické infrastruktury lze považovat návrh USA na vytvoření speciálního centra pro vedení kybernetické války. Centrum by mělo vzniknout v rámci *Agentury národní bezpečnosti ozbrojených sil USA*, která v americkém rozvědném společenství plní úkoly v oblasti elektronického získávání informací.

**

Firma Microsoft a mezinárodní aspekty odhalování softwarového pirátství. Firma Microsoft byla založena v roce 1975. Již záhy se začala velmi rychle rozvíjet. Jak uvádí autor příspěvku [127], její každoroční obrat se tehdy pohyboval okolo čtyř miliard dolarů s ročním přírůstkem asi 60%. Jde o firmu, která určuje směr vývoje v oblasti průmyslu informačních technologií, ať už jsou to operační systémy či aplikace. Microsoft má po celém světě řadu poboček, má též zastoupení v Praze. Firma Microsoft dosahuje i u nás vynikajících obratů. Celosvětové podíly jejích produktů na trhu v jednotlivých druzích aplikací, jako jsou textové editory, tabulkové procesory, grafika, databáze, software na projektový management a software pro elektronickou poštu, průběžně rostou. Microsoft je i na našem trhu pojmem. Napomáhá k tomu přijatá koncepce, uváděná pod názvem *„Česká kancelář na světové úrovni“*. Smyslem služeb poskytovaných firmou je dodávat na náš trh software přizpůsobený zdejším uživatelům, tj. dodávat tzv. *lokalizované programy.* Týká se to operačních systémů *Windows*, textového editoru *Word*, tabulkového procesoru *Excel*, databází *FoxPro* a *Works* a lokalizace dalších verzí programů. Pro našeho prostého uživatele neznalého angličtiny usnadnila obsluhu i náročných systémů tím, že je přizpůsobila co nejvíce českému prostředí, včetně vhodně zpracovaných manuálů v českém jazyce. Na českém trhu však firma Microsoft nechce pouze prodávat softwarové produkty. Soustřeďuje se i na spektrum služeb, jako jsou hotline, autorizovaná školicí střediska, spolupráce s dealery atd. Lze říci, že v tomto směru má, jako jedna z mála firem, komplexní řešení služeb.

Pomineme-li soudem nařízený negativní postih za monopolizační tendence vůči jiným renomovaným firmám, Microsoft vykazuje i značné ztráty v důsledku softwarového pirátství. Obecně se softwarový pirát vystavuje trestnímu stíhání. Mnozí lidé si však neuvědomují, že například ve firmě nebo v nějaké instituci, pokud zde nemají stanovenu hmotnou odpovědnost zaměstnanců nebo kde tuto odpovědnost nemá na sobě systémový programátor nebo správce sítě, za případné zneužití software odpovídá ředitel firmy nebo instituce. V dnešní době se takový činitel vystavuje trestnímu stíhání a může mu být uložen trest až do výšky 5 let. Pirát samozřejmě nemá nárok na hotline, školení a další doprovodné služby, odcizený produkt získává bez dokumentace, vystavuje se nebezpečí šíření počítačových virů atd. Jak známo, technicky problém spočívá v tom, že desátá kopie software je stejně dobrá jako ta první, což na rozdíl u videozáznamů nebo u magnetofonových kazet neplatí. Softwarové pirátství má neblahé důsledky pro každou postiženou firmu. Pro malou firmu může softwarové pirátství znamenat otázku dalšího bytí či nebytí, velká firma nemůže v důsledku ztrát věnovat finanční zdroje na vývoj dalších verzí programů. Softwarové pirátství má však vážné důsledky i pro stát. Vznikají finanční ztráty v důsledku neodvedených daní. Jak uvádí [127], v České republice představuje tzv. „krabicový“ (paketový) software obrat asi za 30 mil. USD.

Odhaduje se, že u nás lze poměr softwarového pirátství vyjádřit poměrem 1:9, tzn. že na jednu legální kopii softwaru existuje 9 nelegálních instalací. Lze si snadno představit co by to znamenalo pro naši státní pokladnu, kdyby se nám podařilo snížit hladinu softwarového pirátství jenom o 5%. Vlivem nezákonného kopírování softwaru jsou do jisté míry ohrožena pracovní místa v softwarovém průmyslu. U menších firem to může znamenat odliv odborníků k velkým firmám, zpravidla však do zahraničí. Může se ale snadno stát, že softwarové pirátství způsobí, že software se bude prodávat do zahraničí, anebo ti odborníci, kteří ho „píší“, budou do zahraničí odcházet. Jestliže u nás pokvete softwarové pirátství, lze očekávat menší zájem zahraničních firem o investování v naší republice. Zde uvedené údaje jsou z roku 1994, doufejme, že důsledky z nich anticipované nebudou vlivem nových vývojových skutečností tak horké.

Microsoft je členem BSA. Boji se softwarovým pirátstvím věnuje nemalé prostředky, stará se též o prevenci, a to v nadnárodních rozměrech. V obchodní činnosti, v reklamě, v každém rozhovoru pro sdělovací prostředky se zpravidla všichni jeho představitelé zaobírají i problémem softwarového pirátství a metodami jeho potírání. Firma se snaží též prosazovat direktivu ES, která jasně chrání software jako duševní dílo. Domnívá se, že každá země bude jedině tehdy zajímavým působištěm pro zahraniční softwarové instituce, pokud bude v ochraně autorských práv plně respektovat kompatibilitu s touto direktivou. Mezi další aktivity v boji se softwarovými piráty lze počítat i účast právníků firmy Microsoft v BSA. Je nutné zdůraznit, že produkty firmy Microsoft jsou bezkonkurenčně nejvíce šířeny načerno, a to, bohužel, v celosvětovém měřítku. Je to dáno reálným uživatelským rozšířením operačních systémů *MS DOS* a *Windows*. Další často pirátsky kopírované produkty jsou kromě operačních systémů programy *Excel, Word, Works, FoxPro, Access*. Podle [127] lze konstatovat, že firma Microsoft je vlastně ze všech dalších softwarových firem zasažena softwarovým pirátstvím nejvíce. Taková je zkušenost firmy nejen u nás, ale i v nadnárodním pojetí. Mezi projevy nejčastějších druhů softwarového pirátství vůči firmě Microsoft patří různé aktivity, jako

-nedovolené kopírování,

-padělání, s nímž se Microsoft setkává hlavně na dálném východě, přičemž „obětí“ se v největším množství případů stává operační systém MS DOS,

-prodej formou *domácí pošty*, což znamená, že jsou inzerována určitá telefonní čísla, kde se dá software koupit přímo domů za podstatně nižší cenu, než v klasickém kanálu výrobce *distributor - dealer - uživatel.*

Podle zkušeností firmy Microsoft byl rozsah softwarového pirátství v roce 1994 odhadován následovně: USA 30%, Velká Británie 50%, Francie 60%, Švédsko, Finsko 65%, ČR, SR, Polsko, Maďarsko 85 - 90%, Rusko 95 -100%. Autor [127] uvádí, že není bez zajímavosti, že když si v Rusku průměrný uživatel koupí u dealera počítač, dostane k němu seznam všeho možného, co má ten který dealer nakradeno. Zájemce si vybere co chce, a když se mu to vejde na pevný disk, tak mu to dealer nakopíruje, většinou bez jakéhokoliv reálného nebezpečí postihu. V Polsku zase sice parlament přijal autorský zákon, ale jde o vítězství pochybné, protože tentýž zákon uznává tříměsíční neomezenou amnestii. To v praxi znamená, že co si nový majitel počítače za tři měsíce (nelegálně) nakopíruje, to se po této době stává jeho legálním majetkem. Právě proto Microsoft zvažoval zastavení prodeje nových verzí

software do Polska, protože při tamní úpravě jakékoliv jiné preventivní kroky nejsou příliš účinné.

Na první místo „sebeobranného systému“ firmy Microsoft proti softwarovému pirátství lze řadit aktivní preventivní činnost. Firma organizuje nejrůznější semináře, tiskové konference a malé i velké reklamní akce. Software je chráněn též *ochrannými známkami*. Na krabicích jsou různé značky viditelné pouze pod speciálním zářením, jsou tam hologramy, loga aj. ochranné známky. Bohužel, zkušenost však ukazuje, že všechny tyto ochranné prvky jsou napodobitelné. Proto jedině úzká spolupráce firmy Microsoft s policejními orgány různých států pomáhá odhalit případné zločiny. Další obranným prostředkem jsou *omezené instalace*, tedy např., že software má v sobě tři „náboje“. Pomáhají i tzv. *OEM smlouvy*, což v překladu znamená, že to jsou smlouvy na prodej softwaru spolu s něčím dalším, převážně s počítači nebo s jiným hardware. Smlouvy jsou dohodnuty s výrobcem hardware nebo s operátorem, který počítače sestavuje. Takové smlouvy mohou být nejrůznějšího typu. Například k počítači, k tiskárnám, myším nebo k jiným zařízením se dávají jen instalační diskety, ale může se k nim přidávat ještě např. odpovídající verze manuálu. Existují i smlouvy, že software je přímo nakopírován na pevný disk. Protože seznam partnerů, se kterými má Microsoft uzavřen kontrakt, je firmě znám, dá se poměrně snadno zjistit, zda software pochází od této firmy nebo odjinud.

Poznatky firmy Microsoft z odhalených případů softwarového pirátství, podávané podle příspěvku [127], skýtají přehled o situaci pouze v některých státech světa:

Itálie. V Itálii byly zaznamenány nemalé zisky pirátů z padělaných produktů firmy Microsoft. Šlo hlavně o produkty *AmiPro* a *Novell*. V Neapoli byla například objevena továrna, kde pracovalo 100 zaměstnanců a vyrábělo se více než 200 softwarových titulů. Tato firma byla dokonce tak smělá, že o sobě inzerovala, že je největší italskou softwarovou firmou. Byla napojena na sicilskou mafii. Firmě byl dokázán nelegální prodej v hodnotě za 10 mil. USD. Odhady odborníků byly však asi třikrát vyšší. Bylo prokázáno, že firma chystala distribuci svých černých produktů do celé Evropy a je zajímavé, že vstupní branou do východní Evropy mělo být Maďarsko, Česká republika a Slovensko.

Německo. Již v roce 1993 bylo odhaleno pět firem v okolí Stuttgartu, kde bylo zabaveno více než 2500 nelegálních kopií *Windows*. Jednalo se o knižní vydavatele, kteří si tímto způsobem přivydělávali. Byl zabaven velký počet nelegálně vytištěných příruček. Pracovníci firmy Microsoft dostali signál od českého distributora, který obdržel od firmy nabídku. Nabízená cena byla šestkrát nižší než je u nás obvyklé. Bylo mu to divné, a proto případ oznámil policii. Další velký případ byl odhalen v Berlíně. Na území východního Berlína působilo množství nelegálních podnikatelů, kteří distribuovali nelegálně software. Šlo o praktiky, vybízející k výměně kradeného software nejen v Berlíně, ale i v Kolíně nad Rýnem, kde bylo zajištěno 1,8 GB nelegálního softwaru. Tyto praktiky se bohužel začínají uplatňovat už i u nás.

Rakousko. Zde byli odhaleni dva dealeři, kteří kopírovali a prodávali nelegální software. Případ skončil smírem, ale firma Microsoft uplatnila kromě úhrady ušlého zisku a soudních výloh satisfakci spočívající v uveřejnění velké černě orámované omluvy, obsahující

mj. tiskovou informaci ze soudního procesu a zaplacení veškerých nákladů. V praxi to pro dané podnikatele znamenalo likvidaci jejich firem.

Thaiwan. V Asijských státech se softwarovým pirátům daří. Byly zde odhaleny případy, u kterých se dokázal nelegální zisk mezi 50 až 70 mil. USD. Zase se jednalo zejména o operační systémy *MS DOS* a *Windows*. Boss tohoto syndikátu, ačkoliv nikdy předtím nebyl trestně stíhán, byl odsouzen na 18 měsíců nejhoršího žaláře. Pro něho z toho plyne konec podnikání. Dále byla ukončena činnost firmy *Ji-Doh*, která šířila software na CD-discích. Postupně bylo zabaveno 800 kopií nelegálního softwaru od firmy Microsoft, ale i Lotus a Borland. V tomto případě se očekává pro pachatele trest vězení asi do 3 let.

Střední Amerika. Nejenom drogy, ale i softwarové pirátství se stává doménou černého obchodu v zemích Střední a Jižní Ameriky.

V *Mexiku* byla objevena firma *Comysa*, jako jeden z největších softwarových a hardwarových distributorů. Bylo jí dokázáno padělání a prodej softwaru ve velkém. Ředitel a majitel firmy byli vzati do vazby. Součinnost mexické a americké policie byla umožněna podepsáním dohod, které jsou všeobecně známé - smlouvy o volném obchodu *NAFTA*. Pro zajímavost - před přijetím smluv bylo za takový trestný čin možné uložit pachateli pokutu 4 USD, což je na tamní poměry vskutku zanedbatelná částka.

Rovněž v *Kolumbii* a *Peru* byly zaregistrovány první případy softwarového pirátství. Byly objeveny díky americké, kolumbijské a peruánské policii.

**

Informační válečnictví, termín použitý autorem studie [120] pro označení nadnárodní hrozby v oblasti velmi nebezpečné počítačové kriminality. Podle tohoto autora, s příchodem mnohoznačně definované informační společnosti se změní nejen podmínky pro bankovnictví, vzdělávání, obchodování či nakladatelskou činnost, ale také pro armádu a národní bezpečnost. Využití počítačů přináší nesčetné výhody, ale i nová rizika. A to, ve všech oblastech, kam jsou informační technologie zaváděny. Nyní se zaměříme na informační válečnictví, oblast, která je obestřena nezvykle mnoha neurčitými termíny. Jedná se sice o téma zdánlivě nepříliš akutní, avšak rovněž nesmírně závažné.

Obrana každého státu závisí nejen na armádě, ale i na tajných službách. Koneckonců i armáda jako taková má své výzvědné služby. Vždy se pracuje na základě dvou nosných principů, spočívajících v aktivitách

-dosáhnout vlastní informační dominance, tzn. mít správné informace na správném místě ve správný čas,

-zamezit nepřátelské straně v dosažení informační dominance.

V této souvislosti se autor [120] zmiňuje o úspěšné kryptoanalýze německých šifrovacích strojů *Enigma* polskými a britskými kryptografy během druhé světové války, která tak podle některých odhadů byla zkrácena o jeden až dva roky. S příchodem radaru se posunulo získávání informací o nepříteli za hranici dohledu oka. Netrvalo ale dlouho a přišlo se na to, že lze vysílat klamavý zpětný signál „od neexistujících letadel“. Dnes již lze dokonce „nahradit“ např. řídicí signál střely nepřítele signálem vlastním. Moderní války se nevyhrávají

zničením co největšího počtu bojových prostředků nebo vojáků v primární fázi. Na to je dost času ve fázi sekundární. V primární fázi je důležité způsobit zmatek, maximálně eliminovat příjem a hlavně výměnu informací na straně nepřítele a přitom si udržet zdroje informací o činnosti a vybavení nepřítele i schopnost dodat informace včas svým jednotkám.

Moderní konflikty bývají děleny na

-*symetrické,* kdy nepřátelské strany disponují obdobnými technologiemi a podléhají podobným omezením (viz mezinárodní konvence o nepoužívání chemických či biologických zbraní),

-*asymetrické,* kdy strany mají k dispozici rozdílné technologie a podléhají rozdílným omezením.

V obou případech může být kryptografie účinnou zbraní. Podle studie [120] je export šifrovacích produktů v mnoha zemích hodnocen vládními úřady stejně jako export zbraní. Je zřejmé, že silná kryptografie představuje významnou zbraň, totiž schopnost utajit (zašifrovat) nebo naopak dešifrovat komunikaci, což může rozhodnout výsledek konfliktu. Uvádí se, že např. vládě USA se takto daří v oblasti kryptografických a hlavně kryptoanalytických objevů udržovat náskok přibližně 10 až 15 let před ostatním světem. Např. *NSA (National Security Agency)*, má dvě zásadní poslání, získávat vládě USA přístup k informacím komunikovaným mimo území USA a pomáhat v tom, aby nebylo možno získat přístup k informacím vlády USA. *NSA* je snad nejméně známou, ale velmi důležitou tajnou službou USA. Disponuje nejvýkonnějšími počítači, jaké jsou vůbec k dispozici. Má analytické pracovníky snad všude, kde lze získávat nějaké informace důležité pro USA.

Boj přes informační „zákopy“ je zatím ovšem velkou neznámou, stejně jako jeho pravidla. Podle [120] je to asi téma vhodné zatím jen pro fantastické romány, možná však, že jde o reálnou hrozbu umocněnou problémy očekávanými u informačních technologií třetího tisíciletí. V úvahu přichází několik zásadních faktorů, jako

-rozsah „elektronické hranice“, který je i pro armádní komunikace stále více významný v porovnání s rozsahem geografické hranice; činnost mnohých organizací včetně armády, je dnes životně závislá na informačních technologiích a vzájemným propojováním sítí se závislost vztahuje nejen na vlastní prostředky, ale i na prostředky mimo dosah daných organizací;

-vznik uskupení, které se v informačním válečnictví budují a udržují stále obtížněji a často nerespektují existující vojenské a politické koalice; dobře je to vidět na případu USA, které mají dobrou výměnu informací s Kanadou a do značné míry i s Velkou Británií, resp. s Austrálií a s Novým Zélandem; výměna informací s dalšími spojenci z *NATO* je ovšem na daleko nižší úrovni, na což např. Francie, známá rozsáhlými aktivitami nejen ve státní, ale i průmyslové špionáži, reaguje postupným navazováním úzkých vztahů s Německem;

-stabilita státu, která nezávisí jen na dobrém fungování armády a vládních úřadů; vzájemné propojení má v běžném životě mnohé výhody, ale nese s sebou problémy, kterým možná budeme na přelomu tisíciletí čelit; problémy s výpadkem elektřiny a telefonního

spojení si dovedeme představit lehce, zatím jsme je ale nezažili v širokém dopadu po dobu několika dnů či týdnů, nefungovaly by pak banky a burza, nešlo by regulovat přehrady, nebyly by zasílány sociální dávky a deklasované živly by mohly vytáhnout do ulic atp.;

-způsoby vedení útoků - jsou v informační válce velmi levné a tak již útok nemusí být záležitostí jen státní moci nebo omezené teroristické skupiny; stojí za povšimnutí, že i např. *Hizballáh* má (podle informací CIA) odborníky školené na útoky na kritické komunikační prostředky států;

-obtíže při zjišťováním útoků - obtížné je nejen zjištění prvotního útoku, ale i místa, odkud útok pocházel a kdo jej vlastně způsobil, pokud vůbec nešlo jen o chybu systému; mnohdy může jít o koordinovanou ofenzívu mnoha aktérů a desítky či stovky jednotlivých útoků.

Ze zkušeností víme, že žádný počítačový systém není zcela dokonalý. Víme také, že „hrátky s ohněm" začínají často u jednotlivců a malých skupin nadšenců či „bláznů", ale ve velkém rozsahu přestávají být hrátkami. Studie [120] dává k zamyšlení, co by asi nastalo, až se v informačním válečnictví přejde v praxi od špionáže a malých výpadků k frontální ofenzívě.

8.6. Použití počítačů při boji s kriminalitou

Společnost *VISA* natočila speciální videoprogram určený policii, vyšetřovatelům a bezpečnostnímu aparátu bank, který informuje o trendech podvodů s kreditními kartami v různých zemích, viz [221]. Upozorňuje na důležitý zdroj informací pro padělatele kreditních karet - nepotřebné kopie použitých formulářů smluv v půjčovnách aut vyhazované do odpadu. Mnohé autopůjčovny do těchto formulářů zapisují důležité informace o klientech, čehož zneužívají padělatelé kreditních karet. K možnosti čelit této činnosti se doporučuje nejen omezit počet kopií na minimum a nepotřebné formuláře mechanicky skartovat, ale především citlivé informace uchovávat v elektronické podobě v počítači. Tento způsob lze zřejmě považovat za bezpečnější proti zneužití, zejména, když se použije vhodných prostředků ochrany do počítače vložených dat. Tyto prostředky videoprogram rozděluje na prostředky ochrany hardware a software a uvádí v rámci toho konkrétní příklady zabezpečení. Blíže k tomu, viz [221].

Jiným příkladem použití výpočetní techniky v boji s počítačovou kriminalitou je aplikace speciálních pomocných programů vyvinutých např. pro expertizní účely. Např. program *DLOOK*, vyvinutý v Kriminalistickém ústavu v Praze pro specialisty v odvětví kriminalistické počítačové expertízy poskytuje rychlou informaci

-o paměťových nosičích kontrolovaného počítače, jaké soubory, data, či systémy se na nich nacházejí,

-o základních údajích týkajících se pevného disku,

-o celkové situaci v počítači, včetně adresářové struktury ve smyslu praktické pomůcky při psaní znaleckého posudku.

Program pracuje tak, že z velkého množství údajů, které lze zkoumáním paměťových nosičů získat, vybírá pouze ty základní, důležité pro expertízu. Z hlediska technické realizace je unikátním programovým dílem, sdružujícím detailní znalosti souborového systému *FAT* a operačního systému *DOS*. Podrobněji k tomu viz [208].

**

Stát ve věku informací. V současné době lze pozorovat podporu rozvoje informačních technologií i českou vládou. To, že dochází k otevřené diskusi, je velmi pozitivní. Na *Invex Fóru 1998,* které probíhalo pod názvem *„Stát ve věku informací"*, bylo konstatováno, že trh informačních technologií ve střední Evropě a v České republice směřuje k růstu, ačkoliv u nás byla zaznamenána určitá hospodářská a kulturní stagnace až recese. Důležité je, že již zdaleka nevykazuje prioritu pouhý prodej počítačů, ale velmi dynamicky roste prodej software a také oblast služeb s tím související. Vzniká nový fenomén informačního věku. Je jím *internetová televize (ITV).* Spojuje v sobě přednosti televize a Internetu a přináší naprosto nové možnosti, a to i v boji se zločinností, speciálně pak i s kriminalitou počítačovou. Je sice ještě v začátcích, ale během několika let se stane jistě důležitým informačním kanálem. Může ji sledovat každý, kdo je připojen k Internetu, bez ohledu na okolnosti odkud se vysílá a kde se divák nachází. Není nutné budovat složité přenosové cesty, používat desítky vysílačů. A pokud je dnes na internetovou síť připojen zlomek populace, brzy to bude podstatně více. Např. ve Skandinávii je to každý čtvrtý obyvatel. Internet samozřejmě nabízí možnost odezvy a komunikace s divákem, který může do jisté míry zasahovat přímo do živého vysílání. Ale to důležitější spočívá v možnosti provázání s dalším obsahem, který rozvádí obsah vysílaný *ITV*. Internetová televize dovoluje navíc značnou obsahovou profilaci díky tomu, že diváckou obec není nutné nijak „pokrývat" signálem, protože si vysílání mohou spustit odkudkoliv. Není problémem, aby takové vysílání bylo úzce specializovaně zaměřeno výhradně k přání uživatele a přesto, aby mělo miliony diváků. Tento moment je podstatný právě pro boj s kriminalitou. *Divák bude moci operativně v interaktivním režimu spolupracovat s orgány činnými v trestním řízení.* V tomto směru jde ovšem zatím jen o hudbu budoucnosti.

Internetová televize pod názvem *TV24* je prvním počinem na na poli *ITV* ve východní Evropě, viz zprávu ČTK [85]. Vysílala pokusně 24 hodin denně v době výstavy Invex 1998 v ČR. Byla věnována informačním technologiím. Jednalo se o experimentální vysílání, které mělo ověřit některé technické parametry a kapacitní možnosti přenosu. Možnosti, které tento fenomén skýtá v nejbližší budoucnosti lze naladit rovněž na příslušné internetové adrese.

**

Impuls k výchově specialistů na počítačovou kriminalitu. Česká republika historicky patří k těm zemím, ve kterých bylo šíření a používání nelegálně získaného software takřka samozřejmostí. Dnes je již situace poněkud jiná. Sílí konečně snaha o konání v souladu s právem, byť teprve se rodícím a ne zcela komplexním. Pro respektování autorských práv v oblasti tvorby a užívání programového vybavení počítačů byly již i u nás vytvořeny základní podmínky. Jak uvádí autor studie [90], problematika ochrany autorských práv je jedním z nejfrekventovanějších pojmů dávaných do souvislostí s počítačovou kriminalitou. Ačkoliv

protiprávní činnost spojená s výpočetní technikou má mnoho podob, nejčastěji se hovoří pouze o softwarovém pirátství, tedy o nelegálním rozšiřování software a jeho neoprávněném používání. A právě to je jedna z poloh, kterou si jako první problém k řešení z oblasti počítačové kriminality u nás vybrala kriminální policie a začala připravovat k potírání tohoto problému své specialisty.

Výchova počítačových expertů. Využití počítačů v boji s kriminalitou, speciálně též s počítačovou kriminalitou je mimo jiné podmíněno adekvátní výchovou specialistů, viz [209]. Příprava expertů počítačové kriminality patří k tradičním formám metodické činnosti *Kriminalistického ústavu Praha Policie České republiky (KÚP)*. Děje se tak nejčastěji formou odborných seminářů. Jde o metodické akce, které jsou pořádány s cílem utřídění poznatků, které adepti na tento expertizní obor získali v průběhu své praxe, případně stáží na odborných pracovištích policie. V současné době má rozsah zpracovaných počítačových expertíz policejními specialisty vzrůstající tendenci. Podařilo se prosadit racionální názor na konstituování této expertizní odbornosti i u nižších organizačních útvarů policie.V dohledné době noví specialisté zavedou tento druh expertizy na úroveň krajů. V případě potřeby se budou moci kdykoliv obrátit na pracovníky oddělení počítačové kriminality a jejich cestou i na vedení *KÚP* o případnou pomoc při řešení problémů, které mohou nastat. Zavedením expertíz tohoto typu dojde nejen k přiblížení nového druhu zkoumání k místu činu, stejně jako tomu bylo dříve v případě dalších druhů expertíz, ale dojde též ke snížení zátěže pracovníků oddělení počítačové kriminality *KÚP*, kteří se tak budou moci více věnovat novým metodám a výzkumné činnosti. Předpokládá se, že v pořádání obdobných stáží a seminářů bude pokračováno. Ze strany *KÚP* bude snaha zajistit na nich účast dalších odborníků, mimo jiné z oblasti práva, např. soudců, státních zástupců apod., kteří by mohli přiblížit expertům problémy, se kterými se mohou setkat v průběhu trestního řízení. K výchově odborných kádrů patří vzájemná informovanost o práci v terénu i v prostředí laboratorním, tedy v prostředí vědecko-technického charakteru. Se svými odbornými poznatky by se experti měli navzájem pravidelně informovat. K tomu jsou právě zmíněné semináře ideálním prostředím. Zde se účastníci seznamují se všemi základními metodami a postupy při zkoumání výpočetní techniky, které se v současné době v *KÚP* i ve světě realizují. Postupně lze probrat i témata týkající se základních prohlídek zkoumané techniky, metod a postupů při zajišťování dat a použití komerčních programů v expertizní činnosti. Účastníci seminářů musí být také seznámeni s možnostmi a použitím speciálních programů, které byly pro expertizní účely vyvinuty. Velká pozornost má být věnována také základním poznatkům z oblasti počítačových komunikací. Ke znalostem experta patří i schopnost ovládat speciální výbavu, jako je systém pro zpracování disket *DUPLIKÁTOR* a výjezdový kufřík *KRIMEX PC*. Oba produkty byly vyvinuty pro potřeby expertizní práce na úseku kriminalistické počítačové expertizy v rámci řešení úkolů technického rozvoje. V praxi bude nutná úzká spolupráce mezi experty všech zainteresovaných složek policie i *KÚP*. Ukazuje se totiž, že při řešení složitějších případů je vzájemná konzultace mezi experty a *KÚP* nezbytná i z hlediska minimálního personálního pokrytí příslušných aktivit v terénu.

Seminární forma školení expertů je zatím nenahraditelná vzhledem k tomu, že jiná metoda předávání informací a praktických poznatků není právě v tomto oboru fakticky možná.

Rozbor kriminálního zpravodajství jako nástroj boje s počítačovou kriminalitou. Analýza, na jejímž základě lze z různých informací dedukovat logické závěry, má podle autora článku [25] své nezastupitelné místo jako jedna z funkcí kriminálního zpravodajství. V boji proti trestné činnosti, především pak proti organizovanému zločinu, hospodářské kriminalitě, včetně kriminality počítačové, představují ve skutečnosti zpravodajské informace konečný manažerský nástroj. Hlavní cíl takové analýzy lze spatřovat v dosažení co nejpřesnějších a platných inferencí, které se z dostupných informací dají získat. V tomto směru existuje mnoho různých analytických technik. Kritický problém, jemuž čelí analytici, kteří mají velká množství informací o osobách, jejich vztazích či aktivitách, spočívá v tom, že informace jsou buď rozsáhlé, nebo dezorganizované anebo obojí. Aby všechny tyto informace mohly být analytikům užitečné, musí se „pospojovat" nějakým vhodným způsobem - např. pro interpretaci dat popisujících velké množství transakcí mezi různými subjekty, grafickým znázorněním vztahů apod. Ruční metody a techniky jsou však limitovány počtem subjektů a spojení, s kterými ještě lze operovat bez jakýchkoliv problémů. Příprava a vytvoření diagramů spojení a vývojových grafů je velice pracná a zabere mnoho času. Sestavit třeba diagram spojení, který by jasně ilustroval vzájemné vztahy mezi 50 subjekty, bez vzájemně se křížících čar, aniž by to narušilo přehled celého diagramu, je velice obtížné. Při větším počtu pak již prakticky nemožné. Pro kriminální zpravodajskou analýzu se v takových případech využívají různé počítačové programy, jejichž přednostmi je

-větší pole působnosti, kdy mohou být rychle vytvořeny např. diagramy spojení s řádově tisíci subjektů, včetně jejich vzájemných vztahů,

-větší přesnost, jaké nelze při popisu vzájemných vztahů ručně dosáhnout, přičemž spojení mohou být definována v různých typech a hodnotách,

-větší účinnost a flexibilita, kdy opět lze např. sítě spojení a toky nejen rychle vytvořit, ale i snadno je doplňovat a přetvářet,

-větší selektivita, umožňující pomocí počítačového programu při sestavování sítě spojení vybírat a volit rozmanité struktury, úrovně validity a selekci informací.

Dva z takových počítačových programů, určených pro kriminální analýzu, jsou předmětem sdělení [25]. Jsou to programy *ECNA - Enhanced Criminal Network Analysis* a *SOCIO - Sociogram Plotting Software*. Vytváření diagramů spojení a vývojových grafů pomocí těchto programů je velice rychlé. Sítě spojení a toky mohou být realizovány v několika minutách po pořízení datového souboru. Rovněž rychlé a snadné je další doplňování a přetváření sítě. Validní závěry o komplexu dané nekalé činnosti nutno založit na pochopení konfigurace vztahů mezi osobami, organizacemi a v tom zahrnuté kriminální činnosti. Program *ECNA* tedy pomůže jednak shromáždit informace, které přicházejí často v neúplné formě a po částech, jednak vytvoří co nejlepší obraz o celém komplexu kriminálních operací, ze kterých je možno dedukovat další.

Analytickými produkty programu *ECNA* jsou

-datový soubor, který sestává ze všech informací, vložených na základě určitého projektu nebo případu, přičemž je organizován tak, že každé spojení je na zvláštní řádce,

-abecední seznam přímých spojení - datový soubor může být získán ve formátu, při kterém jsou všechny subjekty seřazeny v abecedním pořádku a pro každý subjekt je přiřazen seznam všech přímých spojení, se kterými je subjekt propojen,

-cesta spojení, což je série spojení a subjektů, které kombinují dva vybrané subjekty, přičemž program zajišťuje všechny hlavní cesty spojení, spojující vybraný pár subjektů,

-síť spojení sestávající ze všech nejsilnějších cest spojení plynoucích k danému nebo z vybraného subjektu, program je limitován 1800 spojeními v síti, síť je definována vybraným subjektem včetně druhu spojení a vybranou validitou,

-diagram spojení jako grafické znázornění sítě spojení; v závislosti na podstatě informace a její aplikaci může být vytvořen buď spojnicový diagram nebo jako druh grafu s omezením na 100 kolonek v jednom řádku grafu, nebo 800 znaků v rozšířeném řádku grafu bez dalších úprav.

Druhý popisovaný program *SOCIO* slouží pro znázornění sociogramů, tedy vztahů mezi osobami, zločineckými organizacemi apod. Od programu *ECNA* se v zásadě liší pouze tím, že operuje se všemi spojeními mezi subjekty na stejné úrovni - tzv. pevnými spojeními. Ve výsledném sociogramu jsou jednotlivé osoby znázorněny kruhem nebo oválem, který obsahuje jméno, případně jen číslo, např. při práci s utajovanými skutečnostmi. Existující vztahy jsou znázorněny spojnicemi. Program *SOCIO* umožňuje vstup též libovolných jiných relevantních entit libovolnou řadou znaků, např. telefonních čísel, názvů společností apod. Výsledný diagram pak není již jen sociogramem v klasickém pojetí, ale zůstává platným analytickým nástrojem. Lze předpokládat, že oba programy budou užitečným nástrojem v boji se závažnými formami hospodářské kriminality a organizovaného zločinu, zejména pak vítanou pomůckou v analýze rozsáhlejších počítačových gangů.

**

Možnosti použití dalších, tzv. multivariačních metod. Samozřejmě, že při boji s informační kriminalitou pomocí výpočetní techniky lze využívat i dalších metod, včetně jejich programové podoby. Jde zejména o tzv. multivariační přístupy kriminologické statistiky, použitelné i při výzkumu počítačové kriminality. Multivariační metody nacházejí uplatnění hlavně v případech pořádání velkého množství informací. Umožňují vnášet mezi jinak nepřehledné soubory výchozích dat nebo i výsledků předchozích analýz určité smysluplné relace, které se mohou stát základem vhodného globálního hodnocení nebo dalšího bádání. Některé z multivariačních metod umožňují dokonce odhalovat jisté skryté vztahy, nazývané též latentními strukturami. Aplikace těchto metod vyžaduje zvláštní pozornost ověřování předpokladů jejich použití, spojenou se zvýšenou pracností při výběru, při systematizaci či jiné přípravě dat v rámci informačního zabezpečení. Pojem multivariačního zpracování informací nebývá často chápán zcela jednotně. Podle monografie [136] nebo [138] pod tímto pojmem rozumíme zpravidla smysluplnou simultánní analýzu mnohorozměrných veličin, tj. takových údajů, které lze znázornit mnohosložkovými vektory. Ty si můžeme představit jako určité konečné posloupnosti výchozích dat či kvantifikovaných informací. Termínem *smysluplná simultánní analýza* označujeme takové počínání, které transformuje původní, např. empiricky zjištěná data jako celek na soustavu informací s větší

interpretační hodnotou. Tím rozumíme skutečnost, že výsledek takové analýzy má pro nás větší význam než výchozí data, pokud jde o interpretaci nebo z hlediska další celkové použitelnosti.

Základní multivariační přístupy. K multivariačním postupům zpracování hromadných operacionalizovaných informací již tradičně řadíme *analýzu rozptylu, regresní analýzu, faktorovou analýzu, metody charakteristických vazeb, přístupy klasifikace objektů, metody analýzy gangů* a další. Podrobnější popis uvedených postupů by neúměrně překročil rámec této studie. Zde se proto omezíme pouze na smysl a podmínky jejich použití v tom pořadí, v jakém byly vyjmenovány. Hlubší informaci v tomto směru poskytuje již citovaný pramen [136] nebo [138].

Analýzu rozptylu aplikujeme obecně tehdy, kdy potřebujeme odkrýt (vyjasnit) vliv jednoho, dvou, případně většího, avšak jinak vždy malého počtu nějakých faktorových jevů (příčin), přičemž máme k dispozici množství mnohorozměrných pozorování, tedy operacionalizovaných a kvantifikovaných informací. Potom rozložíme celkovou varianci (tj. rozptyl hodnot) na varianci pod vlivem faktoru, tzv. faktorovou složku, a na varianci reziduální, zbytkovou. Dále pak testujeme statistickou hypotézu o rovnosti těchto složek proti hypotéze, že jsou navzájem různé. Překročí-li testové kriterium svou kritickou hodnotu, činíme závěr, že příslušný faktor má signifikantní vliv (na určité hladině významnosti, což je vlastně riziko mylného závěru). Základní podmínkou použitelnosti tohoto postupu je statistická shodnost dispersí (rozptylů) jednotlivých skupin výchozích dat. Tento předpoklad je nutno předem ověřovat např. pomocí Bartlettova testu. Analýzy rozptylu lze použít při vyjasňování toho, zda použité měřící techniky a instrumenty registrovaly vliv apriorního členění pachatelů dle právní klasifikace (nebo i podle jiných kriminologických aspektů) na změny distribuce zvolených charakteristik. Dále lze analýzy rozptylu užít k ověřování stability výsledků při vhodně navržené redukci výchozího informačního systému. Tím můžeme v některých případech docílit snadnější a zřetelnější extrakce hledaných faktorů. Analýza rozptylu se hodí nejlépe pro vyjasnění vlivu jednoho faktoru. Zvyšováním počtu faktorů roste neúměrně komplikovanost a pracnost metody. Tato námitka do jisté míry padá při rutinním využití počítačů s firemně programovanými postupy statistické analýzy. Pokud potřebujeme analyzovat simultánně vliv většího počtu faktorů, používáme buďto metod regresní analýzy nebo metod analýzy faktorové.

Regresní analýzy využíváme v situacích, kdy známe závisle proměnnou, na níž mají vliv různé nezávisle proměnné (faktorové veličiny, faktory). V kriminologických výzkumech bývá nejčastěji závisle proměnnou kriminalita (její typy) a nezávisle proměnnými různé kriminogenní veličiny. Jiný příklad uplatnění tzv. autoregresních analýz skýtá studium závislosti budoucího vývoje kriminality na vývoji předchozím. Rozhodující uplatnění našla regresní analýza při studiu dynamiky kriminality a v kriminolgické prognostice. Podmínky použitelnosti modelů regresní analýzy v této oblasti byly ověřovány nepřímo prostřednictvím shody vyslovených prognóz kriminality s faktickým vývojem. V tomto směru byly úspěšné zejména lineární modely, vhodné např. pro odhalování základních trendů kriminality. Jiné

příklady uplatnění regresní analýzy v dynamice obecné kriminality viz např. [138]. S uplatněním přístupů regresní analýzy v souvislosti s konkrétní počítačovou kriminalitou zkušenosti zatím nemáme.

Metody faktorové analýzy můžeme uplatnit naopak za těch okolností, kdy závisle proměnná známa není a máme k dispozici jen určitou množinu výchozích nezávisle proměnných, které představují veškerý dostupný a často velmi nepřehledný informační materiál. Metod faktorové analýzy lze použít při zkoumání osobnosti pachatele k vyjasnění určitých faktorových rysů osobnosti, při analýze dotazníkových akcí, redukci nepřehledných multivariačních systémů, např. při zkoumání stability výsledků různých výzkumů atp. Téměř všechny aplikace metod faktorové analýzy jsou založeny na linearitě vztahů mezi prvky výchozího parametrického systému a na předpokladu mnohorozměrného normálního rozdělení daných proměnných. Oba předpoklady nelze zpravidla podrobněji ověřovat. Bývají proto předmětem určitých námitek proti použití faktorové analýzy. Jiná věcná námitka vychází z toho, že zejména při rozborech osobnosti pachatele metody faktorové analýzy hodnotí pouze individuální rozdíly. Tedy, že jde o metodu atomistickou, zatímco osobnost ve skutečnosti není jen pouhým součtem nějakých atomárních prvků. Tytéž výhrady bývají někdy vznášeny i vůči nejjednodušší z metod faktorové analýzy, proti *metodě hlavních komponent (hlavních os)*, která mimo jiné je zvláště vhodná pro zmíněné redukce výchozích systémů dat. Pod tíhou poslední z námitek je proto rozumné požadovat, aby faktory byly interpretovány nejlépe jako pouhé aspekty možného seskupení výchozích parametrů a nikoliv jako kauzální příčiny studovaných jevů. Faktorová analýza se může stát např. významným nástrojem předběžné orientace tam, kde chybí základní klasifikační kategorie k zvládnutí popisu vztahů komplikovanějších systémů. Při aplikacích faktorové analýzy hraje velkou roli předběžný výběr výchozích proměnných. Zatím byla v kriminologických výzkumech uplatněna zejména při analýze stability výsledků, viz opět [138].

Faktorová analýza vychází z hodnocení vzájemných vztahů (nejčastěji korelací) daných proměnných kombinovaných podle všech možných dvojic. Z toho důvodu jsou někdy preferovány přístupy *plánování mnohofaktorových modelů*, které berou v úvahu *n*-tice daných proměnných, kde *n* může být obecně větší než dvě.

Charakteristické vazby. Jako pomůcky objektivního rozhodování ve věci zahrnutí příslušné proměnné (parametru) do výchozího souboru, můžeme použít *metod charakteristických vazeb* určité proměnné na jisté závažnější podskupiny daného souboru jednotek. Zmíněné vazby bývají nejčastěji měřeny korelačním koeficientem s následným jeho otestováním. Do výběru pak zahrneme jen ty proměnné, které mají charakteristicky významné (korelační) vazby. Odtud je odvozen název metody se synonymem *metoda charakteristických korelací.* Kromě podmínek použití korelačního koeficientu metoda předpokládá, že máme k dispozici určité rozložení statistického souboru na podskupiny. Není-li toto rozložení dáno předem z povahy řešeného úkolu, můžeme užít některé z metod klasifikace daných objektů. Smysl metod charakteristických vazeb spočívá v tom, že umožňují typovat proměnné s významnými vazbami, které pak zahrneme do parametrického systému, s nimž bude dále

pracováno. Významnost vazeb je nutno při rigorosním rozhodování testovat. Proměnné, u nichž nebylo možno prokázat významnost vazeb, do systému nezahrneme.

Metody klasifikace objektů. K nejjednodušším metodám klasifikace objektů řadíme postup *shlukovací analýzy* na základě vzdáleností objektů. Postupným zhodnocením vzdáleností všech možných dvojic objektů daného souboru se vytvoří jakési kondenzační jádro nejbližších objektů. Vypočte se jeho těžiště a považuje se za charakteristiku nového objektu. Postup se zopakuje na zbývajících prvcích, dokud nedojde k vytvoření adekvátních tříd. Kromě uvedené metody existuje ještě velké množství dalších procedur, které bývají členěny do tří základních typů jako tzv. *hierarchické, paralelní* a *sekvenční procedury.* Liší se vzájemně způsobem konstrukce jednotlivých shluků na základě apriorní informace o závěrečném počtu tříd, na které je třeba rozložit zkoumaný soubor objektů. Kromě tohoto členění rozeznáváme ještě shlukovací *procedury parametrické* a *neparametrické povahy* s podobným významem těchto termínů jako u testů statistických hypotéz, viz [136]. Podle typu výchozí informace o daných objektech, případně o jejich statistickém charakteru, rozeznáváme také tzv. klasifikace při totálně popsaných třídách, klasifikace s částečným učením, klasifikace s učením a bez učení (bez učitele). Poslední z uvedených metod (neparametrický případ) nazýváme též *shlukovou analýzou* či *taxonomií.* Třídy vzniklé touto klasifikací se pak nazývají *shluky, taxony* nebo *obrazce*. V češtině se používá též přejatých pojmů *cluster, clusterová analýza* nebo *numerická taxonomie*, případně rozpoznávání obrazců se samoučením. U metod klasifikace objektů platí snad ještě více než u ostatních multivariačních postupů, že výpočty by neměly nahrazovat závěry vyplývající z věcného přístupu a hlubokých odborných znalostí o předmětu zkoumání. Jsou vlastně jen doplňkem, který má být použit po pečlivé odborné analýze, lépe řečeno paralelně s ní a po adekvátním řešení odpovídajících složek komplexního zabezpečení výzkumu.

Analýza zločineckých gangů, tj. organizovaných skupin nebo part, zabývajících se páchání různých deliktů, je vhodná zejména pro sociometrické či psychologické studie struktury party se speciálními vztahy mezi jedinci. Umožňuje kvantifikovat řadu zajímavých charakteristik, jako např. váhu osoby v partě, váhu daného znaku osoby pro celou partu nebo její předepsanou část, koeficienty soudržnosti, ale také izolovanosti členů party, koeficienty spolupráce členů party nebo její části, vzájemný vliv člena na partu a obráceně party na jedince, míru spolupráce dvojic, dominování jedinců nad partou atp. Metody lze užít např. při analýze *skupinové delinkvence* jako zvláště nebezpečné formy páchání trestné činnosti. Dosavadní nevýhoda této metody spočívá v tom, že většinu uvedených měr nemůžeme ve statistickém pojetí testovat, neboť nejsou zatím známy odpovídající testy. Zadání dat je vhodné předem uspořádat do tvaru obdélníkového schématu (matice) s počtem řádků rovným rozsahu souboru osob a počtem sloupců, který odpovídá počtu znaků osob. Přítomnost znaků u daných osob se vyjádří dichotomicky, např. tzv. nula-jedničkovým způsobem. Zkušenosti s aplikacemi této metody se zatím netýkají problémů počítačové kriminality.

**

Problémy policie. Počítačová kriminalita jako protiprávní činnost spjatá s vědeckotechnickým rozvojem, je vysoce odbornou formou trestné činnosti především proto, že jejími pachateli jsou úzce specializovaní odborníci. Jak uvádí studie [90], je proto pochopitelné, že i represivní orgány musí mít k boji s touto protiprávní činností k dispozici dostatečně kvalifikované síly. V této souvislosti se ale nejedná pouze o policejní experty. Je nutné si uvědomit, že počítačová kriminalita není izolovanou formou protiprávního jednání, nýbrž, že jde většinou o navazující komplex skutků, jejichž objasnění a dokázání je věcí i dalších policejních služeb, které se bojem s kriminalitou zabývají. Specialisty na problematiku počítačové kriminality proto budou muset časem disponovat nejen kriminalisticko-technická a expertizní pracoviště, provádějící znaleckou (expertizní) činnost a poskytující další odbornou pomoc, ale též operativně-pátrací útvary kriminální policie a další orgány činné v trestním řízení. Bylo by mylné se domnívat, že v souvislosti s počítačovou kriminalitou je současná úloha našich orgánů zaměřena pouze na potírání softwarového pirátství cílenému proti produktům firem, které jsou členy BSA.

Speciální pomůcky v boji s počítačovou kriminalitou. BSA má s potíráním softwarového pirátství v nejrůznějších zemích světa bohaté zkušenosti. Jen v Evropě napomohla policii vyřešit několik desítek závažných případů, kdy bylo odhaleno rozšiřování a používání nelegálně získaného software. K tomu používá i vlastního specializovaného programu *SEARCH II*. V roce 1994 byl tento program prakticky předveden a dán k dispozici též specialistům naší kriminální policie. Podle [90] *SEARCH II* je specializovaný programový prostředek zaměřený na software firem sdružených v rámci BSA. Jeho činnost spočívá ve

-spuštění ze speciální diskety,
-prohlídce všech dostupných logických pevných disků,
-vytvoření dvou speciálních kontrolních součtů,
-vytvoření seznamu všech programů s extenzí *EXE* a *COM*.

Součinnost v mezinárodním měřítku. Podle zkušeností aliance v Evropě byl našim specialistům vysvětlen postup použití programu *SEARCH II*, včetně návodu pro vytvoření dokumentace nalezeného software. Tento program má ve Velké Británii atest svědčící o tom, že nepůsobí žádné potíže při pozdější práci s daty nebo s výpočetní technikou, na které byl použit. *SEARCH II* byl vytvořen BSA pro její potřeby a dle jejích představ, které také splňuje. Důkazem je mimo jiné i řada vyhraných soudních sporů se softwarovými piráty, kde právě tento program hrál zásadní úlohu a kde jeho tiskové výstupy sloužily jako hlavní důkazní prostředek. Program *SEARCH II* však nedokáže zjistit, zda pirátské programové vybavení

-nebylo před jeho použitím vymazáno,
-není uschováno v archivech s jinou extenzí pomocí některého z komprimačních nebo archivních nástrojů,
-nezanechalo na pevných discích soubory, které bylo možno vytvořit pouze jeho použitím,
-je uloženo na disketách.

K dalšímu zdokonalování nástrojů. Jak uvádí dále autor [90], pro práci kriminalistických expertů je nutné, aby disponovali jak nástroji, které budou mít všechny klady programu *SEARCH II*, tak i těmi, které budou splňovat nároky tímto systémem dosud neřešené. Ovšem takový nástroj prozatím běžně k dispozici nebyl. Jeho potřebu pociťovalo zejména expertizní pracoviště zabývající se počítačovou kriminalitou v Kriminalistickém ústavu Praha. Postupně byly vyvinuty verze, které se přiblížily kýženému cíli. Vyvíjený programový nástroj slouží jak k expertizní potřebě, tak i k potřebám trestně-procesních úkonů při zajišťování a dokumentování obsahu disket a pevných disků počítačů. Navíc umožňuje jednoznačně individualizovat diskety tak, aby bylo prokazatelné, zda na nich byl realizován jakýkoliv zápis nebo mazání dat. Tato identifikace má velký význam při zajišťování disket a počítačů v průběhu jednotlivých procesních úkonů v souvislosti s vyšetřováním trestné činnosti jakkoli spjaté s výpočetní technikou. Popsané nástroje umožňují policejním expertům dokázat, že bylo zkoumáno médium v tom stavu, ve kterém bylo zajištěno, a že je v tomtéž stavu i vráceno majiteli.

Aspekty účinnosti boje s kriminalitou. A tak pomocí počítačů, počítačových sítí a jejich speciálního programového vybavení lze vést poměrně účinný boj s počítačovou kriminalitou, spočívající zejména

-ve zjišťování způsobů, možných příčin a důsledků zneužití nebo napadení prostředků výpočetní techniky,

-v analýze neoprávněných zásahů do programového vybavení a datových záznamů,

-ve zjišťování neoprávněných zásahů do technického vybavení,

-ve zkoumání případů softwarového pirátství, plagiátorství a porušováni softwarových autorských práv,

-ve zjišťování obsahů paměťových médií výpočetní a organizační techniky,

-v poznání informační kriminality jako fenoménu moderní doby se všemi konkrétními kriminologickými aspekty a společenskými důsledky,

-v možnostech poskytování podkladů pro zpětnou vazbu při systémovém pojetí regulace nežádoucích společenských jevů, jmenovitě i počítačové kriminality,

-v možnostech případného usměrnění speciálních legislativních aktivit.

Meritorní poznatky z boje s počítačovou kriminalitou lze členit na poznatky týkající se bezprostřední represe a poznatky k prevenci počítačové kriminality. Podle studie [90], dosud řešené konkrétní případy se týkaly především represe, jako např. zkoumání obsahů zajištěných počítačů, disket a různých typů digitálních záznamníků. V rámci těchto zkoumání bylo často zaznamenáno i používání nelegálně užívaného software, na základě čehož byl vyšetřovatel upozorňován na možnost rozšíření trestního stíhání. První zajímavé poznatky byly získány při odborném zajišťování prostředků výpočetní techniky na místech trestných činů, při domovních prohlídkách anebo při obdobné konzultativní účasti expertů. Délka jednotlivých expertizních zkoumání se podle složitosti a náročnosti případu pohybovala od jednoho do pěti týdnů. Výjimkou byla pětiměsíční expertiza podvodného převodu částky přesahující jeden milion korun v jedné z našich finančních institucí. V tomto případě ke zjištění mechanizmu podvodu učiněného čistě počítačovou cestou, bylo použito dosud netradičních způsobů a

technik řešení, včetně použití videotechniky a počítačů. Průběžně získávané zkušenosti je neustále třeba zobecňovat formou závěrů a metodických pokynů pro potřeby ostatních orgánů činných v trestním řízení. Autor ve studii [90] doporučuje přitom aplikace nejmodernějších prostředků, včetně výpočetní techniky s adekvátním programovým vybavením.

9. Prevence a represe z pohledu počítačové kriminality

Sestaveno převážně z pramenů: [49], [59], [78], [89], [102], [105], [110], [114], [133], [134], [135], [138], [250].

9.1. Generálně preventivní účinky systému trestního práva

Idea, že lépe kriminalitě předcházet než následně napravovat škody, není nová, ale je v současné době velmi aktuální. Tradičně obecná kriminalita, což platí zejména o kriminalitě majetkové, se z hromadného negativního společenského fenoménu stala jevem masovým. Rovněž i počítačová, resp. informační kriminalita je na značném vzestupu. Určité východisko z této nepříliš nadějné situace nabízí moderně pojatá prevence.

Je známo, že řada států v tomto smyslu vytváří a realizuje preventivní systémy boje proti kriminalitě, jejichž charakteristickým rysem je plánovitost a koordinovanost jednotlivých preventivních aktivit. K nim se připojuje i Česká republika. O tom svědčí např. mimo jiné i Republikový výbor pro prevenci kriminality, který již v roce 1996 schválil *„Metodiku přípravy komplexního součinnostního programu prevence kriminality na místní úrovni“*. Prevence kriminality a trestní právo mají spojitost a vzájemně se ovlivňují hlavně v tom, že některé instituty trestního práva hmotného i procesního působí i preventivně.

Prevence kriminality bývá v řadě prací naší i světové kriminologie velmi různě definována. Podle jedné z nejkomplexnějších definicí, *do prevence kriminality náleží veškeré aktivity, směřující k předcházení páchání trestných činů, ke snížení jejich výskytu cestou zamezení páchání nebo neutralizací příčin a podmínek vzniku trestných činů (kriminogenních faktorů). Patří sem opatření, jejichž cílem či důsledkem je zmenšování rozsahu a závažnosti kriminality, ať již prostřednictvím omezení kriminogenních příležitostí nebo působením na potencionální pachatele a oběti trestných činů* (srov.[133]). Prevence tedy představuje pokus o eliminaci trestné činnosti ještě před jejím započetím nebo před jejím pokračováním.

Trestní kodexy mají reflektovat především dva základní aspekty. Primárním aspektem zůstává funkce *represivní*, jež spočívá v ochraně společnosti před zločinem; činí tak prostřednictvím systému sankcí (trestů), které postihuje jedince či skupiny, jež tyto kodifikované normy určitým právně stanoveným způsobem překročili. V této souvislosti je možno hovořit o moderní koncepci trestního zákona jako „zákona sociální ochrany“. Druhou hlavní funkcí trestního zákona je funkce *expresívní*, tzn., že vyjadřuje prostřednictvím zákazů a zápovědi (interdiktů) určitý systém sociálních a morálních hodnot tak, jak je v té které době uznává kolektivní společenské vědomí. Uvedené hodnoty by měly zákonodárcům být známy do té míry, aby nevznikaly zásadní konflikty mezi zmíněnými dvěma funkcemi trestního práva. Zjišťovány mohou být např. prostřednictvím výzkumu veřejného mínění v příslušné populaci na vymezeném teritoriu. Tyto dvě základní funkce bývají ve vztahu harmonickém, ale též i konfliktním. K poruše harmonického vztahu dochází zvláště tehdy, když nějaká sankce přetrvává, ačkoliv hodnota, jejíž ochranu zakládala, není již součástí kolektivního hodnotového vědomí (systému) příslušné společnosti. Taková sankce je potom chápána spíše již jako výraz přeživších se pozůstatků a nikoliv jako projev ochrany živé hodnoty společnosti.

V práci [133] se autoři kloní k názoru, že současný trend moderních legislativních snah, charakteristický hledáním alternativ systému trestní justice (např. instituty „odklonu“, „narovnání“ apod.), vytváří v současnosti třetí základní funkci práva trestního (ale i občanského, hospodářského, finančního apod.) a tou je jeho funkce *preventivní*. Domníváme se, že zejména ve spojení s počítačovou kriminalitou má tento aspekt nesmírný význam z hlediska budoucího bouřlivého vývoje informačních technologií.

Jednou z hlavních funkcí každého trestně právního systému je jeho *generálně preventivní účinek* v právním vědomí širších vrstev obyvatelstva a zejména pak v povědomí potenciálních pachatelů trestných činů. Bohužel právní povědomí trestnosti například ve sféře softwarového pirátství je u většiny našich občanů celkově slabé. To je i jeden z faktorů, poměrně malé účinnosti našeho trestněprávního systému v oblasti počítačové kriminality. Je třeba si uvědomit, že míra generálně preventivního účinku je spjata v přímé závislosti s účinností právního systému jako celku. Lze očekávat, že čím bude větší účinnost právního systému jako celku, tím větší bude i jeho generálně preventivní účinek v právním vědomí populace. Naopak, velký generálně preventivní účinek na právní vědomí nelze předpokládat při malé účinnosti systému. Logicky vzato, míra generálně preventivního účinku trestně právního systému by neměla překročit míru účinnosti tohoto systému. Podle [133] s přihlédnutím k posledním aktualizacím výsledků výzkumu [134], celková míra generálně preventivního účinku našeho trestněprávního systému v posledním deceniu nepřekročila 26,1%. Hlubším výzkumem zatím neověřené odhady generálně preventivních účinků legislativních úprav, použitelných v boji s počítačovou kriminalitou, leží rovněž pod touto mezí. Vývoj tohoto ukazatele u celkové kriminality za poslední zkoumané období v České republice nelze hodnotit negativně. Průměrná úroveň účinnosti našeho trestněprávního systému (jako pravděpodobné dominanty generálně preventivního účinku úprav použitelných v boji s počítačovou kriminalitou) je podle podaných ukazatelů celkově nepříliš vysoká. Přesto lze aktuální trend jejího vývoje považovat za nadějný.

9.2.Právní regulace elektronického přenosu dat u nás

Jedním z nejúčinnějších prostředků proti zneužívání dat je vhodná právní úprava elektronického přenosu informací.

Jak uvádí autor studie [114], Český obchodní zákoník neobsahuje žádná ustanovení, která by se výslovně týkala právních vztahů navázaných na elektronickou formu. Podle obecných ustanovení občanského zákoníku je zachována písemná forma právního úkonu, je-li učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila. Obchodní zákoník navíc stranám umožňuje dohodnout se na obecných podmínkách nebo na vykládacích pravidlech. I zákon o účetnictví a zákon o správě daní obsahují obecná ustanovení, která umožňují vést a předkládat účetní a daňové záznamy v elektronické formě. I český celní zákon a příslušná sekundární legislativa umožňují nahradit „papírové“ dokumenty záznamy elektronickými.

Vedení záznamů a požadavky na ukládání dat upravuje též zákon o archivnictví a druhotná legislativa. Záznamy v elektronické podobě musí být uloženy po stejnou dobu jako fyzické dokumenty. Navíc musí být, stejně jako jiné psané záznamy, zaopatřeny proti zneužití, zničení ztrátě nebo poškození. Český právní systém je tedy alespoň v zásadním pojetí vybaven pro rozvoj a využití elektronických prostředků v obchodě i v jiných dalších aktivitách.

Z hlediska počítačové kriminality jsou v případech elektronického přenosu dat aktuální zejména *otázky průkaznosti* elektronických záznamů. Podle českého práva jsou elektronicky pořízené záznamy přípustným a dostatečným dokladem skutečností, jichž se týkají. České právo i právní praxe stojí nyní před vymezením konkrétních podmínek právní závaznosti a vykonatelnosti elektronicky realizované komunikace. V současnosti již nestačí akcentovat pouhé obecné požadavky na použití, uchovávání a bezpečný přenos elektronických zpráv. Zatím záleží hlavně na stranách, které využívají elektronické komunikace, aby zajistily, že pravidla jejich vzájemné komunikace těmto obecným požadavkům dostála. Velké naděje vzbuzuje nová zákonná úprava problematiky kolem tzv. *elektronického podpisu*.

Avšak v aplikační praxi nevznikne jednoduchá situace ani po přijetí těchto úprav. Bude nezbytné přesvědčit soudy o dvou hlavních věcech - o otázce přípustnosti (a o možné kolizi) a autentičnosti záznamů v elektronické podobě. Pokud je například možné použít bankovní záznamy v počítači jako důkaz ve sporu, je nutné, aby byly i jiné záznamy podobného charakteru jako důkaz přípustné. Budou-li však přípustné, nebudou mít žádnou důkazní hodnotu, jestliže nebude možné dokázat, že představují autentické záznamy transakcí. Kvůli nedostatku domácí právní praxe se budou muset české soudy obracet k zásadám a metodám aplikovaným v podobných sporech v západní Evropě, případně ve Spojených státech. Rovněž subjekty veřejnosti, fyzické i právnické osoby, nebudou zpočátku jistě plně adaptovány na podmínky možných aplikací ať z principiálních či technických důvodů.

9.3. Prevence nejnebezpečnějších forem počítačové kriminality podle nadnárodních hledisek

Pirátství v Evropě, které se týká počítačového software, je jedním z nejožehavějších problémů počítačové kriminality. Jak uvádí evropský rada Obchodní softwarové aliance BSA ve svém příspěvku [59], pro prevenci je velmi důležité

-obecně popsat některé evropské a mezinárodní normy pro vynucování autorských práv, a to zvláště ty, které se vztahují k software, např. na základě praktických zkušeností BSA s těmito normami v souvislosti s akcemi vynucujícími autorská práva jménem držitelů autorských práv na software;

-na základě těchto, zejména evropských zkušeností doporučit preventivní pozornosti některé oblasti či lokality, o nichž se BSA domnívá, že by v nich mohlo dojít k posílení ochrany autorských práv na software a kde by mohla nastat redukce rozsahu softwarového pirátství, pokud budou v České republice přijaty příslušné dodatky zákonů na ochranu autorských práv;

-vyjasnit a diskutovat problematiku současného stavu českého zákonodárství v oblasti ochrany software a jejího vynucování.

BSA a evropský přehled. Od konce osmdesátých let dochází ke zvyšování rychlosti postupu směrem k mezinárodnímu slaďování zákonných norem, které mají chránit výsledky prací, při nichž vzniká duševní vlastnictví, software nevyjímaje. Tyto v širokém měřítku se shodující mezinárodní normy jsou vytvořeny s cílem podporovat a dále rozšiřovat narůstající mezinárodní vývoj a distribuci výsledků, jejichž podstatou je duševní vlastnictví. Země střední a východní Evropy se po roce 1989 k tomuto mezinárodnímu trendu s nadšením připojily. Počínaje rokem 1990 v Albánii, Bulharsku, Estonsku, Litvě, Polsku, Rusku a v Ukrajině byly přijaty nové zákony o autorských právech. V Československu a Maďarsku pak doplňky zákonů o ochraně autorských práv a uvažuje se ještě o dalších rozsáhlých novelizacích. Rok 1994 byl zvláště důležitým rokem pro proces směřující ke sladění ochrany software. Tehdy jsme prošli dvěma mezníky. Jeden z nich se týkal ochrany autorských práv na software a druhý se vztahoval k vynucování těchto práv, pokud jde o výsledky prací všech typů, jejichž podstatou je duševní vlastnictví, software nevyjímaje.

Softwarová direktiva Evropské rady. Jednoho z významných mezníků bylo dosaženo v okamžiku, kdy v rámci celé Evropské unie, s výjimkou Lucemburska, vstoupila v platnost *Softwarová direktiva Evropské rady*. Tato softwarová direktiva, která je známa pod oficiálnějším označením *Direktiva Rady 91/250 ze 14.5.1991 o zákonné ochraně počítačových programů*, poskytuje základní návod, platný v rámci Evropské unie, pro ochranu autorských práv na software. Francie, Portugalsko a Nizozemí byly posledními členskými státy Evropské unie, které měly přijmout legislativní opatření v souvislosti s uvedením Direktivy v život. Direktiva se rovněž stala vzorem pro legislativu v oblasti ochrany autorských práv software v zemích střední a východní Evropy a státech *EFTA (European Free Trade Association - Evropské sdružení volného obchodu)*. Její ustanovení se stala vzorem pro ochranu autorských práv na software v České republice jako výsledek toho, že Československo v roce 1991 podepsalo Evropskou asociační smlouvu.

GATT TRIPS. Druhého mezníku bylo dosaženo v dubnu 1994, kdy více než 120 států uzavřelo obchodní dohodu takzvaného Uruguayského kola. Dvacet tisíc stran této dohody zahrnuje dohodu o Obchodních aspektech autorských práv týkajících se duševního vlastnictví, známější pod zkratkou *TRIPS (Trade-Related Aspects of Intellectual Property Rights)*. Česká republika je samozřejmě členem GATT. Přestože je v současné době obtížné předvídat datum, kdy bude třeba *GATT TRIPS* uplatnit v České republice, mnoho členských států GATT se začíná touto problematikou zabývat a připravuje změny svých národních zákonů, které mohou být požadovány na základě *GATT TRIPS*.

Evropské zkušenosti BSA. Organizace BSA se nachází v jedinečném postavení, ze kterého má přehled o mezinárodním dopadu všech význačných mezníků ve vývoji problematiky ochrany autorských práv na software a jejich vynucování. Od té doby, kdy byla v roce 1989 založena, BSA věnovala většinu svého úsilí podpoře legálního užívání tzv. krabicového komerčního software prostřednictvím kombinování legislativní reformy, soudních sporů a aktivit v oblasti „public relations“ (vztahů k veřejnosti). Od svého počátku

ve Spojených státech BSA rozšířila své aktivity do 60 států po celém světě, včetně více než 20 evropských zemí. V České republice BSA zahájila svůj program v roce 1994. Tento program do sebe pojal dvě české softwarové společnosti: Software 602 a APP Systems.

V prvních letech evropského působení BSA byl software relativně novým technologickým odvětvím a na akademické půdě se dlouze debatovalo o nejlepších metodách zákonné ochrany tohoto fenoménu. Uvažovalo se o autorských právech, patentech, nebo o něčem zcela novém a odlišném. Šlo současně o oblast, ve které většina veřejnosti nebyla přesvědčena o tom, že software je pod ochranou zákona. Mnoho práce BSA v Evropě v tomto období bylo věnováno vzdělávání jak veřejnosti tak i zákonodárců, s cílem vytvořit povědomí o ceně software a nutnosti chránit jeho vývoj a distribuci prostřednictvím zákonů na ochranu autorských práv.

To, že v členských státech Evropské unie vstoupila v platnost Softwarová direktiva a mezinárodní dohoda vyplývající z GATT TRIPS, vytváří novou éru v oblasti ochrany autorských práv na software. Veřejnost nyní mnohem více používá software pro podnikatelskou činnost i v domácnostech, stále vzrůstá poptávka veřejnosti po nových softwarových produktech a rozšiřuje se povědomí veřejnosti o tom, že software vyžaduje ochranu zákonem. V mezinárodním měřítku je mezi zákonodárci a soudci rovněž široce rozšířen názor - a ne jen akademický, že zákon na ochranu autorských práv je ve většině případů nejvhodnějším a nejschůdnějším řešením ochrany počítačových programů.

Jak ukázaly zkušenosti BSA, zákonem uznávaná ochrana autorských práv na software je sice nezbytným východiskem, nepostačuje však pro ochranu samotných držitelů těchto práv. Musí být rovněž k dispozici zákonné sankce - ať již občansko právní, či kriminální - které by autorská práva vynucovaly.

Prevenci jedné z nejnebezpečnějších forem počítačové kriminality podle nadnárodních aspektů je věnován příspěvek [59]. Autor zde podává informace o legálním softwarovém průmyslu v Evropě a o druhé straně této mince - o nelegitimním, tzv. „pirátském“ průmyslu.

9.4. Některé faktory prevence a represe závažné počítačové kriminality

Základním východiskem pro prevenci počítačové kriminality je především poznání způsobů páchání této trestné činnosti se zaměřením na osobu pachatele. Dále pak poznání stávajících podmínek i perspektiv využívání výpočetní techniky. V neposlední řadě je nezbytné využívat i poznatky o účinnosti preventivních opatření ze zahraničí. Jak mimo jiné uvádí pramen [102], prevenci je nezbytné směřovat k vytvoření podmínek zabezpečujících výpočetní techniku a automatizovaný systém zpracování dat proti neoprávněným zásahům, zničení či zneužití. Na prevenci by se měl podílet výrobce i uživatel (vlastník) výpočetní techniky s cílem vytvořit takové ochranné systémy, jež by vyloučily, respektive snížily

možnost napadení programů viry a případně též zamezily nedovolené manipulaci se zpracovávanými daty. V západních zemích vznikl dokonce specializovaný průmysl zabývající se problematikou ochrany výpočetní techniky. Zdá se však že tato skutečnost motivuje stále početnější okruh osob se zájmem vyzkoušet své schopnosti a proniknout ochranou počítačů. V mnoha případech jsou právě tyto osoby nejrůznějšími formami nátlaku nuceny k jednáním, které má za následek poškození výpočetní techniky či neoprávněnou manipulaci s daty.

Podle [102] prevence počítačové kriminality je zaměřena též k výchově občanů, vytváření prostředí náročnosti a odpovědnosti za práci s výpočetní technikou i zpracovávanými daty. Právě vytvoření podmínek pro posílení odpovědnosti by mělo vést k omezování zájmů odborně erudovaných osob o jednání působící narušení řádné činnosti výpočetní techniky. Preventivní opatření proto směřují především k vytvoření systému zabezpečujícího přístup k výpočetní technice pouze oprávněným osobám při existenci předpokladů pro možnou kontrolu výsledků práce těchto osob. Dalším východiskem je budování technických prostředků a vytváření organizačních předpokladů pro ochranu počítačů. Zásadní význam ovšem stále mají ochranné systémy a jejich zdokonalování, neboť tyto směřují především k realizaci ochrany konkrétní výpočetní techniky i systému automatizovaného zpracování dat.

Preventivní opatření právní povahy představují především právní normy upravující podmínky ochrany autorských práv, informací a výpočetní techniky. Za určující je nutno považovat i způsob trestněprávní ochrany práv chráněných těmito normami, především pak jejich vzájemnou návaznost. Dosud se však u nás neprojevil komplexní přístup k ochraně výpočetní techniky a dat. Podle mínění autorů [102] tuto situaci bude nutno co nejdříve se vší důsledností řešit. Rovněž není formulována generální koncepce právní a mimoprávní ochrany výpočetní techniky a dat. Ukazuje se, že tento problém není možno řešit prostřednictvím zájmů či potřeb jednotlivých subjektů. Přijetím zákona o ochraně osobních údajů v informačních systémech, viz [250], byly vytvořeny předpoklady pro zvýšení ochrany osobních dat. Nelze také podcenit ochranu výpočetní techniky prostřednictvím činnosti policie. To však předpokládá vytvoření specializovaných útvarů v rámci kriminální služby. Dalším prostředkem ochrany výpočetní techniky je využití možností bezpečnostního systému ochrany dat prostřednictvím státních i soukromých podniků, které se zabývají speciálními otázkami ochrany dat a budováním bezpečnostních systémů ochrany dat.

Skupina expertů *Rady Evropy* se po několik let zabývala otázkami počítačové kriminality . Již v roce 1988 byla zpracována studie, z níž vyplývá doporučení, aby všechny vlády členských států zvážily možnost využívání závěrů zprávy pro legislativní řešení otázek počítačové kriminality. Zpráva expertů obsahuje doporučení pro legislativní orgány a je rozdělena do dvou částí. První je označována jako minimální seznam, ve kterém je uvedeno celkem osm základních skutkových podstat trestných činů. V souladu se světovými trendy je potřebná mezinárodní koordinace při budování adekvátní kompatibility právní ochrany informací. Dalším východiskem prevence je pak kriminalizace jednání směřující ke zneužití výpočetní techniky, a to prostřednictvím formulace speciálních skutkových podstat,

umožňujících postih počítačové kriminality v souladu s návrhy a doporučeními *Rady Evropy*. Tento přístup však předpokládá řešení problému na mezinárodni úrovni při akceptování komplexního přístupu, neboť určité formy počítačové kriminality nabývají v současnosti povahy mezinárodního organizovaného zločinu.

**

Softwarový průmysl a jeho produkty. Použijeme-li nejjednodušší definice, pak softwarový průmysl se skládá z tvorby a distribuce počítačových programů. Bez těchto programů nemůže personální počítač (známý v průmyslu nejčastěji pod označením „PC“, nebo jednoduše jako „hardware“) poskytovat žádné užitečné funkce. Některé softwarové produkty, které se nazývají „operační systémy“, řídí základní funkce počítače. Další typy programů, kterým říkáme „aplikace“, dovolují uživatelům řešit mnoho úloh, které pomáhají zvyšovat produktivitu práce. Mnohdy lze tak pomocí počítačů řešit problémy, které by jinak řešitelné nebyly pro jejich časovou, finanční či jinou náročnost. Zpracování textů, vytváření elektronických tabulek, práce s databázemi a konstruování podporované počítačem, představují pouze určitou část souboru takových úloh.

Tvorba počítačových programů vyžaduje intelektuální dovednost a vzdělání v oboru počítačového programování. Psaní programu pro počítač se sice nepodobá psaní románu nebo jiné literární činnosti, ale je ve většině případů rozhodně náročnou tvůrčí činností. Programátor vytváří organizovanou strukturu svého programu známou jako *algoritmus* a poté píše posloupnost příkazů v programovacím jazyce, který si zvolil, přičemž tento zápis musí být v souladu s vytvořeným algoritmem. Takto vznikající *zdrojový program* zpravidla nebude pracovat na počítači sám o sobě; programátor jej musí přeměnit nebo „kompilovat“ do podoby, které počítač „rozumí“, tj. do formy, které říkáme *objektový (spustitelný, exekuční) program.* Tento objektový produkt je konečným programem, který je ve skutečnosti distribuován zákazníkům. Distribuce je obvyklá na pružných discích (floppy discích - disketách) o průměru 3,5 palce (8,9 cm), dříve 5,25 palce (13,4 cm), dnes již i na CD nosičích. Diskety se softwarem solidních výrobců jsou většinou zabaleny společně s vysvětlující dokumentací, záručním listem a licencí uživatele, která je z hlediska autorských práv nejdůležitější věcí. Přestože software může být napsán jednotlivými programátory, většina paketových (krabicových) komerčních programů je vytvářena středně velkými až velkými týmy v období několika měsíců až let; poté jsou tyto programy pravidelně aktualizovány a vylepšovány, čímž vznikají jednotlivé verze.

Distribuce počítačových programů se ve většině rozvinutých zemí uskutečňuje prostřednictvím dvoustupňového systému velkoobchodníků a dealerů, který je podobný systému, jaký je využíván i v jiných průmyslových odvětvích. Společnosti vydávající software vytvářejí programy, distribuční společnosti se starají o velkoobchod a dodávky software dealerům a dealeři software prodávají koncovým uživatelům. Takzvaní koncoví uživatelé software jsou jednotlivci, komerční společnosti, vzdělávací instituce nebo vládní a jiné úřady, které software používají.

Udělováni licencí je v oblasti výroby a distribuce software velmi rozšířené. Společnosti vydávající software obvykle uživateli poskytují právo používat softwarový produkt na jednom počítači prostřednictvím licence, která vstupuje v platnost porušením obalu a je součástí softwarového balíku. Tato licence stanoví pravidla omezující použití software koncovým uživatelem. Velké společnosti nebo vládní a jiní koncoví uživatelé, kteří chtějí nainstalovat softwarový produkt na větší počet personálních počítačů, často se společností vydávající software vstupují do vztahu, kterému říkáme licence na lokalitu. Někteří vydavatelé software využívají elektronický přenos a poskytování licencí prostřednictvím telefonních modemů a počítačových sítí propojených na velké vzdálenosti, takže jejich zákazníci mohou autorizovaný software obdržet čistě elektronickou cestou.

Společnosti vydávající software jsou přesvědčeny o tom, že zákon o ochraně autorských práv je nezbytným legislativním základem pro vývoj a distribuci počítačového software. Protože počítačový software je v současné době možné velmi snadno kopírovat a protože kopie software pořízené počítačem jsou identické s originálem, vydavatelé software jsou nuceni spoléhat na zákon o ochraně autorských práv a na důrazné vynucování těchto práv. Závisí na tom jejich přežití. Ve stávajících politicko-ekonomických podmínkách by nikdo nemohl vyvinout a uvést na trh program, kdyby mohl prodat pouze jedinou kopii tohoto programu. Jestliže jsou později vyrobeny další kopie bez jeho svolení, pak nemá hmotnou motivaci vytvářet jakýkoliv nový software. Zákon na ochranu autorských práv zajišťuje zpětný finanční tok, který držiteli práv v tržních podmínkách postačuje pro návrat jeho investic, udržování a zlepšování software, přijímání nových zaměstnanců a vývoj nových produktů tím, že autorizovaným výrobcům software poskytuje výhradní právo řídit kopírování a distribuci výsledků jejich práce.

Hrozba softwarového pirátství. Podobně jako v dalších průmyslových odvětvích založených na ochraně autorských práv, největší hrozbou pro růst softwarového průmyslu je softwarové pirátství, tedy okrádání softwarového průmyslu o zisk plynoucí z držení autorských práv k duševnímu vlastnictví specifického charakteru. Enormní hrozba, kterou softwarové pirátství pro softwarový průmysl představuje, vyplývá hlavně

-ze zvyšující se dokonalosti forem páchání této kriminality,

-ze vznikající a prohlubující se organizovanosti zúčastněných struktur,

-ze stále rostoucího rozsahu.

Typy softwarového pirátství. Autor příspěvku [59] rozeznává pět základních typů krádeží software. Některé z nich se podobají typům pirátství, které se vyskytují i v jiných průmyslových odvětvích založených na ochraně autorských práv, jiné jsou specifické právě jen pro softwarový průmysl. Můžeme definovat následujících pět základních typů softwarových pirátů:

1. Pirátství organizací - koncových uživatelů je největší hrozbou softwarovému průmyslu. Jde o typ pirátství, který je z hlediska softwarového průmyslu specifický. V případě průmyslu video nahrávek a zvukových záznamů většina uživatelů pořizuje pouze jedinou

kopii výsledků práce, jejíž podstatou je duševní vlastnictví. Pro vlastní domácí použití jedinců to zpravidla stačí. V protikladu k tomu organizace, které nezákonně používají softwarové produkty, zhotovují mnoho nelegálních kopií software, které se pak používají na personálních počítačích v rámci podnikatelských, vládních, vzdělávacích, či jiných činností.

Organizace BSA vznesla občanskoprávní i soudní obvinění proti několika organizacím - koncovým uživatelům - v rámci celé Evropy, Českou republiku nevyjímaje. Mezi žalovanými koncovými uživateli byly některé velmi známé a jinak respektované společnosti z bankovnictví, žurnalistiky, ze sektorů konstrukčního a leteckého průmyslu a z mnoha dalších průmyslových odvětví. Představitelé těchto vážených společností by nikdy nepomysleli např. na krádež řádově desítek personálních počítačů pro své kanceláře. Avšak pořízení často i daleko většího počtu nelegálních kopií programů považovali za samozřejmé, místo aby zakoupili práva pro užívání tohoto software od legálního dodavatele. Tyto společnosti nikterak nepřipouštěly skutečnost, že nelegální používání software je totéž jako nelegální používání hardware- tedy, že je to v podstatě nezákonný akt.

2. Plagiátoři. Jde o jeden z typů komerčních podnikatelů či podniků, které vydělávají peníze prodejem neautorizovaných kopií softwarových produktů, nikoliv jejich používáním. Nejrafinovanější softwaroví plagiátoři produkují diskety, dokumentaci a obaly, které se velmi podobají výrobkům společností vydávajících legitimní software. Plagiáty softwarových produktů, které se nejvíce podobají originálním produktům, se často zhotovují v Asii a jsou obvykle importovány tranzitem přes státy jižní, střední a východní Evropy na cílové evropské trhy.

3. Pirátství překupníků se objevuje tehdy, když si distributoři nebo dealeři zhotovují kopie software na diskety, CD nosiče, nebo na vnitřní paměťová zařízení („pevné disky“) počítačů, které prodávají, aniž by k tomu měli povolení od vydavatele software. Tito softwaroví piráti profitují ze svých protizákonných aktivit, jejichž podstatou je prodej ilegálních kopií programů, které nelegálně kopírují s téměř zanedbatelnými náklady. Tito piráti rovněž šidí své zákazníky, kteří často nedostanou dokumentaci nebo další informace o software, neobdrží záruku výrobce, nemají možnost získat technickou podporu a nezískají přístup k novým verzím produktu.

4. Pirátství zásilkových služeb spočívá v distribuci nelegálních kopií software na disketách nebo dalších mediích prostřednictvím pošty. Štítky na disketách jsou v tomto případě často popsány ručně nebo na psacím stroji. Piráti pracující jako zásilkové služby často své nelegální produkty inzerují v novinách a katalozích, šíří reklamu faxy a propagují též prostřednictvím stanic BBS.

5. BBS piráti nekalou činnost realizují prostřednictvím nedovolené reprodukce a distribuce software po telekomunikačních sítích. Tito piráti obvykle pořizují kopie programů na svém počítači, aniž by k tomu měli povolení od vlastníků autorských práv. Software pak bez povolení držitele autorských práv distribuují dalším osobám, které jsou na příslušný počítač napojeny prostřednictvím telefonu a modemu.

Úlohu statistiky v prevenci i represi počítačové kriminality nelze podceňovat. Rozsah počítačové kriminality, jejích forem a společenských dopadů může být důležitým vodítkem taktiky i strategie nejen boje s kriminalitou, ale i impulsem ke správné orientaci preventivních opatření. Jak uvádí pramen [110], v současné době je počítačová kriminalita v České republice zahrnována policejními orgány do oblasti *hospodářské kriminality*, což nevyhovuje, protože to plně nevystihuje různorodost i podstatu této oblasti trestné činnosti. Policejní orgány mají pro evidenci trestné činnosti a její následné využití k dispozici databázové systémy celostátních policejních evidencí a statistik. Tyto systémy se dělí na dvě oblasti.

První oblast zahrnuje celostátní policejní evidence vedené na *Odboru evidencí a statistik (OES)*, jimiž jsou *Evidenčně statistický systém kriminality (ESSK), Zájmové osoby policie (ZOP), Neukončené přípravné řízení o známých pachatelích (AVIZO), Nápad trestné činnosti (NTC), Pátrání po odcizených vozidlech (PATRMV), Pátrání po osobách (PATROS), Centrální evidence odcizených a ztracených zbraní (ZBRANE), Systém bezpečnostního značení skel automobilů (SBZ), Systém evidence uměleckých děl (SEUD)*. K tomuto přistupuje dosud manuálně vedený fond *Základní evidence pachatelů (ZEP)*.

Druhá oblast zahrnuje správní a podpůrné evidence dostupné na OES: *Evidence dopravních nehod (DN), Centrální registr občanů (CRO), Evidence motorových vozidel (EMVO), Registr organizací a Obchodní rejstřík (FIREMM MONITOR), Vytváření podob osoby podle výpovědi svědka (FACETTE)*.

Z vyjmenovaných evidencí se podle [110] využívají pro evidenci trestné činnosti nejčastěji následující evidence:

-*Evidenčně statistický systém kriminality (ESSK)* -počítačově vedený systém, který registruje a zpracovává údaje o neobjasněné i objasněné trestné činnosti a jejích pachatelích v období od roku 1973 do současnosti. Databázi tohoto systému naplňují případy, které šetří policie, úřady vyšetřování. Databáze se naplňuje zpracováním formulářů (*Formulář trestného činu*), který je vyplňován na základě existujících číselníků, kde určité skutečnosti jsou nahrazeny kódem.

-*Nápad trestné činnosti (NTC)* -evidenční systém používaný kriminální policií pro zachycení nápadu trestné činnosti na daném území. Jeho databáze je poměrné rozsáhlá a dostatečně podrobná při zachování únosné míry nároků na obsluhu a hardwarové vybavení. Základním prvkem tohoto systému je okres, kde se tato evidence vede a kde by měla být databáze tohoto systému doplňována všemi kriminálními případy, které se v daném okresním regionu udály.

Statistika v resortu Ministerstva spravedlnosti má zásadní význam pro jednu z možných cest měření účinnosti právního systému vůči počítačové kriminalitě. Postup byl u nás poprvé navržen, realizován a popsán ve studii [135]. Postupně pak rozveden až do současné fáze, popularizované též v článku [134]. Je založen na kvantifikaci procesu legalizace (kvalifikace) systému registrované kriminality u nás pomocí základních

statistických údajů. Proces legalizace (kvalifikace) kriminality je založen na prosívání objemu a v restrukturalizaci skladby kriminality během průběhu trestního řízení. Přitom měřitelnost a kvalifikovaná struktura registrované kriminality co do typů trestné činnosti se postupně zlepšuje směrem k finitním, soudním statistikám. Pojem „zlepšování“ chápeme jako zpřesňující se aproximaci objektivně existující reality, ať co do skutkových podstat deliktů či jejich registrovaných objemů podle nejrůznějších nástrojů aparátu měr kriminality. Na těchto principech je pak založena operacionalizace procesu legalizace kriminality. Policejní statistiky mají pro resort vnitra své nezastupitelné místo a význam, pomáhají takticko-operativní činnosti, informují o vytíženosti policejních orgánů činných v trestním řízení a jak již bylo uvedeno, plní řadu dalších důležitých funkcí. Avšak z výše uvedených důvodů musíme pro odhady účinnosti trestněprávního systému preferovat statistiky resortu spravedlnosti. Jako nejspolehlivější z hlediska struktury kriminality byla proto volena justiční statistika pravomocně odsouzených osob. Tato statistika však není jediným pramenem informací využitelných k jmenovaným účelům. V resortu Ministerstva spravedlnosti jsou k dispozici celkově tyto zdroje:

-údaje o činnosti státních zastupitelství

-ve dvou druzích statistik:

-trestní statistika,

-evidence podnětů ke stížnostem pro porušení zákona;

-ve třech druzích výkazů:

-o agendě všeobecné,

-o agendě trestní (včetně případů, kdy pachatel není znám),

-o agendě netrestní;

-údaje o činnosti soudů

-ve čtyřech statistikách:

-statistika T-trestní,

-statistika C-občansko-soudní,

-statistika O-týkající se nezletilých dětí,

-statistika R-rozvodů;

-v 10 druzích výkazů, např. o hlavních agendách soudů, o trestních věcech, vazbách, o obchodním rejstříku atp.

Dodejme, že opodstatněnost navržených měr účinnosti a tedy i generální prevence je spjata s určitými teoretickými východisky dynamiky, stability a perseverance trestně právních systémů. Tyto pojmy a vazby k dané oblasti našeho zájmu byly rozpracovány a podrobněji studovány v *kriminologické statistice*, jako mezní disciplině na pokraji kriminologie a matematické statistiky, ještě před zahájením vlastního výzkumu účinnosti legislativních úprav. Důležitou roli zde hrají též odhady objemů skryté kriminality, opřené o expertní odhady policejních specialistů. Implicitně se do možností odhadů měr generální prevence právních systémů promítají i zkušenosti z praktických aplikací i teoretického zázemí

kriminologické dynamiky a prognostiky. Bez rozvoje těchto disciplin v minulosti bychom dnes rozhodně neměli k dispozici tak široké operační pole uplatnění statistických metod v oblastech našeho zájmu. Smysl rozpracování kriminologické prognostiky lze spatřovat především v ověření použitelnosti lineárních regresních modelů pro hodnocení dynamiky kriminality, jevů s ní spjatých i měr účinnosti a generální prevence právních systémů. Získané poznatky byly uplatněny ve všech dosavadních etapách výzkumu účinnosti legislativních úprav našeho právního systému. Podrobněji k tomu viz např. [138]. Pokud jde o prevenci či represi z užšího pohledu počítačové kriminality, aplikace stávajících i vyvíjených přístupů kriminologické statistiky mohou při dobrém věcném rozpracování problémů sehrát významnou roli, podobně jako tomu bylo dříve i v jiných řešených případech. Jejich širší exploatace je proto z hlediska nebezpečí mohutného růstu informačních deliktů žádoucí.

Spolupráce policie s jinými orgány je rovněž jedním z důležitých faktorů prevence i represe počítačové kriminality. Jak uvádí [110], policejní sbory všech vyspělých států se ve stále větší míře zabývají problematikou zneužívání výpočetní techniky. Hledají speciální metody identifikace a prevence a své síly spojují i v mezinárodním měřítku prostřednictvím mezinárodní organizace kriminální policie - *INTERPOL*. V těchto státech policejní organizace, prokuratury a soudní orgány pořádají školení, semináře a konference pro své zaměstnance o počítačových trestných činech, vytvářejí se specializované vyšetřovací týmy pracující na tvorbě potřebných ochranných opatření a jsou navrhovány a přijímány nové zákony zaměřené na prevenci a postih pachatelů počítačové kriminality. U nás byla a je registrována a soudně stíhána řada případů počítačové kriminality. Ve většině známých případů byl však pachatel odhalen spíše náhodou než systematickou prací policejních nebo jiných bezpečnostních orgánů. S celkovým rozvojem využití výpočetní techniky je třeba zabývat se problematikou počítačové kriminality kvalifikovaně a řešit i otázky prevence tohoto druhu kriminality. Ze známých případů počítačové kriminality vyplývá, že nejdůležitější podmínkou odhalení pachatele je perfektní a poctivá práce všech zaměstnanců postižené instituce, dodržování předepsaných postupů a provádění stanovených kontrol. Pro vyšetřovatele platí, aby byl co nejdříve na místě činu a co nejdříve zajistil stav počítačového systému a získal všechny informační podklady podmiňující zahájení vyšetřování. Nejzávažnějším a také nejobtížnějším problémem je zjištění, co se skutečně v počítačovém systému stalo, přičemž je třeba dbát na to, aby byly co nejrychleji analyzovány možnosti a postupy pachatele. Pochopitelně na tuto vysoce specializovanou práci nemůže stačit policista sám, byť by byl vysoce kvalifikovaný a dobře obeznámený jak s technickou, tak i s programovou a provozní stránkou počítačových technologií. Vynikající kvalifikace vyšetřovatele usnadní spolupráci s dalšími specialisty, zejména pak se znalcem při vyžadování kriminalistických expertíz.

**

Kriminalistická počítačová expertíza při dokazování v trestním řízení podle [110] představuje zkoumání výpočetní a organizační techniky, a to jak technických, tak i programových a jiných prostředků, které s tím bezprostředně souvisejí. V kriminalistické počítačové expertize se vychází z poznatků řady vědních specializací, zejména kybernetiky, informatiky, elektroniky a dalších oborů. *Smyslem kriminalistické počítačové expertízy* je

-zjišťování technických parametrů zkoumané techniky,

-zkoumání informací uložených na záznamových médiích.

Především se zkoumají

-technické prostředky, druh, typ, možnosti, osazení jednotlivými prvky a jejich základní charakteristiky;

-neoprávněné zásahy do technických prostředků, zejména poruchy a důsledky vzniklé těmito zásahy;

-záznamová média; zjišťují se uložené nebo smazané soubory, jiné dochované informace, vytvářejí se identické kopie zjištěných souborů a dochovaných informací pro další potřeby, hlavně daňového, grafického a jiného zkoumání např. též v oboru fono- a video-techniky pro usnadnění práce orgánů činných v trestním řízení; vše při současném zjišťování možných souvislostí, které mohou vyplynout ze zkoumaných objektů;

-soubory a jejich uspořádání; zjišťuje se, jak jsou soubory na záznamovém médiu vytvořeny, časový sled vytváření souborů a další souvislosti vyplývající z organizace souborů na záznamovém médiu;

-programové produkty, porušování autorských práv při softwarovém pirátství a plagiátorství;

-neoprávněné zásahy do automatizovaných informačních systémů, užití programů nepatřících do vybavení daného systému, neoprávněné změny v užívaných programech v rámci daného systému, realizace neoprávněných úkonů a operací se vstupními nebo výstupními daty, případně s užívanými pomocnými datovými soubory, je-li podezření ze spáchání trestného činu.

V praxi na sebe obvykle jednotlivé druhy expertíz navazují a jejich použití je proto závislé nejen na zkoumaných předmětech, ale také na otázkách, které mají být zodpovězeny.

Expertní zkoumání. Složitost problematiky výpočetní a organizační techniky, se kterou se orgány činné v trestním řízení setkávají při posuzování různých protiprávních činností, vyžaduje použití specifických metod vyhledávání, zajišťování, zkoumání a vyhodnocování počítačových kriminalistických stop. U těchto stop nás zajímá nejen jejich technická hodnota potřebná k úspěšnému procesu kriminalistické identifikace, ale i jejich taktická hodnota, která je velmi významná z hlediska určení způsobu spáchání konkrétní kriminalisticky relevantní události. Úspěšnost celého tohoto procesu závisí na technickém vybavení a na důkladnosti ohledání místa této události související s výpočetní technikou. Dříve než k těmto úkonům dojde, je nutná dokonalá příprava, spočívající v ujasnění základních otázek, tj. jakého cíle má být dosaženo, jaké úkony se budou provádět, v čem úkony budou spočívat, v jakém prostředí se úkony budou provádět, na jaké technice a za použití jakého programového vybavení se budou úkony realizovat. To vše je důležité pro další *expertní zkoumání.* Podle autorů sdělení [105], kriminalistická počítačová expertíza

-zkoumá způsoby, důsledky a příčiny programového nebo technického zneužití nebo napadení prostředků výpočetní techniky v rozsahu zjišťování manipulace s daty, neoprávněných zásahů do programového vybavení, do technického vybavení, zjišťování případů softwarového pirátství, softwarového plagiátorství a porušování softwarových autorských práv;

-analyzuje obsahy paměťových médií výpočetní a organizační techniky;

-poskytuje konzultace orgánům činným v trestním řízení před zahájením vlastních procesních úkonů a zajišťuje konzultativní účast při jednotlivých kriminalistických úkonech.

Aniž bychom chtěli zabíhat do příliš podrobných kriminalistických aspektů, lze říci, že ve všech případech počítačové kriminality v procesu odhalování, vyšetřování a dokazování trestné činnosti je třeba postupovat cílevědomě, se znalostí věci, uvážlivě a současně bez zbytečných průtahů. Pachatelé jsou totiž většinou vysoce kvalifikovaní, s hlubokou znalostí možností a tajů výpočetních systémů. Jimi používané metody jsou obvykle dosti složité a komplikované. Těmto skutečnostem odpovídá i náročnost zajišťování potřebných stop trestných činů. Zde nesmí být opominuto detailní naplánování jednotlivých činností včetně typování různých verzí objasňování.

Dosud byla při těchto úkonech zaznamenána pochybení spočívající v tom, že

-zajišťování nebylo realizováno v souladu s trestním řádem,

-zajišťování nebylo důsledné a úplné,

-zajišťování bylo uskutečněno poškozenou osobou nebo osobou, u níž proběhla prohlídka,

-zajišťování technických prostředků nebylo adekvátní; že např. byly předávány k prvotnímu zkoumání osobě, která není znalcem, čímž mohlo dojít nejen ke ztrátě možných „informačních“ stop, ale i k negativnímu ovlivnění závěrů případného následného znaleckého posudku.

V některých případech se nezkoumají originály z dané techniky, nýbrž kopie pořízené na jiných počítačích, dokonce takových, kde nelze vyloučit možnost zavirování nebo kde není znám technický stav odpovídajících mechanik.

Je-li orgánům činným v trestním řízení předem známo, že při připravovaných procesních úkonech a opatřeních se pravděpodobně setkají s výpočetní nebo organizační technikou (v jakékoliv formě vlastnictví), nutno se řídit specifickými zásadami, blíže k tomu viz [105]. V případech, kdy nelze - zejména při nebezpečí z prodlení - zajistit na prováděném úkonu účast znalce a předpokládá se pouze odborné zajištění počítačové nebo organizační techniky a médií, je nutné přizvat k těmto úkonům skutečného odborníka, tj. osobu „znalou“ problematiky. Nesmí jít ale o osobu, která je nějakým, byť i vzdáleným způsobem zainteresována na objasňovaném zločinu (hrozí otázka podjatosti).V neposlední řadě nutno pro předem vybrané specialisty pořádat odborné zdokonalování formou stáží, seminářů apod.

Zásady práce při zajišťování výpočetní techniky pro expertizní zkoumání lze podle autorů [105] koncentrovat do této podoby:

a)úloha znalé osoby spočívá především

-v kvalifikovaném zajištění a dokumentování stavu techniky v daném prostředí,

-v určení, co fotografovat nebo snímat videotechnikou,

-ve vypracování schémat zapojení, v určení záznamových médií, odborné literatury apod. pro případy vydání nebo odnětí věci ke znaleckému zkoumání,

-ve spolupráci při identifikaci zajišťovaných listinných materiálů, zvláště pak kupních smluv a smluv o užívání programů či software, licenčních ujednání k software, výpisů programů nebo jiných výstupů z tiskárny, různých druhů poznámek apod.;

b)se zajišťovanou technikou nebo médii zásadně nemanipulovat tak, aby vznikly úniky informací z paměťových medií; zejména se vyvarovat jakéhokoliv spouštění programů, orientačnímu zjišťování obsahů adresářů počítačů jejich spuštěním.

Jak uvádí pramen [105], zkoumání zajištěných technických prostředků a dalších předmětů mohou provádět pouze znalci (experti) v příslušném oboru. Jejich procesní postavení je dáno trestním řádem a zákonem o znalcích a tlumočnících. Orgán činný v trestním řízení je do procesu přibírá formou usnesení. Expertizní zkoumání naopak nelze požadovat na osobě „znalé“, neboť případná zjištění takovými osobami nemají procesní hodnotu a formu.

**

Spolupráce se znalci. Podle ustanovení §105 odst.1 trest.řádu rozhodne orgán činný v trestním řízení o přibrání znalce, je-li k objasnění skutečnosti důležité pro trestní řízení třeba odborných znalostí. Jak uvádí autor studie [110], to se vztahuje pouze na orgány činné v trestním řízení a platí pouze pro účely trestního řízení. V řízení před soudem o tom rozhoduje předseda senátu. Toto ustanovení také umožňuje spokojit se v jednoduchých případech s potvrzením nebo odborným vyjádřením příslušného orgánu, o jejichž správnosti nejsou pochybnosti. V citované studii [110] autor naznačuje na jednoduchém příkladu možné znění požadavků vyšetřovatele ve formě dotazů na soudního znalce. Fiktivním předmětem zkoumání je zde elektronický diář patřící do kategorie organizační techniky, který mohl být např. zajištěn při domovní prohlídce u zadržené podezřelé osoby při vyšetřování kriminálního deliktu. Příklad vychází ze skutečnosti, že údaje z elektronického diáře mohou být důležitým zdrojem informací pro orgány činné v trestním řízení. O tom, zda zajištěný elektronický diář je způsobilý ke zkoumání, zejména je-li zjevně poškozen, rozhoduje pouze znalec. Autor [110] formuluje zde celkem sedm otázek pro znalce a vysvětluje podrobněji jejich vhodnost. Na dalších příkladech ukazuje naopak nepřípustnost dotazů. Poukazuje též na skutečnost, že možnosti zkoumání i poškozených technických nosičů informací se stále zdokonalují, takže otázky případného obnovení dat by měly být vždy předmětem konzultace se znalcem. A to i v případech zdánlivě bezvýchodných.

Poučení z kasuistiky je v boji s počítačovou kriminalitou rovněž důležitým faktorem. Ve studii [110] se hodnotí více než dvacet aktuálních případů, které byly v policejní evidenci uvedeny jako počítačová kriminalita. Podle [110] je četnost výskytu jednotlivých druhů počítačové kriminality nízká, a tím by se mohlo zdát, že počítačová kriminalita není příliš rozšířena. Nutno však uvážit, že téměř všechny její formy jsou ve značném rozsahu latentní. Odhalování počítačových deliktů je obtížné jak z principiálních důvodů, tak i pro procesní složitost. Jejich kvalifikovaný postih vyžaduje hlubších speciálních znalostí. To se odráží nejen v akcích policie, ale i v práci ostatních orgánů činných v trestním řízení, včetně soudů.

Pachatelé této trestné činnosti jsou zpravidla dříve netrestáni, požívají často u zaměstnavatelů dobré pověsti, obvykle byli zaměstnáni u podniku déle, znali jeho chod a zavedený systém zpracování informací. Mezi pachatele počítačové trestné činnosti patří lidé s různou profesí. Základním motivem většiny pachatelů v analyzovaných speciálních případech bylo osobní obohacení a zisk. Analýza finančních ztrát však ukazuje, že škody jimi způsobené se pohybují od několika desítek tisíc do několika miliónů korun. Což proti jiným případům současné hospodářské (podnikatelské) kriminality není mnoho.

Jinak k historii zkušeností s počítačovou kriminalitou autor [110] připomíná, že v tehdejším Československu byly registrovány první případy počítačové kriminality již v sedmdesátých letech. Šlo např. o úmyslnou trestnou činnost při počítačovém zpracování důchodů v *Úřadu důchodového zabezpečení v Praze*, která způsobila několikaměsíční ochromení veškerého provozu zpracování a výplat důchodů na celém našem území, dále pak o finanční machinace při zpracování mezd ve válcovnách závodu *Poldi Kladno*, jejichž výsledkem byly celkové ztráty vyšší než 200 000 Kčs. V té době velmi omezená část laické, ale i odborné veřejnosti byla případy doslova šokována. Došlo ke zhroucení obecného názoru, že práce na vysoké odborné a technické úrovni, využívající výpočetní techniky, je velmi přesná, bez možných chyb a nepravostí. V osmdesátých letech byly zaznamenány a tehdejšími bezpečnostními složkami rozpracovány další případy počítačové kriminality. Již v té době byly podobné případy zahrnuty do oblasti hospodářské kriminality a jako takové byly statisticky dále registrovány. Autor [110] uzavírá, že z výše uvedených myšlenek a názorů vyplývá, že odhalovat jevy nebo činy počítačové kriminality vyžaduje týmovou práci specialistů. Nelze požadovat po každém subjektu orgánů činných v trestním řízení, aby ovládal veškeré detaily této složité problematiky, i když bude sám dobře s výpočetní technologií seznámen a bude mít i jistou praxi v ovládání personálních počítačů, což je samozřejmě velmi výhodné. V takovém případě se bude určitě lépe orientovat při odhalování, objasňování i právní kvalifikaci a zejména při spolupráci s dalšími specialisty. Pro policistu je důležitá znalost možností a způsobů jednání pachatelů v této oblasti kriminality, včetně důsledků jejich činností. Vzhledem k tomu, že policejní orgány operují v první linii ve styku s kriminálním prostředím, jsou onou bezprostřední silou, která vede boj se zločinností a usměrňuje ho. Zvyšování kvalifikace v této oblasti je nezbytným předpokladem úspěchů policie, zejména, když si uvědomíme trendy rozvoje informatiky, rozšiřování počítačových sítí, bouřlivý rozvoj počítačové techniky, softwarového vybavení apod.

Softwarové odvětví očekává, že po roce 2000 bude stále více software využíváno přes Internet a lokální sítě než jiným způsobem. Dojde tak k novým vztahům adekvátním této nové skutečnosti, i když principy ochrany autorských práv a další podmínky práce s informační technologií zůstanou pravděpodobně po určitou dobu neměnné. To může být zdrojem určitých dalších obtíží v boji s počítačovou kriminalitou.

K nebezpečí tzv. čtvrté světové války počítačových sítí. Důležitým faktorem prevence zneužívání počítačových sítí v nadnárodním pojetí je vybudování efektivního programu fungování jednotné systemizované obsluhy podle zvláštních pravidel, tzv. *Oranžové knihy*. Na

různých klíčových uzlech síťových magistrál by toto systémové opatření umožňovalo vybudovat efektivní struktury agentur působících proti zneužívání toků informací organizovanými zločinci. Je to velmi aktuální problematika zvláště dnes, kdy určité organizované skupiny asiatských mafií propagují plán (podle materiálu [78] tzv. iniciativa „šikmookých“) na vytvoření specifické velmoci *Spojených států asijských (SSA)*. Hlavním městem SSA se má stát Abakan nejen pro etnické složení obyvatelstva převážně mongolského typu žijícího v tomto městě, ale i pro terénní předpoklady pro výstavbu. Mírné podnebí podél sibiřské magistrály umožňuje zde navíc usadit milióny čínských zemědělců a vytvořit zde základnu průmyslu SSA. Jeden z důležitých předpokladů spočívá prý v tom, že státní administrativa bude realizována smluvním ruským jazykem. V souvislosti s tím, jak uvádí [78], jsou na asijské půdě zkoumány možnosti implementace virů do počítačových soustav cizích zemí. Podle osobního dohadu jistého cizince budou objektem zamýšleného nasazení počítačových virů asi Spojené státy. V evropských zemích se zatím s širokým „využitím“ virů nepočítá, protože vstupy do počítačových systémů jsou většinou zajištěny přes evropské pobočky japonských firem.

**

Výchova uživatelů výpočetní techniky ke zvýšení úrovně právního vědomí je rovněž velmi důležitým faktorem prevence. Díky pochopení vedoucích činitelů resortu školství, na některých našich školách jsou pořádány přednášky nebo i ucelené kursy týkající se výchovy ve zmíněném směru. Jako příklad uveďme kurs *počítačového a informatického práva*, realizovaného na *Vysoké škole ekonomické v Praze*. Předmět je pro speciálně orientované frekventanty povinný, pro další pak pouze volitelný. Podle schválené osnovy lze ho považovat za příkladné řešení i pro posluchače s jiným než ekonomickým zaměřením. Zahrnuje

-přehled jednotlivých právních forem ochrany počítačových programů a jejich vývoj ve světě a v České republice;

-způsoby ochrany počítačových programů a jejich neúspěch;

-aspekty autorskoprávní ochrany počítačových programů a databází u nás i ve světě, včetně konkrétních právních případů;

-pojednání o mezinárodních úmluvách v oblasti autorského práva s ohledem na software;

-rozbor směrnic *Evropského Společenství* o právní ochraně počítačových programů, pronájmu a půjčování autorských děl, obchodním tajemství, o nekalé soutěži a právní ochraně dat i dalších informací v rámci jejího postihu;

-informace o právní ochraně software pomocí patentů a užitných vzorů, včetně konkrétních právních případů.

Dále pojednává o zlepšovacích návrzích, průmyslových vzorech, topografii polovodičových výrobků, ochranných známkách, obchodních jménech, o připravovaném zákonu o datové inspekci, o právní ochraně osobnosti a osobních údajů v informačních systémech v České republice, o konvencích *Rady Evropy*, o státním informačním systému, registru obyvatel, o směrnicích týkajících se právní ochrany databází, osobních údajů, o elektronickém copyrightu, o právních aspektech Internetu, o smlouvách v oblasti pořizování a

úprav hardware, software a periferní techniky, o právních aspektech elektronického obchodu, systémové integrace, licenčních smlouvách a antimonopolním právu.

Rovněž zahrnuje problematiku právních úkonů formou výpočetní techniky, elektronických podpisů, kódování a dále právní otázky toků dat přes hranice, úpravy telekomunikací, vztahů k organizacím spojů a radiového přenosu dat. Kurs je v závěru orientován též k základům počítačové kriminality, např. k dokazování deliktů ve sféře informační technologie se zdůrazněním právní odpovědnosti za systémy řízení a systémy pro podporu rozhodování.

Funkce výchovných a informativních seminářů hraje též nezanedbatelnou roli v systému prevence počítačové kriminality. V této oblasti působí pozitivně např. *Sekce ochrany dat a počítačové kriminality Společnosti pro kriminalistiku.* Jako příklad lze uvést řešení problémů zneužívání platebních karet. Autor příspěvku [89] zdůrazňuje, že naše dosavadní představa o náplni seminářů vychází z obecných požadavků na rámcovou, ale i specializovanou znalost problematiky počítačové kriminality. Z tohoto pohledu se prozatím tématicky rozdělují semináře na dvě části, obecnou, vysvětlující základní pojmy a rozsah problematiky a specializovanou, kde by byly diskutovány problémy v přijatelném rozsahu a hloubce. Například specializovaná část zmíněné problematiky zneužívání platebních karet může obsahovat

-otázky užívání, ochrany a zneužití magnetických karet vůbec,

-otázky specializovaných karet, jako např. *smart cards* apod.,

-otázky týkající se přehledu o aktivitách a vývojových tendencích firmy *BULL*,

-otázky provozu bankomatů, možnosti jejich zneužití z pohledu počítačové kriminality,

-otázky finanční kriminality a podvodů páchaných různými typy platebních karet,

-otázky trestněprávní problematiky.

I aktivní účast přednášejících na seminářích přispívá k jejich růstu, protože v diskusních situacích si mohou utřídit, precizovat či korigovat své znalosti. Vydáním sborníku pak mohou být poznatky šířeny i pro všechny další zájemce nejen z řad policie, státních zastupitelství a soudů.

9.5. Ochrana a vynucování autorských práv na software v Evropě

Ochrana autorských práv, Softwarová direktiva Evropské rady. Po mnohaleté debatě odborníků a zákonodárců o nejvhodnějších způsobech zákonné ochrany software dala v Evropě na tuto otázku konečnou odpověď *Softwarová direktiva Evropské rady* přijatá v roce 1991. Tvůrci konceptu Direktivy vycházeli z existence mezinárodních pravidel upravujících autorská práva, která se v praxi ukázala jako velmi užitečná a vyslovili předpoklad, že autorská práva jsou nejpředvídatelnějším, nejkonzistentnějším a nejefektivnějším základem pro zákonnou ochranu software v celoevropském kontextu. Tímto způsobem Direktiva rovněž

potvrdila volbu mnoha evropských zemí, v nichž zákonodárci a soudci zkonstruovali ochranu software na základě autorských práv.

Direktiva rovněž vyřešila spor mezi držiteli práv na software, který se týkal rozsahu užití software odvozeného z podrobného rozpracování výhradních práv držitelů práv na software s určitými speciálně vymezenými a omezujícími výjimkami, které se týkají uživatelů software. Nejdůležitější články Softwarové direktivy Evropské rady, které vyústily do typických akcí BSA zaměřených na vynucování autorských práv, jsou tyto:

1. Ochrana autorských práv - Článek l, kapitola 1 chrání počítačové programy „na základě autorských práv, stejně jako literární díla, tak jak jsou chápána Bernskou konvencí o ochraně literárních a uměleckých děl". Dokonce i v zemích, kde soudní orgány uznaly, že softwarová díla jsou implicitně chráněna národním právem, například v Portugalsku, narušitelé autorských práv rutinně shromažďovali aplikace s argumentací, že software není chráněn zákonem. To, že v roce 1994 v Portugalsku vstoupila v platnost Softwarová direktiva Evropské rady, nadobro vyřešilo tento problém.

2. *Originalita* - Článek l, kapitola 3 chrání počítačový program „jestliže je původní v tom smyslu, že jde o vlastní intelektuální výtvor autora. Pro určení toho, zda je tento výtvor hodný ochrany, nebudou používána žádná další kritéria". Právnicky myslící komentátor souhlasí s Direktivou, že úmyslem této normy originality je vytvoření minimální normy pro ochranu autorských práv, která by měla chránit většinu softwarových děl (s výjimkou totálních kopií) a měla by předcházet potřebě toho, aby držitelé práv prověřovali kvalitu nebo kreativitu svých konkrétních softwarových děl v souvislosti s narušiteli autorských práv. Hlavní efekt této normy původnosti byl pocítěn v Německu, kde Nejvyšší federální soudní dvůr ustoupil od pravidel platících v období před Direktivou, která poskytovala ochranu pouze 20% až 30% softwarových prací, nebo jinak pouze „nadprůměrným" dílům, viz [49].

3. Omezené a zvláštní výjimky pro užívání bez souhlasu - Články 5 a 6 ustanovují, že je uživatelům povoleno, aby bez souhlasu držitele autorských práv zhotovili kopii pro opravy chyb, aby zhotovili záložní nebo náhradní kopii pro případ nutného přeinstalování či archivování, kopii pro studium činnosti programu nebo pro dosažení schopnosti spolupracovat s jiným nezávisle vytvořeným počítačovým programem. Na rozdíl od platného českého práva Direktiva nerozeznává výjimku pro „osobní potřebu" nebo „osobní užití" v souvislosti s použitím softwaru bez souhlasu držitele práv. Mnoho evropských států zjistilo, že tyto výjimky implikují zhotovování nebo distribuování velkého množství neautorizovaných kopií software pro individuální užití při podnikatelské činnosti. Tyto státy pozměnily své zákony o autorských právech v tom smyslu, že pro počítačový software neexistuje výjimka, která se týká „osobního užití".

4. Přiměřená soudní opatření - členské státy Evropské unie se musí řídit Článkem 7, podle kterého nutno uplatnit „přiměřená soudní opatření" proti těm, kteří uvedli do oběhu nebo disponovali pro komerční účely nelegálními (narušitelskými) kopiemi počítačových programů. Narušitelské kopie podléhají konfiskaci. Povětšině spíše obecnější formulace Softwarové direktivy Evropské rady mají za následek, že občansko právní i soudní sankce se v různých evropských zemích navzájem liší. Občanskoprávní sankce vykazují tendenci být dosti mírné a ostatní soudní sankce i tehdy, jsou-li vysoké, jsou zřídka vynucovány.

Vynucováni autorských práv. Softwarová direktiva Evropské rady představuje hlavní výsledek boje proti softwarovému pirátství. Významně velký rozsah softwarového pirátství však ukazuje, že držitelé práv na software jsou stále poškozováni v důsledku těžkostí spojených s vynucováním jejich práv. Aby byl tento problém eliminován, jsou potřebné jasné a efektivní vymáhací postupy a sankce, zvláště z pozic občanskoprávních. Normy pro odhad kompenzačního odškodnění v občanskoprávním řízení nejsou například vyjasněny ve většině evropských zemí, protože existuje velmi málo soudních rozhodnutí vydaných v souvislosti s akcemi narušujícími autorská práva na software. Poměrně obecnou formulací článku o přiměřených soudních opatřeních Softwarové direktivy Evropské rady absence jasných norem bohužel vyřešena není.

GATT TRIPS - předpisy pro prosazování specifik systémů národních práv v oblasti softwarového vlastnictví - by však měly jít mnohem dále na cestě prosazování či posilování evropských zákonů týkajících se software a dalších problémů informačního práva. Na rozdíl od Článku 7 Softwarové direktivy Evropské rady, *TRIPS* poskytují podrobné a specifické návody pro členy *GATT* ve věci osvojení postupů a sankcí při prosazování vlastního národního práva. Zde je stručný výčet těchto aspektů s vysvětlením, proč je pro držitele software každý z nich důležitý:

1. Prohlídky v občanském sektoru „Inaudita Altera Parte“. Předpisy GATT TRIPS vyžadují, aby soudní orgány byly oprávněné přijímat prozatímní opatření „inaudita altera parte“ taková, aby mohly být shromážděny odpovídající důkazy a aby jejich záznam byl chráněn. Držitelé práv na software potřebují legalizovat nenadálé prohlídky u organizovaných koncových uživatelů, které by umožnily získat přesvědčivé důkazy o softwarovém pirátství. Lze to zdůvodnit výjimečností software mezi díly chráněnými autorským právem, spočívající v tom, že software může být kopírován i zničen během několika minut či dokonce vteřin. Zkušenosti BSA z Evropy naneštěstí ukazují, že zaměstnanci často zničí důkazy o nelegálním kopírování software, jestliže jsou nějakým způsobem před akcí předem varováni. Ve Velké Británii například tyto nenadálé prohlídky -organizované občanskými soudy, nad nimiž dohlíželi soukromí právníci a které realizovali počítačoví odborníci- byly povoleny od roku 1976. Většina dalších států západní Evropy rovněž využívá tyto prostředky v občanskoprávním řízení ve prospěch držitelů práv na intelektuální vlastnictví. Naproti tomu v Rakousku, Německu, Maďarsku a v Polsku je pouze policie oprávněna uskutečňovat zmíněné nenadálé prohlídky. Takováto opatření v občanskoprávním řízení jsou v České republice teoreticky možná, avšak jejich využití v praxi je obtížné. V důsledku toho se BSA v České republice obrátila na orgány činné v trestněprávním řízení, aby získala adekvátní důkazy o nezákonném užívání software dokonce i v případech, které by se mohly zdát vhodnější pro postih v řízení občanskoprávním.

2. Občanskoprávní sankce. GATT TRIPS vyžadují, aby orgány justice byly oprávněny ukládat pokuty, které „odpovídají způsobeným škodám“, a které „vytvářejí zábrany pro budoucí přestupky“. Berou rovněž v úvahu „hrazení předem stanovených pokut“ v „přiměřených případech“. Téměř ve všech evropských státech jsou realizovatelné potřebné reformy, které by zajistily splnění těchto požadavků v případech narušení autorských práv na

software. Správná míra odškodného v souladu s platnými zákony je diskutovaným problémem při téměř všech zákonných akcích BSA, protože zákonná ustanovení zřídka dávají jasné návody a existuje málo precedentních soudních rozhodnutí. Narušitelé softwarových práv říkají, že by držitelům práv zaplatili z celkové prodejní ceny nelegální kopie pouze jejich omezený ušlý zisk, nebo pouze částku odpovídající snížené ceně nelegální kopie nebo pouze ztrátu zisku, který nastal po zhotovení nelegální kopie a před nákupem legální kopie. Všechny tyto teorie o odškodném mají jednu fatální vadu - narušitelé autorských práv na software platí na odškodném při akcích na ochranu zákona méně, něž by museli zaplatit za nákup legálních software. Aby bylo zajištěno, že narušitelé nebudou mít finanční motivaci pro výrobu nelegálních kopií, soudci by měli mít oprávnění nařizovat „platbu předem stanoveného odškodného“ v případech narušení softwarových práv. Jestliže zákonné opatření stanoví pevnou částku maloobchodní ceny za každou nelegální kopii, pak by suma měla být dostatečně vysoká na to, aby odstrašila narušitelskou společnost i další potenciální narušitelské společnosti od realizace nezákonných aktů v budoucnosti. Alternativně by mělo být definováno „přenechání zisku“ jako částky odpovídající poplatku za prodej licence, kterému se společnost vyhnula tím, že zhotovila nelegální kopii, místo aby si zakoupila původní program s licencí na jeho použití.

3. Zákonné poplatky a náklady. Předpisy GATT TRIPS rovněž opravňují národní justiční orgány „mít právo nařizovat narušitelům placení nákladů držitelů práv, které mohou zahrnovat i přiměřené poplatky obhájců“. V mnoha evropských zemích je obtížné kompenzovat více než jen malou část skutečných nákladů vynaložených na úspěšné akce vynucující občanská autorská práva. Evropské zákony upravující poskytování náhrad zákonných nákladů tyto náhrady obvykle omezují na určité typy zákonných akcí podle podílu uložených pokut nebo podle rozpisu zákonem stanovených poplatků za nelegální obchod. Pokud držitelé práv nedostávají plnou náhradu za zákonné poplatky a náklady, jsou vlastně penalizováni za občanskoprávní akce vynucujících jejich práva.

4. Trestněprávní odpovědnost. GATT TRIPS požadují, aby členské státy vyvozovaly trestně právní odpovědnost za pirátství proti autorským právům „která by byla dostatečná pro odstrašení a porovnatelná s úrovní trestních sankcí uplatňovaných v souvislosti se zločiny, jež jsou podobně závažné“. Mnoho evropských zemí - včetně Maďarska, Francie a Belgie - zavedlo nebo zvýšilo trestní sankce za trestné činy proti autorskému právu. Týká se to nedávno uplynulých let. V mnoha jiných státech jsou však skutečně ukládané tresty příliš nízké na to, aby omezily zisky realizované nelegálními překupníky software. Dokonce v Řecku, kde sazby odnětí svobody za trestné činy související s porušováním autorských práv dosahují až deseti let, dochází k soudním rozsudkům v těchto případech zřídka nebo k nim dokonce nedojde vůbec. Pro řešení daných problémů je povzbuzující skutečností, že byla vydána první soudní rozhodnutí proti překupníkům nelegálního software ve Španělsku a ve Velké Británii a lze doufat, že další případy budou následovat. Překupníci budou prodávat nelegální software do té doby, dokud soudy nezačnou zvyšovat úroveň sankcí a dokud nebude vydán větší počet soudních rozhodnutí. I když nutno zdůraznit, že pachatele odrazuje vždy spíše neodvratnost a bezprostřednost trestu než jeho výše.

5. Účinné postupy vynucování. Postupy vynucování v občanskoprávní i trestněprávní oblasti používané v souladu s normami GATT TRIPS musí být účinné, nikoli nežádoucím

způsobem komplikované, ani nákladné a musí zabraňovat nedefinovatelným zpožděním. Naneštěstí zkušenosti BSA z Evropy říkají, že narušitelé dělají co mohou, aby postupy co nejvíce zkomplikovali, prodražili a prodloužili. Občanskoprávní akce proti narušitelům autorských práv mohou trvat několik let, přičemž obžalovaní v těchto sporech zápasí s myšlenkou, zda je software chráněn autorskými právy, zda software držitelů práv je dostatečně původní, aby zasluhoval ochranu a bojují o výhodnou výši placených pokut. BSA například v Itálii dokončila mnoho občanskoprávních akcí v oblasti nelegální distribuce softwaru, na jejichž základě během plných tří let nebylo vydáno žádné rozhodnutí o odpovědnosti za přestupky! Pokud jde o trestní odpovědnost, vyšetřování inklinují k trvání po dobu několika měsíců, někdy i několika let, než je vzneseno obvinění z trestného činu. Tento zdlouhavý postup justice podněcuje narušitele autorských práv, aby pokračovali ve své trestné činnosti, místo toho aby legalizovali užívání svého software a zaplatili odpovídající náhradu. Jedno z řešení, které vede ke zjednodušení tohoto problému, spočívá ve vyjasnění základních pravidel, týkajících se na například norem pokutování, tak aby nedocházelo k mrhání časem justičních orgánů při hledání odpovědí na obvyklé otázky. Dalším možným řešením je vytvoření zvláštních oddělení občanských soudů a orgánů činných v trestním řízení, která budou specializována na problematiku autorských práv. Tím by zkušení soudci, policisté, státní zástupci či prokurátoři mohli efektivněji vykonávat své funkce.

Pokud v následujících několika letech dojde k dalšímu propracování postupů a nápravných opatření vyplývajících z ustanovení GATT TRIPS do národních zákonů, držitelé softwarových práv budou s větší pravděpodobností pozorovat rychlejší zpracování výsledků prohlídek, jejichž cílem je získání důkazního materiálu, a konečně zaznamenají i více mimosoudních řešení závěrů akcí proti narušitelům. Spolu s legislativní a justiční reformou v oblasti ochrany autorských práv dojde k růstu zábran softwarovému pirátství a sníží se zátěž evropských soudních systémů.

Lze předpokládat, že výsledkem silnějšího prosazování autorských práv bude

-zdravější evropský i mezinárodní softwarový průmysl,

-větší tok daňových prostředků plynoucí ze softwarového průmyslu směrem k národním vládám,

-rozvoj tvorby nových softwarových produktů, na které ostatní průmyslová odvětví spoléhají ve snaze o zvýšení růstu a produktivity jejich aktivit,

-nárůst zaměstnanosti.

**

Z pohledu boje s počítačovou či obecně informační kriminalitou by prevence i represe měla působit ve vzájemné jednotě. Pokud bychom chtěli dosáhnout vysoké efektivity, takovou součinnost nelze pojímat jako pouhé jednorázové, ryze účelové akce. Mělo by jít spíše o systematický, preventivní i vyhledávací proces. V nutných případech zakončený přiměřeným zákonným postihem s rysy bezprostřednosti a neodkladnosti.

10. Osobnost pachatele počítačové kriminality

Sestaveno převážně z pramenů: [11], [35], [36], [37], [38], [39], [40], [66], [76], [77], [98], [110], [133], [138], [142], [175], [185], [237].

10.1. Nové aspekty přístupu k osobnosti pachatele

Současné poměry sociální, ekonomické i politické ve světě i v České republice dávají přednost funkci trestního práva v oblasti sekundární a terciární prevence kriminality. Moderní projekty trestní politiky jsou charakteristické tendencemi k dekriminalizaci, depenalizaci, odklonu (diverzi), alternativním trestům a alternativním opatřením, což souvisí vedle snah o zefektivnění celého systému i se snahami o humanizaci trestní justice. Tím je podstatně ovlivněn přístup k osobnosti pachatele ve smyslu humánních principů.

Humanizace trestní justice předznamenala práci kongresu OSN o prevenci kriminality a zacházení s pachateli prakticky již od 1. kongresu, který stanovil *Standardní minimální pravidla pro zacházení s vězni*. Užití alternativních sankcí bylo doporučeno *Rezolucí 7. kongresu OSN o prevenci kriminality a zacházení s pachateli* v Miláně 1985. *Osmý kongres OSN*, konaný ve Vídni v roce 1988 a věnovaný prevenci kriminality a zacházení s pachateli, zdůraznil potíže s aplikací existujících standardů a směrnic v kodexech jednotlivých členských států. Důvody těchto obtíží byly shledány v nedostatku koordinace příslušných aktivit, nízkých finančních fondech, v nedostatečném přisouzení priority této závažné problematice i adekvátním lidským a profesním zdrojům a prostředkům a často i v nedostatku politické vůle a převládající apatie veřejnosti.

Alternativní přístup k pachatelům, problematika alternativních trestů a alternativních opatření je nepochybně jednou ze stěžejních tématik současné trestní politiky. Procesy společensko-ekonomických změn, nové a modernější pohledy na kriminalitu pachatele, smysl a cíl trestání, vyvolaly potřebu zavádět do systému trestně právních sankcí alternativní tresty a hledat další možnosti alternativních opatření místo klasického odsouzení pachatele. Kromě humanizace trestně právních prostředků je jejich smysl i v účinnější ochraně společnosti před pachateli trestných činů a v přizpůsobení sankčních systémů a procesních postupů novým společenským podmínkám. Hlavní důvody, pro které je nutno usilovat o rozšíření alternativních sankcí, nutno spatřovat v tom, že převýchova odsouzeného se vykonává v rámci společnosti, bez zpřetrhání jeho sociálních vazeb s prostředím ve kterém žije. Další jejich předností je, že umožňují podstatně vyšší individualizaci trestů s přihlédnutím k charakteru osobnosti jedince a jeho vlastností. Nelze ani pominout, že přinášejí podstatně menší finanční náklady na jejich výkon. Alternativní opatření nesporně napomáhají ke zrychlení trestního řízení a k jeho ekonomičnosti.

Do skupiny alternativ nespojených s odnětím svobody, které nezahrnují kontrolu nebo dohled, bývají řazeny peněžité tresty, náhrada škody, propadnutí věci, ztráta práv, odebrání určitého oprávnění a zákaz vykonávat zaměstnání nebo povolání, odklad trestu nebo jeho výkonu. Některé tyto alternativy mají spíše povahu sankce vedlejší než hlavní a jsou často kombinovány např. s náhradou škody nebo s podmíněným odsouzením. Samozřejmě, že principiálně jsou použitelné i v případech méně závažných deliktů páchaných ve spojitosti s počítači.

Odklon chápeme jako alternativu trestního řízení před soudem, kdy je upřednostněno neformální (mimosoudní) vyřízení trestní věci. Pod tento pojem zahrnujeme podmíněné zastavení trestního stíhání (§§ 307, 308 trest.řádu) a narovnání (§§ 309-314 trest.řádu). Institut narovnání se uplatňuje zejména v případech, kdy stát na trestním postihu pachatele nemá výrazný zájem, neboť trestný čin má spíše povahu sporu mezi obviněným a poškozeným. Základní podmínkou schválení narovnání je skutečnost, že obviněný zaplatí vzniklou škodu, resp. jinak odčiní újmu, způsobenou trestným činem. Podrobněji k tomu viz např. [133].

Souhrnně lze konstatovat, že v oblasti preventivní funkce trestního práva hraje roli vedle generální prevence (obecného zastrašování) v poslední době zvláště rozšiřující se oblast alternativních trestů a opatření i mimosoudní vyřízení věci (odklon). Je ovšem problematické nakolik lze prakticky uplatňovat tyto instituty vůči pachatelům počítačové kriminality. Nicméně nelze apriorně vyloučit existenci i méně závažných forem trestné činnosti páchané pomocí počítačů, kdy případné aplikace by byly možné.

Za podstatné pro boj s počítačovou kriminalitou z pohledu psychologie pachatele však považujeme aspekty spjaté s globálním klimatem změn trestní politiky. Celkově lze charakterizovat odborné poznatky o odstrašujícím účinku trestních sankcí, tj. generální prevence na pachatele tak, že páchání kriminality nejvíce snižuje zvýšená neodvratnost zatčení a rychlé potrestání pachatele, zatímco charakter trestních sankcí a výše sazeb mají na rozsahu kriminality relativně malý vliv. Je tomu tak pravděpodobně i proto, že většina populace nezná skutečnou výši trestních sankcí. Z těchto teoretických poznatků lze pro praxi dovodit, že každý odstrašující účinek musí spočívat na snahách systému trestní justice i společnosti o stálé zvyšování úrovně rizika postihu za trestnou činnost pro potencionálního pachatele především závažných trestných činů. Tedy neodvratnost a bezprostřednost trestu by měla být dominujícím aspektem v mysli počítačového pachatele. Zatím tomu tak v praxi ovšem zdaleka není. Uvidíme v dalším, že osobnost pachatele je dosud formována a ovládána poměrně širokou škálou jiných dominant.

Výzkum osobnosti pachatele počítačové kriminality. Dosavadní empirické výzkumy uskutečněné v místních podmínkách, viz [142], přinesly některé dílčí výsledky k názorům specialistů na počítačovou bezpečnost a k osobnosti potenciálních pachatelů počítačové kriminality. Na základě výsledků uvedené akce bylo konstatováno, že si správci sítí uvědomují svou odpovědnost za svěřené databáze, a z nich především za citlivé informace,

které někteří spravují. Uvědomují si závažnost případných deliktů spojených se zneužitím takových informací. Tomu však v řadě případů neodpovídá reálné zabezpečení proti neoprávněným průnikům a jiným útokům. Výzkum byl postaven jen na dotazníkové akci, takže při interpretaci výsledků nutno brát v úvahu nejméně čtyři roviny možného poznání, týkající se reality, jejího odrazu ve vědomí subjektů, názorů na realitu podmíněných tímto odrazem a konečně výpovědí subjektů k vytvořeným názorům. Je třeba mít neustále na zřeteli, že analýzou výsledků dotazníkových akcí nezkoumáme přímo realitu, ale především názory na ni prostřednictvím subjektů, kteří jsou ochotni vypovídat. Zejména u otázek choulostivého charakteru, jimiž dotazy na počítačovou bezpečnost či přímo kriminalitu jistě jsou, si nemůžeme být nikdy jisti, na které z uvedených hladin se pohybujeme. Výpovědi zúčastněných subjektů mohou být často i vědomě účelově zkreslené. Jak vyplynulo z odpovědí respondentů, spoléhá většina provozovatelů počítačových sítí na prostředky technického zabezpečení. A to ještě na ty, které jsou přímo implementovány výrobcem síťového software. Snaha o výrazné úpravy ve smyslu zlepšení pro tu kterou instituci podle místních podmínek nebyla registrována. Situace v oblasti uplatňování organizačních prostředků, jako např. monitorování práce uživatelů, i v oblasti personální politiky je obdobná. To vše pak nahrává potenciálním pachatelům počítačové kriminality též z řad vlastních zaměstnanců. Uskutečněný výzkum podle [142] vycházel z toho, že potenciálním pachatelem počítačové kriminality, nepřihlížíme-li k počítačové kriminalitě mzdových účetních, je pravděpodobně programátor. To však samo o sobě nedostačuje. Akcent by měl být kladen na zjištění, zda se programátor od ostatní populace liší také něčím jiným, než jenom tím, že odborně komunikuje s počítačem a ovládá ho. Pokud je něčím výlučným, je třeba jít dál a určit, zda mezi programátory existují další vzájemně se lišící skupiny, z nichž některá by mohla být považována za rizikovou z hlediska počítačové bezpečnosti. Na tyto skutečnosti nedávají zatím uskutečněná empirická šetření dostatečně průkaznou odpověď.

Nové formy metodologického přístupu k výzkumu osobnosti pachatele a k případné individuální predikci spočívají ve využití postupně rozvíjených metod zkoumání osobnosti, které jsou založeny na principech chování systémů. Zde hrají důležitou roli pojmy perseverance a stability chování. Jak již bylo řečeno v souvislosti s dokazováním autorství programů, perseverancí rozumíme tíhnutí jedince, případně systému jedinců k určitému stereotypu chování, čili k určité charakterické stabilitě projevů. Jde v podstatě o zobecnění teorie *kriminální perseverance,* tak jak o ní pojednává práce [11]. Zde mohou najít zajímavé a užitečné uplatnění jak elementární přístupy, tak i náročnější multivariační metody. Praktické poznatky v tomto směru získané lze uplatnit nejen k tzv. *individuální predikci* kriminálního chování určité osoby a v návaznosti na to k případnému přijetí odpovídajících preventivních opatření, ale i v kriminalistické praxi k vytypování pachatele, který vtělil svůj „rukopis„ do stylu spáchání trestného činu. O individuální predikci hovoříme v souvislosti s předvídáním (anticipací) chování dané osoby, např. potenciálního pachatele, recidivisty, atp. Je zřejmé, že k matematické formulaci a zpracování takovéto problematiky jsou vhodné především ty modely, jejichž prvky jsou náhodné veličiny, tedy *modely stochastické* (pravděpodobnostní). Deterministické, tj. nestochastické pojetí nevede k úspěchu zpravidla pro mnohost, nepostižitelnost a náhodnost těch vlivů, které posléze podstatně ovlivní chování pachatele.

Stochastické modely umožňují upřesňovat pravděpodobnostní závěry v závislosti na hloubce empirického poznání příslušného problému. V tom tkví jejich síla a význam. V rámci těchto modelů jsou zkoumány určité znaky osobnosti pachatele nebo způsoby jím páchaných trestných činů v nějakém časovém intervalu a lokalitě. Zkoumání je zaměřeno k *variabilitě* znaků nabývajících svých alternativních variant. Pokud je variabilita malá nebo dokonce nulová, příslušný znak je pro danou osobu určující, neboť osoba preferuje některou z jeho variant více než jinou. Navíc, není-li takový znak typický pro prokazatelně nedelinkventní osobu, může být zahrnut do tzv. *predikčního nástroje*, s jehož pomocí lze sestavit individuální predikci. Jde-li o způsoby opakovaného páchání trestných činů, je malá variabilita známkou tíhnutí recidivisty k určitému stálému stylu. Tehdy mluvíme o *kriminální perseveranci*. Demonstrace celkového konceptu teorie kriminální perseverance a jejího využití byla uskutečněna na databázích recidivistů v Německu koncem osmdesátých let. Tyto výzkumy přinesly řadu cenných poznatků a podtrhly užitečnost matematicko-statistického pojetí daného problému. Výsledky bádání zaměřené výlučně ke kriminalistickým účelům podává studie [11]. Autoři si zřejmě neuvědomili širší dosah jejich teorie a zejména možnost jejího adekvátního zobecnění v systémovém pojetí analýz chování. Pokus o zobecnění byl uskutečněn v práci [138]. Užitečnost či hodnota perseverance pro kriminalistickou praxi je v podstatě dána odlišností chování recidivisty od chování „průměrného pachatele„. Tento jev bývá v literatuře nazýván *signifikancí* chování pachatele. Je-li chování recidivisty výrazně signifikantní, tím spíše může být podle typických znaků identifikován a odhalen. Určitá obdoba platí též pro identifikaci jakýchkoliv systémů a jejich chování. „Průměrnost„ (potenciálního) pachatele se posuzuje vždy *relativně* vůči větší či menší skupině jiných (potenciálně) trestně činných osob. Je zřejmé, že pojmy a přístupy hodnocení užitečnosti z kriminalistické praxe lze přenést na hodnocení vzájemných vztahů systémů. Místo o pojmu „průměrný pachatel„ lze hovořit o „representantu„ z třídy nějakých výchozích modelů; místo míry užitečnosti perseverance lze brát v úvahu míru identifikovatelnosti modelu vůči representantu z hlediska stability jeho chování atp. Zatím však toto zobecnění nebylo hlouběji propracováno, ani v praxi uplatněno. Rozhodně však skýtá široké možnosti uplatnění nových účinných přístupů nejen při zkoumání osobnosti počítačového pachatele, nýbrž i systému prevence či represe informační kriminality vůbec.

Moderní přístup k osobnosti pachatele počítačové kriminality nutno podmínit dobrou znalostí nových forem kriminality páchané prostřednictvím počítačů. Na tuto skutečnost upozorňuje autor pojednání [175] s odkazem na studii [66], která je věnována novým formám počítačové kriminality s ohledem na specifika osobnosti pachatelů. Zabývá se kriminálními strukturami, které pomocí známých metod a prostředků nelze buď vůbec odhalit nebo jen s určitými nemalými problémy. I když detaily výkladu se týkají problematiky německého prostředí, lze je akceptovat jako základ určitého obecného pojetí. Diskuse o výměně dat, obrazů, filmů a hudby pomocí počítačů se totiž týká téměř všech oblastí života v celosvětovém záběru, doslova od mezinárodních jednání a veletrhů přes hospodářské zprávy až po nabídky zboží pomocí katalogů obchodních domů. Pro tento nový svět médií se již vžil pojem „multimédia„. Multimediální trh prožívá nebývalý rozvoj a podle [66] zaznamenává

růst obratu o 15-25 % ročně. Je to rozsáhlý obchod s velkou budoucností. Jen v Německu dnes používá asi 1 mil. domácností *on-line* služby, asi 1,5 mil. multimediální personální počítače a 14 mil. kabelový systém. Žijeme v době digitalizace, kdy ve světě informací padají hranice zemí a kontinentů. Vyvíjí se druh umělého paralelního světa, který lze označit jako *kybernetický prostor (cyberspace)*. Je to dosud nezávazně definovaný pojem z literatury science-fiction, který vyjadřuje druh tzv. *virtuálního počítačového životního prostoru*. I když člověku může přinést hodně pozitivního, existuje však také rubová strana tohoto vývoje - aktivace dosud latentní počítačové kriminality resp. její vznik v důsledku speciálních technologických zdokonalení počítačů. Nový „virtuální svět„ se tedy stává kriminogenním faktorem, objevují se nové formy počítačové kriminality, nové aspekty osobnosti pachatelů, a je nezbytné zkoumat jejich účinky z kriminologického i kriminalistického a samozřejmě též právního pohledu.

**

Internet a pachatelé počítačové kriminality. Víme již, že Internetem se obecně rozumí celosvětové dynamické sjednocení množství síťových zařízení a počítačů. Jako synonym se používají také pojmy *datová dálnice*, či *síť sítí* apod. Internet reflektuje jednak potlačený vliv států, jednak světový charakter tohoto média. Internet zahrnuje podle [66] více jak 60 tisíc vnitrostátních a mezinárodních sítí, které jsou vzájemně pojeny asi 30 mil. (podle jiných zdrojů až 60 mil.) počítačů. Počet pravidelných účastníků Internetu autor [66] odhaduje na 35-40 mil. Ročně je odesláno a přijato obrovské množství digitálních zpráv. Podle [66] asi 1 miliarda, avšak zcela určitě jsou tato čísla dnes již dávno překonána. Internet byl vyvinut na počátku šedesátých let americkým ministerstvem obrany jako „dítě studené války„ a měl spojovat jednotlivá vládní místa v USA pro případ nukleárním útoku. Dnes je Internet nejvolnějším a nejméně kontrolovaným médiem, neboť nemá žádnou organizační, finanční, politickou nebo operační správu. Nikdo není za celkový komplex odpovědný, což souvisí s mezinárodním charakterem tohoto fenoménu. A to je ideální živná půda pro kriminální úvahy a jednání. Například *neonacisté* rozšiřují neomezeně svá nehorázná poselství. Objevují se i návody na zhotovení výbušných systémů (bomb) nebo k míchání nitroglycerinu. Je rozšiřována pornografie všeho druhu, a to i dialogy a obrázky o sexu mezi dětmi a zvířaty, o znásilnění dětí, o sexu s mrtvými dětmi apod. Zejména děti jsou podněcovány k prostituci nebo ke svému prodeji pedofilům, pederastům nebo jiným úchylným osobám. Velice se rozšiřují podvody v souvislosti s objednávkami zboží, obchody s akciemi, zjišťují se předem rodinné a finanční poměry pro efektivitu vloupání, rozšiřuje se sexuální obtěžování zejména po zavedení telefonů s obrazem, rozšiřuje se nekalá soutěž, softwarové pirátství. Při trestních jednáních padají jakékoli zábrany, neboť pachatel a oběť nepřicházejí do bezprostředního verbálního nebo vizuálního kontaktu. Vyhlídky na zisk (kořist) jsou velké, riziko odhalení malé. To vše působí na osobnost pachatele a utváří jeho specifické rysy.

Internet jako prostředek pomsty. Podle zdroje ČTK z roku 1999, jistý bývalý agent tajné služby *MI6* dal britské vládě pocítit, jak nebezpečná je moc Internetu a jak zrádná může být světová informační pavučina. Zmíněný agent upadl do podezření, že zveřejnil na americké

webové stránce jména více než stovky členů *Tajné zpravodajské služby (SIS)*, britské rozvědky, dříve známé jako *MI6*. Britská vláda proto vyvinula prostřednictvím soudu nátlak na média, aby obsah stránky nepublikovala, a v tomto sporu uspěla. Dotyčný agent vstoupil do *MI6* v roce 1991 a působil služebně v Bosně, v Moskvě a na Blízkém východě. Po čtyřech letech byl však propuštěn, protože *MI6* přestala mít o jeho služby zájem. V roce 1997 byl zatčen, jelikož se vláda obávala, že odjede do Austrálie, kde chtěl zveřejnit knihu o praktikách tajné služby. Agent strávil šest měsíců ve vězení a potom dál pokračoval ve mstě vůči svému bývalému zaměstnavateli. Podle některých pramenů šlo o jedno z největších porušení britské národní bezpečnosti za uplynulých několik let. Vládní činitelé jsou znepokojeni zejména tím, že britským agentům nyní hrozí nebezpečí od protivníků ze znepřátelených zemí, případně též od teroristů. O dalším řešení situace však zdroj již neříká nic.

Digitální manipulace s obrazem a virtuální realita. Na počítači lze části reálného obrazu přesunout nebo nahradit jinými tak, že za normálních okolností není možno místa spojení bezprostředně rozeznat, zejména použije-li se méně kvalitního papíru, tisku apod. Jak uvádí autor [175] takové obrazy v rukou zločinců mohou mít nedozírné následky. Oběť vydírání sice pozná nepravost obrazu, ale nedokáže ji prokázat. Každý žárlivý manžel nezapochybuje o pravosti obrazu, který ukazuje jeho manželku v náručí milence. Věří tomu, co vidí. Kdo tedy může v době digitalizace a kybernetické virtuální reality garantovat věrohodnost obrazů pořízených počítačem. Imitace je nerozlišitelná, což může mít fatální následky v soudním řízení. To, co na monitoru počítače vidíme a co je v počítači uchováno, představuje vlastní skutečnost, kterou obecně chápeme jako simulaci či model jiné skutečnosti, jež existuje mimo počítač. Jsou-li tato data tak změněna, že nemají žádný vztah k realitě (jsou tedy nereálná), pak to znamená počátek *virtuální reality*. Tento pojem, pro nějž neexistuje dosud závazná definice, je jakousi analogií techniky, pomocí níž člověk může být v interakci s trojrozměrným umělým světem, který sám vyprojektoval a počítačem vytvořil. Ve vytvořeném virtuálním prostoru se mohou uživatelé pomocí sítí setkat a komunikovat. V šedesátých letech byla počítačová simulace využívána k vojenským účelům, dnes je využívána nejen na úseku průmyslu, vzdělávání, architektury, medicíny aj., ale bohužel i zločinu. Zanechávají-li originální zločiny vždy stopy, pak v umělém světě bychom je většinou marně hledali. Virtuální zločin se tak stává velmi těžko pochytitelný.

**

Nový profil pachatele. Není tomu tak dávno, kdy se počítačové delikty považovaly za kriminalitu středních a vyšších vrstev, za kriminalitu podivínů a specialistů. Tato kriminalita nebyla považována za originální zločin, nebyla příliš zjevná, nebyla na očích veřejnosti a zdála se být i méně nebezpečná. I dnes platí, že počítačové delikty vyžadují vysokou schopnost přizpůsobivosti, odpovídající „know-how„ a jistou míru inteligence. V důsledku dalších a dalších technologických zdokonalení je činnost pachatelů spíše ulehčována. V počítačové kriminalitě nenajdeme jeden typ pachatele, ale množství určitých, často velmi specializovaných typů. Podle [175] nelze přehlížet to, že některá počítačová kriminalita může

mít blízko k organizované kriminalitě, neboť vykazuje její základní znaky, jako např. větší počet zúčastněných osob, jejich hierarchizaci, organizovanost, délku páchání, trvale cílenou činnost, využití moderní techniky, orientaci na zisk ap. Neřadí-li se dosud počítačová kriminalita k masové kriminalitě, bude zřejmě záhy nutno toto stanovisko revidovat. Tím spíše, že poroste rozsah soukromých a komerčních personálních počítačů využívaných formou tzv. *„home banking„*. Autor [66] vidí problém v globálních sítích dat v odpovědnosti provozovatelů systémů. Za nevyjasněné považuje to, zda a v jakém rozsahu mohou či mají být národní orgány trestního stíhání činné též v zahraničí. Domnívá se, že by měla být přijata adekvátní mezinárodní dohoda, která by působila i preventivně v kladném smyslu na utváření osobnosti pachatele, např. tím, že by ho odradila od nekalé činnosti, jež dosud nemohla být podle zákona stíhána. Neexistují kriminalistické postupy, kterými by bylo možno rekonstruovat padělání dat ze stop na datech samotných, protože žádné stopy nevznikají. Již zmíněný „virtuální zločin„ dostává tak zásadní specifické rysy. Orgány činné v trestním řízení nemají za takových okolností vypracovány vhodné strategie podezření a postrádají odpovídající znalosti a zkušenosti. Z aspektů chování moderního pachatele nelze se spoléhat na počítačovou morálku, neboť morálka jako taková podle [175] upadá obecně. Věcně správnější se zdá proto sázka na technickou prevenci, která může zajistit určitou právní jistotu v elektronickém přenosu dat. Kreace celosvětových sítí dat a používání digitální techniky jsou výchozími kroky k multimediální formě společnosti. Že tento vývoj nemá jen své pozitivní stránky, musí být co nejdříve vzato na vědomí; nemá však také jen objektivní povahu nezávislou na psychice zúčastněných osob. Specifické formy počítačové kriminality, které se již projevují, nelze v budoucnu potírat dosavadními vyšetřovacími metodami bez přihlédnutí k aspektům psychologie chování pachatele těchto deliktů.

K profilu osobnosti pachatele podle autorky studie [77]. S tradiční představou počítačového zločince, teenagera ve věku 14 až 16 let, který sám v hluboké noci připravuje jednotlivé útoky na počítačové systémy především pro vlastní zábavu, příliš nekoresponduje statisticky zjištěná skutečnost, že věk těchto osob se rozšířil až k hranici 35 i více let. Pachatel je obvykle vzdělaný, ovládající potřebné dovednosti. Používá automatizované postupy přesahující svým trváním často i časovou hranici delší než 24 hodin, pracuje v týmu a nezákonnou činnost obvykle neprovádí pro zábavu, ale pro zisk. Výrazným rysem bývá skutečnost, že pachatel většinou nemá dosud záznam v trestním rejstříku. Často pracuje na místech, která vzbuzují respekt i důvěru společnosti. Krádež finančních částek realizuje obvykle po menších částkách. Nechce ublížit konkrétní osobě, ale neosobnímu zaměstnavateli, jímž se často cítí být vykořisťován. Krádež software nebo dat považuje za jejich pouhou výpůjčku, s cílem je později vrátit. Ženy - průnikářky mají svůj debut až v roce 1988. Při analýze osobnosti pachatele jakéhokoliv zločinu, tedy i počítačového, je často používán v anglosaském světě akronym *MOMM,* vzniklý z počátečních písmen termínů známých z kriminalistické praxe vyšetřování jakéhokoliv deliktu: *Motive (motiv), Opportunity (příležitost), Means (prostředky), Method (metoda).* Podle [77] nejsilněji motivují peníze, ideologie, možnost kompromitování. Příležitost k páchání zločinu je podmíněna legálním či nelegálním přístupem k systému a obvykle určitými hlubšími znalostmi. Počítačová kriminalita očima analýzy osobnosti pachatele je rozsáhlou oblastí a dotýká se

téměř všech disciplin věd o člověku. Chování pachatelů pak může ovlivnit nejrůznější oblasti našeho života. Počítače kontrolují totiž dodávky energie, letecký provoz, finanční služby, na počítačích se uchovávají záznamy o našem zdraví i o kriminálních případech samotných, při volbách se rozhoduje o budoucnosti národů. V důsledku počítačových chyb a útoků na počítače byly již ztraceny lidské životy, došlo ke krádežím peněz i ke krádežím důvěrných informací. Hrozby proti počítačovým a komunikačním systémům mohou mít mezinárodní, politický i vojenský charakter. Realisticky konající vlády kladou proto na počítačovou bezpečnost i výzkum motivace pachatelů odpovídající důraz. Předstih angažovanosti americké vlády z pohledu současného vývoje nebyl samoúčelný, a je i pro nás určitou výzvou. Krátkozrakost v tomto směru může mít dalekosáhlé následky.

**

K analýze osobnosti pachatele počítačové kriminality, speciálně pak programátora, lze použít také metod *software forensics*, disciplíny o níž jsme se zmínili v souvislosti s možnostmi dokazování autorství programů. Autor článku [237] k tomu říká, že když zadáme pořízení jedné a téže úlohy různým programátorům, je málo pravděpodobné, že mezi výsledky budou dva shodné. Zejména programovací jazyky, které se vyznačují bohatou nabídkou tzv. typů údajů a řídících struktur, umožňují realizovat i poměrně ou úlohu mnoha různými způsoby. Například opakování nějaké činnosti prostřednictvím příkazů programovacího jazyku. Lze to udělat primitivním taxativním opakováním příkazů, ale také použitím často několika způsobů cyklení. Zkušenost a rutina programátora se pak projeví v odlišnostech pojímání cyklů, ve fixním nebo podmíněném členění, ukončování činnosti cyklů apod. I když se jednotlivé verze liší, jsou vzájemně nahraditelné. Použití konkrétní struktury cyklu je tedy obvykle určeno programátorem a nikoliv skutečností, že by řešení úlohy nebylo možné bez použití tohoto konkrétního obratu.

„Rukopis„ programátora jako vodítko k deskripci některých rysů jeho osobnosti. Je nesporné, že prakticky každý programátor si časem vytváří svůj vlastní styl programovaní, podmíněný řadou faktorů, zejména pak stupněm znalosti programovacího jazyku, použitého při konstrukci konkrétního programu. Preferováním konkrétního programovacího jazyku pro řešení úloh, stupněm poznání rozličných struktur údajů a efektivních algoritmů pro zvládnutí drobných rutinních podúloh (například pro řazení, třídění apod.), používáním oblíbených programátorských triků, vědomou snahou o jistou čitelnost či nečitelnost apod., vzniká programátorský „rukopis„. Do jaké míry a za jakých podmínek je takový rukopis jednoznačný, je zatím otevřenou otázkou. Platí však, že se jím může pachatel nejen prozradit při páchání trestné činnosti, ale zároveň se i presentovat co do charakteru své osobnosti, zejména profesní zdatnosti, či rafinovanosti ve věci zamaskování nekalých úkonů.

10.2. Psychologie pachatele počítačové kriminality a problém predikce jeho chování

V praxi je formována osobnost pachatele nejčastěji neoprávněným užíváním software, na základě několika výchozích forem této trestné činnosti. Kromě toho existují i pachatelé, kteří jinak legálně používaný software zneužívají příležitostně nebo i soustavně k nekalým aktivitám. Lze hovořit

-o tzv. domácím uživateli jako konkrétním fyzickém subjektu, který získal, případně dále získává různým způsobem software pro svou osobní potřebu;

-o podnikateli nebo společnosti při užívání nelegálního software pro komerční účely;

-o zvláštní formě zneuživatelů software provozováním počítačových heren;

-o *gamblerech,* hráčích s morbidní závislostí na hracích automatech, kteří mohou být považováni za potenciální pachatele nikoliv ovšem nutně počítačové trestné činnosti, realizované právě kvůli ukojení jejich chorobné hráčské touhy;

-o novém typu potenciálního pachatele, tzv. *počítačového povaleče*, který většinu času věnuje „brouzdání„ v informačních sítích (Internetu) s cílem získat příležitostně nějaký profit, ať již hmotný nebo i nehmotný;

-o *počítačovém teroristovi,* jehož činnost je na rozdíl od počítačového povaleče ostře cílená, bez známek získání pouze nějakého příležitostného profitu.

Počítačoví piráti jsou často zcela obyčejní, jinak bezúhonní uživatelé. Může se jím stát každý, kdo nelegálně zkopíruje např. od přítele disketu, třeba jen pro svou osobní potřebu. Někteří z nich to dělají ovšem i z výdělečných důvodů. U nás jde většinou o nadšence, z nichž např. jeden má třeba přes Internet přístup k software a ostatní kopírují diskety a CD-disky, které dál prodávají buď na burzách, nebo pomocí inzerátů. V současné době je možná fixace nelegálního software i za milion korun na jednom CD-disku. Pak ovšem může být takový pachatel za jediný pirátský disk potrestán i újmou na svobodě. Závažným faktorem ztěžujícím boj proti počítačové kriminalitě je pasivita uživatelů pirátského software, pokud jde o jejich ochotu ke komunikaci s dalšími osobami. I přes stále se zvyšující úsilí policie a dalších orgánů činných v trestním řízení je jejich trestná činnost obtížně postižitelná. Psychologie chování pachatele je v tomto případě založena na prostém pravidle - získat pokud možno zdarma nebo za minimální náklady programy a celkem utajeně je užívat. Většinou je značně omezen okruh osob, které vědí v daném případě o užívání nelegálního software. Určitou výjimkou jsou počítačové herny. Jejich majitel nebo provozovatel však také nedává ve všeobecnou známost, že nemá souhlas autora k užití jeho díla touto formou. Pachatel se domnívá, že nejlepší cestou k beztrestnosti je maximální utajení jeho nekalé činnosti. S jistou mírou úspěchu se o to může pokusit pouze domácí uživatel, avšak počítačové programy musí někde získat. Tím se zapojuje do černého trhu a rozšiřuje okruh osob, které se o jeho činnosti, projevené poptávkou po software, dovědí.

Jak uvádí autor studie [40], v případě domácích uživatelů je nalezení odpovědné osoby, která vědomě nelegální počítačové programy nainstalovala a užívala, celkem snadné.

Je až zarážející, jaký rozsah pirátského software bývá na jediném počítači uživatelů praktikujících jen soukromé domácí aktivity. Mnohdy je takový software naprosto nevyužitelný vzhledem k nevyhovující konfiguraci počítače. I přes tyto skutečnosti lze na počítačích nalézt různé verze náročných inženýrských systémů, ekonomických a jiných programů, často dávno překonaných. Není výjimkou, kdy je na pevném disku počítače ponecháno několik operačních systémů, a to tak, jak se historicky vyvíjely od velmi starých verzí DOSů k nejnovějším verzím Windows.

Komerční užívání nelegálního software má dva základní druhy subjektů. Prvním je jakýkoliv podnikatel, společnost, organizace nebo firma, tedy právnická osoba, která z různých důvodů nemá v podstatě žádný legální software. Jedná se obvykle o menší společnosti. Hlavním z důvodů takové činnosti je nedostatek investic nebo neochota investovat do software. Spektrum zúčastněných osob sahá v takových případech od naivních lidí, kteří se pustili do podnikání a pak se snaží přežít, až po takové, kteří se naprosto chladnokrevně rozhodli neutratit ani haléř za „zbytečnosti„. Samozřejmě u některých právnických osob jde o kolektivní rozhodnutí, ale obvykle lze nalézt konkrétní osobu, která nese odpovědnost za takový postup.

Existují právnické osoby, které pro svou činnost zakoupily licence k užívání, ale ve skutečnosti užívají většího než legálního počtu licencí. Takový postup volí subjekty užívající finančně náročný software, grafická studia, ekonomická zařízení, projekční kanceláře apod. Rovněž zde je spektrum pohnutek pro takovou činnost velmi široké. Vyhledávání a odhalování nelegálního užívání počítačových programů v komerční sféře je velmi obtížné. Zatím neexistuje optimální způsob zjišťování, zda konkrétní společnost užívá nelegálního software. Nabízí se samozřejmě spolupráce s finančními úřady, které z titulu své činnosti mají nejlepší možnost takového zjištění. Prakticky ovšem taková spolupráce naráží na mlčenlivost příslušných pracovníků danou zákonem o finančních úřadech. Proto je postup orgánů činných v trestním řízení mnohdy podobný jako v případech vyšetřování fyzické osoby. Zkušenost s neblahým dopadem na svou činnost mají v tomto případě i takové firmy, jako je Microsoft, viz např. [98]. Tato firma zjistila, že na území západní Evropy a rovněž i v jiných částech světa velký počet všelijakých společností kopíruje software pro svou interní potřebu. Zavedla soudní řízení s několika největšími a nejbohatšími společnostmi (korporacemi) v Evropě, které, jak bylo zjištěno, zakoupily pouze jednu kopii programu a poté bez jakéhokoliv váhání si pořídily pro své zaměstnance stovky nelegálních kopií. Pro společnost je taková metoda jedinečnou příležitostí, jak ušetřit peníze. V těch zemích, kde je tento způsob pirátství hodně rozšířen, mají tvůrci programů obavy z toho, že se nebudou moci udržet na trhu. I když vyvinou velmi dobrý software, prodá se jen minimální počet kopií. Poškození programátoři se pak dostávají do tvůrčích depresí a zvažují, zda má cenu rozvíjet nové nápady a pokračovat v další, často duševně velmi vyčerpávající práci, protože je to ekonomicky naprosto neúnosné.

Z hlediska psychologie pachatelů je dosud nejúčinnějším řešením úzká spolupráce orgánů činných v trestním řízení, zejména policie, s distributory a prodejci software - s tzv.

představiteli distribučních kanálů. Pracovníci distribučních organizací nebo i jednotliví prodejci obvykle disponují konkrétními informacemi o množství nelegálního software užívaného jejich zákazníky. Ve spolupráci s policií jim však často brání falešná „etika„ obchodování a především strach ze ztráty zákazníka, který by se dověděl o tom, že distributor nebo prodejce spolupracuje s policií. Pro odstranění tohoto strachu je nutné s informacemi tohoto druhu pracovat co nejopatrněji. Žádný subjekt neposkytne informaci o svém zákazníkovi v případě, že by vzniklo nebezpečí jeho prozrazení, a tím v podstatě i vznik obavy z postupné komerční likvidace jeho firmy.

V komerční oblasti neexistují většinou osoby, které by před všemi, a to i před zaměstnanci podniku, utajily natrvalo informaci o nelegálnosti používaného software. Znalosti občanů se neustále zlepšují, a proto mnohý zaměstnanec více či méně ví, že software, se kterým pracuje, je pirátský. Zde se pak ocitáme na poli problematiky morálky lidí, kteří vědí, že se sice sami nedopouštějí ničeho protizákonného, ale na druhé straně takovou činnost v podstatě mlčky schvalují. Zvláštním případem zaměstnanců jsou počítačoví odborníci, kteří jako různí správci firemních sítí, analytici apod. vědí, že společnost užívá nelegální software. Mnohdy se tito zaměstnanci podíleli na zavádění nebo přímo sami instalovali pirátský software u společnosti. V konkrétních případech pak tvrdí, že k tomu byli donuceni. V současné neutěšené ekonomické situaci mnohých podniků si ovšem lze představit takový nátlak zaměstnavatele, který by přinutil i dobře poučeného zaměstnance ke spáchání trestného činu s dosti nepříjemnými následky. Řada lidí je denně vystavena např. hrozbě ztráty zaměstnání, což zejména pro kvalifikované, lépe placené pracovní síly bývá velmi citelné. Je zcela pochopitelné, že možnost propuštění z práce je značně nepříjemným následkem, zvláště tam, kde není možnost alternativní volby, a kdy vzniknou negativní dopady pro celou rodinu postiženého. Ovšem případné dopady trestního stíhání a odsouzení pachatele za úmyslný trestný čin představují následky podstatně horší. Není třeba zdůrazňovat, že v případě možnosti trestního stíhání se bude snažit každý řídící pracovník společnosti, případně její majitel, o přenesení odpovědnosti na jinou osobu - zaměstnance. U společnosti pak obvykle dochází k snaze vyhnout se trestnímu stíhání konkrétní osoby zamlžováním odpovědnosti a zamlžováním informace, kdo rozhodl o takovém postupu. V některých větších společnostech bývá pachatelem správce sítě (supervizor) nebo osoba mu přímo nadřízená. Obvykle dochází k rozhodnutí o užívání nelegálního software na této řídící úrovni. To neznamená, že by pachatelem nemohl být počítačový entuziasta, který z vlastní vůle u společnosti nainstaloval řadu nelegálního software. Stanovení konkrétní odpovědné osoby u větší společnosti, která užívala množství nelegálního software, je jedním z nejdůležitějších, ale i nejsložitějších úkolů. Je nutno opětovně říci, že v popsaném problému jde především o morální stránku věci. Pokud by zaměstnanci odmítali uposlechnout své nadřízené a nenechali se donutit k instalacím nelegálního software, situace by dnes v této oblasti byla poněkud příznivější. Přiměřeně k tomu by kleslo množství nelegálního software užívaného u nás. Situace je ze strany zaměstnance poměrně jednoduše řešitelná. Odmítnutím připojit se k trestné činnosti sice riskuje okamžitý osobní následek, ale rozumně se vyhne budoucímu trestnímu stíhání. V opačném případě pak u žádného orgánu činného v trestním řízení ani u soudu neobstojí

tvrzení o nevědomosti nebo strachu. Pravděpodobně bude mít tato obhajoba vliv na výši trestu, ale k rozhodnutí o nevině určitě nepovede.

Životní styl počítačového piráta lze při prvním pohledu považovat za lukrativní a pro dotyčného člověka vnitřně uspokojující. Anonymita davu stejně smýšlejících a jednajících osob přináší bezpečí a pocit naprosté beztrestnosti. Opačnou stranou této mince jsou pak propady příjmů českých i zahraničních firem, které jsou poškozovány na svých zájmech. Většina pirátů je sice obeznámena z větší či menší míry s následky jejich nekalého chování, avšak vzhledem ke zmíněné anonymitě se téměř každý z nich domnívá, že speciálně jemu bezprostředně nebezpečí odhalení nehrozí. Ve skutečnosti je však stále více pirátů za svou činnost hnáno k zodpovědnosti. Psychologicky nejvíce akcentovanou problematikou je u uživatelů porušování autorských práv ve vztahu k počítačovým programům. Každý uživatel výpočetní techniky by měl vědět , že se dopouští trestného činu podle §152 trestního zákona, pokud se vydá na cestu nelegálního šíření, a dokonce i jen pouhého nelegálního užívání software pro svou vlastní osobu. K tomu postačí i jen pouhá instalace nelegálního software na pevný disk. Stejně tak je vystaven možnému trestnímu stíhání každý kdo vytváří více kopií, než povoluje autorský zákon. Je totiž možno mít jen tři kopie programu. Jednu na nosiči, na němž byl program zakoupen, druhou na pevném disku počítače a třetí jako bezpečnostní kopii na libovolném nosiči kdekoliv. Samozřejmě není možný jakýkoliv prodej nebo půjčování za úplatu. Jedinou výjimkou je souhlas autora nebo jeho zástupce s odlišným postupem. Ten bývá obvykle upraven v licenčním ujednání. Často se lze setkat s různými názory na velmi specifický způsob nakládání se softwarem a obvykle je nelze jednoznačně hodnotit. Nejlepším řešením je pak kontaktování autora, případně místní zastoupení firmy a dohodnutí příslušných odlišností. Podle zákona může autor vyjádřit souhlas s jiným způsobem nakládání se svým dílem, čímž sejme zodpovědnost uživatele za takové aktivity. Bohužel k takovému legálnímu přístupu se však počítačový pirát zpravidla nepřikloní, ať již z pragmatických, zjištných či „principiálních„ důvodů, kdy se ani vnitřně nemůže s legálním způsobem chování ztotožnit. V psychologii povědomí pachatele počítačové kriminality se již méně odráží skutečnost velmi snadného překročení *hranice značného prospěchu (rozsahu)* trestné činnosti pirátů. Ta je podle autora studie [37] dána jedním stonásobkem minimální mzdy. Této částky lze dosáhnout skutečně snadno, ceny programových produktů, nejsou zanedbatelné zejména u nejnovějších verzí rozsáhlejších systémů. Psychologicky vzato je třeba v povědomí občanů vytvořit alespoň rámcovou představu o tom, čím a kolik by dotyčný zaplatil za možná pohodlnější životní styl počítačového piráta, než spořádaného uživatele. Trest vyměřený soudem není zdaleka to jediné, co nekalého uživatele čeká. Jde i o zajištění věcí důležitých pro trestní řízení, což je počítač, veškeré datové nosiče a další materiál, např. písemnosti. Realizace toho se pochopitelně odehrává na místě, kde je počítač, což bývá obvykle doma, nebo v sídle společnosti. Policejní prohlídka bytu nebo prostor firmy není nijak vítanou záležitostí, jde vždy o jakýsi zásah do soukromí. Jedinec, který se rozhodne riskovat užívání nebo šíření nelegálního software, by měl nejdříve zvážit, jestli je ochoten nést odpovídající následky. Zda mu postavení obviněného, obžalovaného a odsouzeného, včetně záznamu v trestním rejstříku stojí za jeho nelegální činnost. Jak se uvádí ve studii [40], většině občanů nestojí počítačový program či systém jakékoliv ceny za

poměrně veřejné označení, že je pachatelem trestné činnosti. Nejde pouze o morální újmu, ale i o následky s dopadem na profesionální kariéru, rodinné prostředí atd. Pokud lze psychologickými, sociologickými i jinými technikami zjistit nedostatečnou úroveň povědomí potenciálního pachatele počítačové kriminality v nastíněném směru, nemůžeme u takové osoby vyloučit do budoucna případný další sklon k pirátství či jiným podobným deliktům.

**

Pro predikční činnost je velmi důležitá adekvátní klasifikace kriminálních delinkventů. Pokud jde o *psychologická hlediska*, autor studie [110] klasifikuje pachatele počítačové (informační) kriminality jako

-cílevědomé kriminogenní osobnosti,

-příležitostné typy.

Z rozboru vybraných trestných činů počítačové kriminality podle [110] vyplývá, že se převážně jedná o typy příležitostné, využívající dané situace nebo dosavadní vlastní sociální zkušenosti. Ty pak můžeme podrobněji ještě rozdělit na typy

-kořistnicky zaměřené, podle [110] je lze charakterizovat jako nenasyty, hamouny, podvodníky,

-plánovité, se zaměřením převážně na překonávání překážek ochrany systémů nebo na vlastní uspokojování z utajování vlastní činnosti,

-situační, využívající příhodných podmínek k uskutečnění jakékoli motivace.

Specifika počítačové kriminality podle druhu a psychologie pachatelů. Ve studii [110] se uvádí, že pachateli trestných činů ve spojení s počítači bývají obvykle jedinci

-se středoškolským, jiným vyšším nebo vysokoškolským vzděláním, zejména v technických oborech, speciálně v oboru informačních technologií,

-často nadprůměrně inteligentní, vynalézaví, zejména ve specifické programátorské oblasti,

-zneužívající svého vyššího výsadního postavení v zaměstnání s tomu odpovídající pravomocí,

-ve svém pracovním zařazení nebo ohodnocení neuspokojení,

-jejichž protiprávní jednání neobsahuje prvky násilí a je vzdáleno vůbec tradičním hrubým formám delinkvence,

-jednající v podstatě nebo zásadně individuálně,

-sebevědomí, psychicky silní, dominantní (což u nich ovšem nevylučuje existenci určitých, mnohdy utajovaných komplexů) a jen v menší míře jedinci duševně labilní, či více či méně vyšinutí.

**

Motivace chování pachatelů. Pokud jde o motiv jejich jednání, u nás podle studie [110] zatím zcela jednoznačně převažuje touha po zisku. Statistiky ukazuji, že např. počítačová bankovní kriminalita je jednou z nejvýnosnějších forem zločinnosti. Existují však i jiné motivy, např. touha po získání domnělé převahy nad zaměstnavatelem, euforie z pocitu beztrestnosti nebo neodhalitelnosti, snaha po kompenzaci pocitu ukřivděnosti, osobního

zneuznání, nedostatečného ocenění práce, odstranění pocitu vykořisťování zaměstnavatelem apod. Bujení určitých nových specifických vlastnických a ekonomických vztahů u nás podmiňuje u některých jedinců vznik a gradaci „třídní„ nenávisti a v návaznosti na to snahu programově škodit, kde je to jen trochu možné. S postupujícím zhoršováním ekonomických a vůbec životních podmínek, s nezaměstnaností a beznadějnou perspektivou zejména pro naše mladé občany, nutno s podobnými excesy počítat i do budoucna. V souvislosti s tím souvisí i názor některých zaměstnanců, že organizaci nelze nijak příliš uškodit a když, tak na tom stejně nezáleží. To je pak motivuje k nekalým, většinou prospěchářským postojům. U dobře situovaných jedinců, ne vždy ovšem jen u nich, bývá častým motivem k páchání počítačových deliktů i touha po uplatňování rizika nebo dobrodružství.

V roce 1999 proběhla našimi sdělovacími medii zajímavá zpráva o psychologicky silně deprimující havárii mnoha počítačů na celém světě, způsobené virem *CIH*, zvaným též *Černobyl*. Tento vir patří mezi nejnebezpečnější, je jen velmi obtížně detekovatelný a pro jeho další vlastnosti byl označen jako „divoký„. Dokáže přepsat *BIOS systém* počítače, který je nezbytný pro start a spuštění systému, systémové soubory na pevném disku může zničit a navíc i infikovat soubory další. Jeho autorem je bývalý tchajwanský student strojírenství. Vytvořil virový program, když studoval na technice v Tchaj-peji. Když zamořil školní internetovou síť, byl vedením školy pokárán, ale nikoli vyloučen. Od 26. dubna 1999 (toto datum je připomínkou černobylské katastrofy z roku 1986), kdy se virus dostal do systémů, bylo poškozeno na 70 milionů počítačů na celém světě. K motivaci tvorby viru autor říká: *„Vytvořil jsem ten virus, protože mě štvalo, že všechny antivirové programy jsou na nic„*. Nepředpokládal prý, že by mohl způsobit škody v celosvětovém měřítku. Čtyřiadvacetiletý autor tvrdí, že viru je možné se zbavit eliminací příslušného data ze softwaru. Virus je totiž tímto datem aktivován. Je prý také možné znovu program přepsat pomocí antivirového programu Microsoftu. To, že tento vir stále ještě přežívá, ukazuje, že podniky neberou antivirovou ochranu tak vážně, jak by měly, varuje odborník na počítačové viry společnosti *Articon Information Systems*, která je dodavatelem bezpečnostních řešení. *CIH* není žádný nevinný virus. Jeho účinky působí na zasvěcené pracovníky i psychologicky depresivně. Napadené počítače nelze spustit, ani znovu nastavit k základním úkonům, data uložená na pevném disku jsou nepoužitelná. Tentokrát byly postiženy zejména firmy v Asii. Ale i v Evropě došlo ke značným škodám. Jejich odstranění si vyžádá enormní finanční a časové náklady, důležitá data mohou být ztracena na vždy. Nejnověji aktivovaná verze viru *CIH* platí za obzvláště nebezpečnou, daleko více než populární I LOVE YOU. Ohroženy jsou všechny personální počítače se systémy Windows 95 a Windows 98. Počítače pracující pod Windows NT, DOS nebo Windows 3.x se jej nemusí tolik bát, stejně tak nemůže způsobit žádné škody na počítačích s procesory třídy 386 a 486, kde zpravidla není používán Flash-BIOS. U počítačů s procesorem *Pentium* jsou naopak obvyklé. Tyto skutečnosti budou snad motivovat dosud „spící„ provozovatele počítačových sítí k větší bdělosti, respektive k opatřením podle doporučení organizace *Articon*. Protože anticipace chování potenciálních pachatelů je podle odborníků této organizace velmi těžko objektivně pochytitelná, *Articon* doporučuje předcházet neblahým situacím nasazením antivirového scanneru. Vzhledem k tomu, že mnoho virů proniká do sítě z Internetu, měl by na přípojném bodě být použit systém

pro centrální virovou ochranu, jako je např. *Interscan Viruswall*, který je vysoce kvalitním, mnoha instalacemi prověřeným produktem. Lze samozřejmě použít i jiný dostatečně spolehlivý systém. Dále je potřeba chránit lokální stanice vlastními antivirovými prostředky, protože ne všechny viry přicházejí z Internetu. Pokud je už počítač napaden virem *CIH* a nelze ho nastartovat, musí být BIOS-ROM vyměněn. Dále musí následovat nabootování z bezpečnostní diskety s antivirovou ochranou. Důsledná antivirová ochrana může působit i psychologicky na potenciálního pachatele počítačové kriminality tak, že ho odradí od experimentů s viry.

Motivace hackerů - „sportovců„. Osobnost pachatelů informační kriminality bývá v poslední době formována poměrně novou volní motivací. Jde o motivace založené na soutěživosti blízké psychologii sportovce, která ovšem může v krajních případech hraničit až s jakousi frajeřinou, projevující se výjimečnými „husarskými„ akty. Např. v roce 1999 informační systém Pentagonu čelil poměrně silným „kyber útokům„ hackerů, kteří zatím uspěli pouze v proniknutí do neutajených sítí a nenapáchali žádné materiální či jiné škody. Vyšetřovatelé se důvodně domnívají, že jde o určité, zatím celkem nepříliš nebezpečné akce motivované jistou soutěží pořádanou ilegálně v kybernetickém prostoru Pentagonu. Tyto akce povedou odpovědné činitele k zesílení ochrany informačních systémů, takže podle mínění odborníků větší nebezpečí do budoucna od podobných narušitelů nehrozí.

Motivy chování pornopirátů. Již méně nevinnou se jeví motivace založená na pornokratických aspektech chování některých hackerů, kteří rozlamují zámky dobře placených sex- či porno-míst na Internetu. Odtud pak kopírují a zdarma distribuují materiály, či jinak zabezpečují bezplatné čerpání těchto služeb. Odhaduje se, že celosvětový obrat v této části Internetu se pohybuje okolo 51 milionů dolarů US ročně. Evidentně jde o částku, o které se ostatním podnikavcům v Internetu může jenom zdát. Díky pornopirátům provozovatelé příslušných služeb konstatují, že některá místa vykazují až sedmínásobek čerpání služeb oproti tomu, co je skutečně placeno. Daleko horší jsou však další následky - snížení propustnosti linek až na padesátinu původní kapacity a konečně v jistých případech i havarování serverů, odstavení Web-míst na několik týdnů a totální čistka v účtech, jejichž hesla byla běžně dostupná na Internetu.

K motivaci porušování pravidel ochrany zaměstnance při práci s počítačem. Pro úplnost konstatovat, že při práci s počítači nemusí být v rozporu s etickými pravidly či dokonce se „zákonem„ vždy jen zaměstnanec, ale také zaměstnavatel. Je známo, že pracovník, který tráví většinu pracovní doby před počítačem, je vystaven řadě nepříznivých vlivů hmotných, jakým je např. zdraví škodlivé vyzařování, i vlivů psychických. Každý zaměstnavatel by měl především zajistit vhodný pracovní prostředek určený k ochraně zraku. Takovým prostředkem je např. filtr před monitorem nebo obrazovka s již zabudovanou ochranou. Základní požadavky, které určují odpovědnost zaměstnavatele související se zajištěním bezpečné práce a ochrany zdraví zaměstnanců při práci na zařízeních se zobrazovacími jednotkami (sem patří počítače včetně monitorů), byly stanoveny *evropskou směrnicí* z 29.5.1990. Zásady pro úpravu pracovního režimu jsou doporučeny *Mezinárodním úřadem práce*. Zmíněná směrnice kromě jiného uvádí, že zaměstnavatel je povinen

organizovat činnost zaměstnanců tak, aby práce u monitoru byla během směny periodicky přerušována přestávkami nebo změnami činnosti, které by snížily pracovní zatížení vyplývající z použití monitoru. Existují u nás zaměstnavatelé, kteří plně respektují uvedené zásady, někteří dokonce poskytují svým pracovníkům, trávícím většinu pracovní doby před monitorem, určitý příplatek. Příplatek sice nemůže plně kompenzovat příslušné újmy, ale může motivovat či zavazovat samotné zaměstnance k dodržování ochranných pravidel. Nás však zajímají především důvody, které vedou některé zaměstnavatele k porušování uvedených zásad. Jde zejména

-o neznalost podstaty věci i příslušných ustanovení, což samozřejmě zaměstnavatele neomlouvá;

-o nedbalost, která se zpravidla projevuje i v dalších sférách činnosti dané organizace, tedy nejen při práci s počítači;

-o podceňování ať již tvůrčí či rutinní práce s počítači, které se projevuje zejména na zaostávajících pracovištích, nebo na pracovištích s diametrálně odlišnou náplní práce od exaktního či jinak adekvátního nazírání na realitu;

-o vědomé nerespektování úprav z jiných než zištných důvodů, např. z neschopnosti vedoucích činitelů organizačně či finančně zabezpečit příslušná opatření;

-o vědomé nerespektování ze zištných důvodů, což je aktuální zejména v poslední době ekonomického propadu a všeobecné platební neschopnosti podniků či organizací, kdy určití podnikatelé, jejichž chování je mnohdy přímo determinováno malformovanými ekonomickými vztahy, nerespektují pro osobní profit zájmy a práva svých zaměstnanců.

Mnohdy jde o kombinace uvedených faktorů chování zaměstnavatele, přičemž poslední tři lze považovat za zvláště závažné z hlediska obtížnosti jejich případné nápravy.

**

Z hlediska *vztahu pachatelů k informacím* bychom je mohli dělit

-na amatéry, kam bychom zařadili hackery, crakery, eventuálně ostatní typy zatím nepojmenované,

-na profesionály, kam by patřili pracovníci speciálních tajných služeb, detektivové, žurnalisté, podnikatelé všeho druhu, včetně specialistů-manažerů, specialisté informatici, teroristé.

Podle autora [110] bychom mohli pachatele specifikovat i jinak, ale uvedené členění je pravděpodobně nejrozšířenější.

Uvedené skupiny jsou v práci [110] charakterizovány podle hledisek a zkušeností *policejní praxe* takto:

1)*Amatéři* jsou osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že vyhledávají zranitelná místa. Osobnostně jsou to lidé zpravidla s vyšší inteligencí, jednostranně rozvinutou, ovšem plně si uvědomující své počínání. Velmi snadno a rychle se naučí pracovat s počítači, většinu úkonů prováděj i automaticky, jsou schopni neustále vstřebávat nejnovější informace, analyzovat je a pružně reagovat na změněné situace. Jsou tedy pružní, flexibilní, vytrvalí, velmi často vynalézaví, uspokojovaní procesem řešení složitých problémů. Jejich cíle nebo motivace jsou různé. Lze je rozdělit na

- *průnikáře* (hackery), pronikající do ochraňovaných systémů, přičemž jejich cílem je prokázání své vlastní schopnosti, kvality, aniž by měli zájem získat nějaké informace nebo systém narušit. Hlavní jejich snaha spočívá v překonávání ochranných bariér, což považují za dobrodružství, zábavu, soutěživost ve smyslu sportu, aniž by očekávaly osobní profit. Stačí jim, jestliže se o jejich činu hovoří. Snad by vyhovovalo srovnání se žháři, kteří mají požitek z pozorování ohně, přičemž se někdy podílejí i na jeho likvidaci. Hackerství je jejich koníčkem, u počítačů vysedávají po dlouhý čas a získaná data nebo programy využívají spíše pro svoji potřebu nebo pro přátele. Např. v roce 1997 se u nás projevil hacker, který se označuje jako *Czert*. Pronikl na webovské internetové stránky několika našich ministerstev a ty pak neuctivě pozměnil. Podle mínění kriminalistů jde pravděpodobně nikoli o jednoho člověka, ale o partu mladých počítačových exhibicionistů z hlavního města - pokud budou dopadeni budou zřejmě pyšní na to, jak kriminalistům „zamotali hlavu„;

-*neúspěšné kritiky*, jejichž motivace je ovlivněna neúspěšným poukazováním na závady a nedostatky v informačních systémech, zejména v jejich ochraně. Průnikem chtějí upozornit na naléhavost situace a nutnost jejího řešení. Nesledují zištný cíl, chtějí pouze vyburcovat odpovědné činitele k zásahu. Vlastní průnikářskou činnost považují za krajní prostředek řešení;

-*mstitele*, jejichž motivace vyplývá ze msty vůči zaměstnavateli, který je z různých, pro ně ovšem nespravedlivých, důvodů propustil ze zaměstnání nebo jinak poškodil;

-*škodiče* (crackery), což jsou spíš patogenní osobnosti, jimž nejde jen o překonání ochranných překážek, ale po průniku různým způsobem nabourávají informační systémy, získávají data, aniž by snad měli zájem je využít pro svůj prospěch. Potěšení mají spíše z destrukce systému.

2)*Profesionálové* - jejich náplň práce je dána informačním procesem. K prostředkům získávání, shromažďování, třídění, systemizování, vyhodnocování, analyzování a dalšímu využívání informací mívají v rámci možností zaměstnavatele v podstatě neomezený přístup. Tuto činnost nevykonávají většinou pro sebe, ale pro zaměstnavatele. Špionáž, nekalá reklama, boj i jinými prostředky s konkurencí apod., se může stát jejich „koníčkem„ a později třeba zneužitelným komerčně i pro jejich osobní potřebu. Z hlediska počítačové nebo informační kriminality není tato kategorie příliš zajímavá, dokud se tyto osoby nedopustí protiprávního činu. Což přichází v úvahu hlavně u manažerů z různých institucí, nikoli u profesionálů ve státních nebo bezpečnostních službách. Do této kategorie však podle [110] lze řadit i ty softwarové piráty, jejichž hlavním cílem je neoprávněný zisk z prodeje nelegálně získaného software.

3)*Teroristé* - tvoří zvláštní skupiny osob zpravidla spjatých s organizovaným zločinem, operující většinou vlastními zpravodajskými sítěmi, jak pro získávání potřebných informací, tak i pro vlastní ochranu gangů. Mohou být velice kvalifikovaní, obdobně jako pracovníci oficiálních zpravodajských služeb; jen jejich zaměření, cíle a pochopitelně i způsoby a prostředky dosažení těchto cílů jsou naprosto jiné. *Počítačoví teroristé* ke svým nekalým aktivitám využívají stále častěji prostředí mezinárodní sítě Internet. Tato síť jim v případě potřeby poskytuje dostatečnou anonymitu, jak pro získávání informací a komunikaci s ostatními členy gangu, tak i pro cílené aktivity.

Podle [110] je právě uvedená klasifikace značně vágní, protože ve skutečnosti se jednotlivé kategorie mohou prolínat, např. pokud jde o motivaci chování.

Psychologie počítačového teroristy vykazuje v praxi určitý stereotyp chování. Terorista může pracovat buď zcela individuálně nebo ve spojení s organizovaným zločinem, což je považováno obecně za společensky velmi nebezpečnou činnost. Zpravidla jde nejdříve o získání inkognita osobnosti využitím nekalých (placených) služeb nabízených na Internetu. Pachatel se pomocí falešného pasu může stát např. fiktivním občanem nějakého, široké veřejnosti méně známého (exotického), státu. Dále následuje založení poštovních schránek, bankovních kont, kreditních karet, pořízení nebo prolomení tajných klíčů pro získání potřebných informací a nekalou komunikaci s ostatními členy kliky, nepracuje-li ovšem pachatel ryze individuálně. Přípravná fáze je zpravidla ukončena nelegálním ozbrojením pachatele a pořízením falešných průkazů, opravňujících pachatele ke vstupu do objektů, v nichž se má realizovat teroristický útok. Vše lze uskutečnit rovněž prostřednictvím nabídek na Internetu. Úspěchu některých teroristických akcí předchází ještě podvodné získání finančních prostředků, např. pomocí nelegálních bankovních převodů. Vlastní činnost pak závisí na charakteru útoku. Při bombových akcích může terorista čerpat informace o stavbě bomby rovněž přímo z Internetu. K vlastní akci může použít pak předem připravené kamufláže profese, vydávat se např. za opraváře, novináře, reportéra atp., případně si najmout ke „špinavé„ práci pomocníky. Po ukončení akce následuje zahlazení stop a po určité prodlevě odlet inkognito do zahraničí. Samostatně působící terorista většinou hodlá zachovávat anonymitu. Ke spáchaným činům se oproti tomu organizované skupiny v důsledku proklamované ideologie často dodatečně hlásí. Přitom se ovšem snaží o maximální utajení individuality svých členů. V tom nutno spatřovat kořeny variability psychologie chování teroristů.

10.3. Právní vědomí pachatele počítačové kriminality

Etika, morálka, právní vědomí a počítače. Právní vědomí uživatele počítačové techniky nelze studovat bez patřičných vazeb na etiku a morálku, respektive na aktuální stav, společenský úzus i vývoj kulturních společenských vzorců v této oblasti. Studie [76] je uvedena lapidárním bonmotem: *„Věda bez lidskosti je marná a nebezpečná. Výchova bez charakteru je marná a nebezpečná. Ekonomie bez morálky je marná a nebezpečná. Jsou-li mravy a společenské normy neadekvátní, nelze zákony vynutit. Jsou-li mravy adekvátní, zákony nejsou nutné.„* Určitou nadsázkou je zde aproximován hlubší smysl vztahů jinak dosti abstraktních filosofických kategorií. Etika je dle definice systém morálních principů, pravidel chování. Počítačová etika je aplikace systémů morálních hodnot a pravidel chování na práci s počítači. Základem jsou tedy principy morálky. Podle autorky studie [76], jakož i v souladu s dalšími specialisty na počítačový zločin a počítačovou bezpečnost, lze vidět etiku ve třech různých úrovních motivace nebo chování, jde

-o úroveň zákona - je třeba mít dobré zákony, aby si např. mladí hackeři uvědomili, že nestojí za to pokračovat v hackerských aktivitách, protože pokuty či jiné sankce jsou příliš

vysoké, pravděpodobnost odhalení velká, takže podobná nekalá činnost se nevyplácí; k formulaci autorky [76] podotkněme navíc, že zejména neodvratnost a bezprostřednost trestu je ústředním faktorem, který by měl pachatele odrazovat od nekalé činnosti;

-o úroveň konvence ve smyslu ustálených kódů chování, např. takových, které byly již v šedesátých letech navrhovány v USA, jako vodítko pro uživatele rozvíjející se výpočetní techniky;

-o morální úroveň, což je to, co každý jedinec se učí od rodičů, v mezilidských vztazích, ve škole, na pracovištích apod.

Morálnímu chování jako takovému se lze těžko naučit. Můžeme se učit aplikovat etické hodnoty, které jsme získali již dříve. Při aplikacích na nové, rychle se měnící technologické prostředí, či přímo do prostředí kybernetického prostoru, máme podle [76] korektiv: *„Pokud něco udělám já, co by se stalo, kdyby to udělal každý? Máš-li pochybnosti, zeptej se těch, které to může ovlivnit, na jejich názor!„* Mezi další pravidla podle [76] můžeme řadit ta, kterými by se měl řídit vlastník výpočetní techniky a její uživatel. Pravidlo vlastníka říká: *„Představ si, že by ostatní chtěli zacházet s tvým produktem nebo službami, které nabízíš, jako s vlastními, jako by byly veřejně přístupné - chceš je mít v takovém případě soukromé nebo veřejné?„* Proti tomu stojí pravidlo uživatele: *„Předpokládej, že všechno, co používáš, jako je počítač, program apod., patří někomu jinému – pokud to není explicitně nebo v souladu s určitou konvencí určeno k veřejnému použití.„* Zjevně v rozporu s těmito pravidly je podle [76] etika hackera, která má prostou logiku - informace patří všem, proto musí být i počítačové systémy všem k dispozici bez omezení.

Porušování pravidel počítačové etiky. Jak uvádí autorka [76], v atmosféře univerzitního nebo i jiného vzdělávacího prostředí je mezi studenty běžné, že některé jejich činy nejsou vnímány jako deviantní. Jde zde pouze o určité aspekty povahy technologie jako takové, tj. o anonymitu, schopnost toulat se prostřednictvím počítače kybernetickým prostorem, nevidět přitom lidi, s kterými je dotyčný uživatel ve spojení, nevidět ani následky případných neetických činů atd. Autorka [76] se ptá: „Nejde však o daleko více, o všeobecnou krizi morálky?„ Matoucí je také povaha informace jako nehmotného vlastnictví. Od někoho si vezmeme počítačový soubor, ale on ho má i nadále k dispozici, nezbavili jme ho tedy jeho používání.

Na případu *internetového červa* lze ukázat, jaké potíže mohou nastat při implementaci zákona v podmínkách internetového zločinu. Tvůrce internetového červa, student a syn jednoho z nejznámějších expertů v oblasti počítačové bezpečnosti, koncem roku 1988 způsobil v síti ARPANet v USA zhroucení více než šesti tisíc počítačů. Obviněn byl podle tehdy platné zákonné úpravy, která zakazuje neautorizovaný přístup k „počítačům federálního zájmu„. Ty jsou definovány jako počítače, které

-jsou vlastněny americkou vládou nebo vládním smluvním partnerem,

-jsou používány ke zpracování finančních transakcí (bankovní sektor),

-jsou používány k mezistátní komunikaci.

Pachatel se hájil tím, že mu byly přiděleny legitimní účty na hostujících počítačích sítě ARPANet, a že byl tedy na této síti autorizovaným uživatelem. Napsat program k dosažení jiných počítačů na síti, bylo dle jeho názoru jeho právem, stejně jako je právem uživatele posílat jiným uživatelům zprávy elektronickou poštou. Obhajoba pachatele se tímto způsobem pokoušela využít dvojznačnost termínu „neautorizovaný přístup„. Obžaloba přesvědčila porotu, že využití bezpečnostních zranitelností pachatelem k tomu, aby získal přístup k systémům, bylo základem pro neautorizovaný přístup a dotyčný byl z tohoto činu usvědčen. Blíže k tomu viz opět [76].

Pokud solidní uživatel výpočetní techniky chce dodržovat zákony a pravidla běžné etiky např. v oblasti počítačového práva, avšak nehodlá studovat stovky stránek informací a právních úprav týkajících se tohoto problému, měl by se držet následujících pravidel.

1. Předpokládat, že cokoliv bylo zveřejněno kdekoliv (týká se např. i manuálů přiložených k software), může být autorským dílem, tedy dílem automaticky chráněným. Výskyt či absence značky copyrightu (C), ©, ® apod. není rozhodující. Podobně je celkem jedno, zda jde o program, manuál, doprovodný text, grafiku, proužek, specifický kód či skript.

2. Šíření autorského díla spočívá v jeho dalším zveřejnění, pokud jde o programy, pak jejich neoprávněným kopírováním a užíváním.

3. Chráněno je ovšem dílo, nikoliv idea. Při nakládání s ideou je citování autora věcí určité konvence etiky. Idea ale není totéž co forma či vzhled.

4. Při použití programu získaného jinak než legální koupí, je třeba získat souhlas od autora-programátora. Nejlépe v písemné dohodě a za jasně stanovených podmínek.

5. Věci onačené „*public domain„* jsou volně použitelné, ale nemůžeme si být asi nikdy zcela jisti, že jde v daném případě opravdu o tuto třídu produktů.

6. Fakta o určité události či produktu nespadají pod ochranu copyrightu, ale forma jejich presentace ano, tedy např. vytváření nové stránky na Internetu o určitém výrobku není dovoleno pouhým stáhnutím reklamní agendy od výrobce.

7. Zvýšené opatrnosti je třeba i při přejímání a presentování citlivých dat týkajících se osobnosti občana. Není bez zajímavosti, že rozšíření autorské ochrany počítačových děl dokumentem *Copyright Treaty* z roku 1996, uveřejněným organizací *WIPO (World Intellectual Property Organization),* se dotýká i databází.

8. Nelze nic pokazit uvedením zdrojů, z nichž bylo tvůrčím způsobem čerpáno. Naopak, je to žádoucí i z hlediska konzumentů informací pro případné další rozšíření jejich obzoru.

Počítačoví piráti zpravidla porušují tyto zásady ať již z nedbalosti, či vědomě. Někteří výrobci software poskytují „generální pardon„ v souvislosti s neoprávněným užíváním jejich, zejména již překonaných starších produktů. To však může na různé typy uživatelů či pachatelů působit rozporuplně podle vyspělosti jejich právního a etického cítění. Existují zneuživatelé software, kteří se pod vlivem určité benevolence výrobce domnívají, že dříve či později budou jejich prohřešky prominuty a svou nekalou činnost rozšiřují bezostyšně dále.

Pomluva a poškození pověsti. Nedostatek etiky je v pozadí četných právních kauz, uplatňujících nároky na odškodnění pro pomluvu nebo poškozování pověsti. Ve studii [76] je uveden případ *Stratton versus Prodigy* z roku 1994. Firma *Prodigy,* provozovatel Internetu, poskytuje uživatelům také službu *BBS*. Jeden uživatel umístil na tuto „nástěnku„ velmi negativní zprávu, týkající se produktu, s kterým nebyl spokojen. Výrobce produktu zažaloval firmu Prodigy pro pomluvu. I když firma Prodigy uváděla, že je pouze vydavatelem informace, nikoliv autorem, byla shledána vinnou, protože monitorovala obsah BBS a pomlouvačnou zprávu neodstranila. Podle [76] *monitorování* je přitom z hlediska práva dvojsečná zbraň, můžeme být odsouzeni za narušení soukromí, nebo v jiných případech pro nedbalost, to v případě, že jsme dostatečně nemonitorovali.

Nezajištění ochrany ze strany provozovatele systému. Podle autorky studie [76], uživatelé Internetu obvykle očekávají zachování soukromí. Pravděpodobnost, že nezašifrovaný text bude nelegálně zachycen a v určitém místě přenosu přečten, je však znepokojivě vysoká. Nabídka objednání zboží, poskytnutí půjček, převod finančních prostředků provozovateli komerčních služeb zasláním čísel kreditních karet nebo osobních identifikačních čísel přes Internet s sebou nese nebezpečí zachycení přenášených dat. Následně může dojít k podvodným aktivitám, např. výběru peněz nebo podvodného objednání zboží apod. Povinností provozovatelů je zajistit alespoň základní opatření, aby jakékoliv citlivé informace posílané přes Internet byly šifrovány adekvátně bezpečným šifrovacím mechanismem.

Problémy šíření pornografe. Internet je v poslední době používán stále častěji k šíření různých nekalých informací, nevědeckých poznatků, náboženského či sektářského tmářství, pověr, pomluv a také pornografie. I když se definice pornografie v jednotlivých státech různí, skutečnost, že mohou být pornografické obrázky prohlíženy ze vzdálených míst a stahovány z mnoha BBS a WWW stránek, je závažná a může způsobit organizacím vážné potíže. Jak uvádí studie [76], v USA již několik společností, včetně jednoho ministerstva, utrpělo na ztrátě pověsti poté, co byly na jejich systémech pornografické obrázky objeveny. Dokonce i u nás došlo již na Internetu ke zveřejnění pornografických fotomontáží některých význačných osobností. Obavy uživatelů, že by mohli být při ukládání a přenášení takovýchto zpráv přistiženi, vedou často k tomu, že se snaží získat neautorizovaný přístup k systémům někoho jiného a na těchto systémech obrázky ukládají.

Cesty ke zlepšení etiky. Podle studie [76], počítačoví profesionálové se shodují v tom, že jsou dvě možné cesty nápravy - příklad a výchova. Mladí lidé jsou v rodinách často svědky toho, jak rodiče kopírují videokazety. Není divu, že si potom bez jakýchkoliv zábran kopírují software na svůj počítač. Rodiče často s tímto nelegálním způsobem souhlasí, protože v tom vidí využití pro studijní účely. Na druhé straně hackeři pokládají tyto nelegální postupy za zajímavější a více vzrušující, než je počítačová výuka. Velmi důležitým faktorem ovlivňujícím chování jednotlivců je úroveň morálky celé společnosti. Výchova k osvojení pravidel počítačové etiky by měla probíhat u každého již od mládí. Ve škole i na univerzitách se mladí lidé učí, jak provozovat počítač, jak ho používat, studují obslužné manuály, ale nic se nedovídají o tom, jak používat počítač „eticky a zodpovědně„. Na kurzech vyšší úrovně se studenti učí prolomit šifrovací systémy. V praxi pak získaných znalostí mohou použít buď k ochraně počítačových systémů, nebo zneužít k jejich narušení. Zda převáží pozitivní způsob využití znalostí, je věcí nejen rodičů, školy a počítačových profesionálů, ale celé společnosti, všeobecné úrovně právního vědomí a hlavně pak úrovně morálky.

**

Právní vědomí a počítačová kriminalita v pojetí autora studií [35]-[40]. Právní vědomí každého občana se postupně konstituuje již od dětství. Je smutné, že se počítačová kriminalita, zejména pak zneužívání software, týká i dětí. Ty samozřejmě nejsou trestně odpovědné, ale časem budou. V případě, že jejich rodič jim podává negativní příklad nerespektováním zákona a jeho pohrdáním, nelze čekat, že se budou později chovat jinak. Mnohdy to začíná již na škole, když si např. žáci prvního stupně základní školy mezi sebou vyměňují počítačové hry stejně, jako si dříve vyměňovali poštovní známky.

Autor pojednání [40] uvádí tento případ: Jedna z řídících pracovnic velké softwarové firmy, jako dárek při návštěvě u známých, dala dítěti asi ve věku osmi let hru za 1500 Kč. Dítě po zjištění ceny dárku se velmi rozzlobilo a vysvětlovalo, že za tyto peníze by ve škole mělo pět her a ne jednu.

Nelze v daném případě vinit z odpovědnosti pouze naše jistě problematické školství. Jde o ukázku toho, že již dnes roste ve školních lavicích generace lidí, která získává velmi negativní postoj k respektování cizích práv. Ani rodiče, ani škola jim nejsou schopni dát pozitivní vzor. Je proto žádoucí, aby již na základních školách byla stávající specializovaná výuka zaměřena na pochopení a akceptování nutných norem. Pokud již dnes vkládáme do dětí špatné návyky a pokřivený pohled na to, co je správné a co nikoliv, bude obtížné v budoucnu jejich názory a přístupy podstatně změnit. Budou na tom podobně jako současná populace, kdy většina uživatelů výpočetní techniky je velmi často konfrontována s aktivitami okolo nelegálního programového vybavení a především jeho užívání. Úloha správné výchovy, školní nevyjímaje, je v tomto směru nezastupitelná.

Poněkud specifická jsou podle [40] hlediska psychologie porušování autorského práva v hernách. V počítačových hernách se realizují zvláštní formy užívání software. Většinou se jedná o bojové hry, které umožňují hru většímu počtu hráčů. Pro poměrně širokou skupinu

mladistvých jde o velmi atraktivní zábavu. Atmosféra v těchto hernách bývá často taková, že spolu s hráči se hrou baví i řada přihlížejících. Málokdo z nich si uvědomuje, že velmi často v takových situacích dochází k porušování autorského práva. Jak uvádí pramen [40], firma JRC podle vlastního stanoviska jako zástupce zahraničních společností vyrábějících hry, nedala dosud nikomu právo takto hry komerčně užívat. I když firma ví o této činnosti, je v podstatě bezmocná, protože veškerou aktivitu směřuje na dovoz, distribuci a prodej počítačových her. Je tedy i na represivních orgánech, aby se k tomuto problému postavily a následně byl schopen reagovat celý trestní systém. Samotné řešení ale není jen v trestním postihu. Podle [40] není třeba kriminalizovat problém, který by šlo vyřešit i jiným způsobem, např. uzavřením smlouvy mezi firmou příslušnou firmou a majitelem - provozovatelem počítačové herny. Aby k tomu došlo, musí vzniknout oboustranné pochopení. První krok však by měl udělat ten, který hodlá autorsky chráněný software oprávněně užívat. K tomu ho při současné neutěšené situaci donutí asi jen reálná hrozba trestního stíhání.

Problémy počítačových heren velmi dobře odrážejí stav lidského myšlení specifické části populace. Pokud není jedinec nucen nebo sám se necítí být ohrožen, nejeví zpravidla snahu po legálním chování. Zisk heren je postaven ve většině případů nade vše ostatní a jeho výše je jediným kritériem spokojenosti podnikatele. V tomto směru, jak uvádí autor [40], máme co napravovat.

Rozvoj možností výroby a šíření software, vznik průmyslové a domácí výroby, lisoven, kopírovacích služeb, půjčoven software, možností instalace software do nové výpočetní techniky apod., dalo vzniknout novému typu pachatele. Pachatelem je obvykle dospělá osoba. To ovšem již nemusí platit o zákaznících nebo koncových prodejcích. Oproti jiným případům počítačového pirátství je možno očekávat, že pachatelé těchto forem trestné činnosti mohou mít rozsáhlé předchozí zkušenosti s prací policie a je možno očekávat jejich dřívější trestní stíhání. Např. na počítačové CD-disky tito pachatelé pohlížejí jako na standardní zboží, které jim má přinést zisk. Často se dovozem těchto produktů zaobírají i lidé, kteří obchodují i s jiným zbožím, oděvy, obuví aj., mnohdy neoprávněně označovaným různými falešnými ochrannými známkami.

Vzhledem k tomu, že právní vědomí průměrného občana naší země je vcelku minimální, málokdo si plně uvědomuje hranice zákonného chování a dosah možných následků. Mnohdy nastává situace, kdy se v daném okamžiku mění doposud bezúhonný člověk v osobu trestně stíhanou. Často je to otázkou morálního nazírání na věc. Vlivem nových společenských vztahů, ať již výrobních, vlastnických či komunikativně osobních, dochází k posuvu i v oblasti morálky občanů. To nejlépe dokresluje množství nelegálního software nejen u nás ale i např. v bývalém východním Německu.

Z hlediska přístupu represivních orgánů není zde možno podceňovat *kriminální činnost nezletilých*, i když jsou samozřejmě trestně nepostižitelní. Podle [40] nelze tolerovat páchání počítačových deliktů a navíc je omlouvat jen pro neexistenci dostatečných finančních prostředků. Je naprosto zřejmé, že morálními apely se nedosáhne podstatného zlepšení situace, ale nelze je proto pomíjet a používat přímo jen tvrdé sankce.

10.4. Fenomén erotiky a pornografie na Internetu

Při práci s Internetem se lze přesvědčit, ať náhodným nebo i cíleným surfováním, o poměrně široké nabídce sexuálně orientovaných artefaktů. Podle formy může jít o texty, grafiku (zejména fotografie), hudbu, kombinované útvary (videoklipy), statické, ale i více či méně animované (pohyblivé) artefakty. Pro jejich bližší vymezení či členění můžeme hovořit o typech se sexuální tématikou (lékařskou, osvětovou apod.), typech erotických (mnohdy i s nezanedbatelnou estetickou či uměleckou hodnotou), o lehkém pornu (v případě obrázků, někdy i textů, o pornografii), tvrdém pornu (pornografii). Ostré vymezení těchto termínů neexistuje, vyskytuje se množství artefaktů na pomezí těchto jinak velmi volně pojímaných typů. Zvláštní skupinu aktivit na Internetu tvoří pak ještě

-diskusní skupiny (kluby), kdy členové skupiny zasílají příspěvky na speciální server a ten je rozesílá do přihrádek elektronické pošty jednotlivých členů, diskuse probíhá off-line, členové si vyměňují nápady, fantazie, poznatky atp.;

-rozhovory probíhající tak, že na jednom serveru se sejde několik uživatelů a ti si zasílají krátké příspěvky, zhruba jako v normálním hovorovém kontaktu, jde o tzv. kyber-sex, což je obdoba sexu po telefonu;

-video, kdy vzhledem k náročnosti na velikost paměti jde o krátké, několikaminutové sekvence s pornografickou tématikou;

-live-streaming video, speciální forma videa podobající se televizi po Internetu, postrádající nevýhody klasického Internetového videa;

-nabízení sexuálních služeb a pomůcek po Internetu, jako obdoba inzerce v časopisech a denním tisku, navíc i s případnými možnostmi přímých objednávek.

Mimo to v elektronické pornografii existují ještě dvě další kategorie, které prozatím nejsou příliš frekventovány. Jsou to speciální sexuální programy pro vytváření modelu ženského nebo mužského těla podle představ uživatele, s možností realizace různých poloh, simulování autoerotiky, koitu apod. Dále pak zařízení pro virtuální sex, která existují v podobě pro muže (elektronická vagina) a pro ženy (elektronické vibrátory vaginy, vnějšího genitálu, análu). Tyto systémy mohou obousměrně přenášet data a reagovat na ně, a tak simulovat přirozené orgány. Systémy je možné propojit přes počítač a Internet a virtuálně tak kontaktovat partnera v jiné části světa. Podobný systém se pravděpodobně zatím komerčně nevyužívá, vše je dosud v experimentální podobě. Ovládací programy jsou značně náročné a dosud velmi sporadicky se vyskytující.

Z hlediska zaměření této publikace nás budou zajímat kriminologické aspekty spojené s nabídkou, prezentací a konzumováním uvedených artefaktů. Jsou to:

1.*Otázky společenské nebezpečnosti a porušování zákonů popsanými aktivitami.* Internet šíří informace v mezinárodním měřítku. Je proto možné, že artefakty porušující zákony nebo alespoň pravidla vžitých měřítek morálky v jedné zemi, mohou být jinde plně tolerovány. Je např. známo, že filmová tvorba v USA prezentuje v některých případech dvě verze určitého díla, jednu jako „domácí„ druhou tzv. „evropskou„ liberálnější. V

nadnárodním pojetí neexistuje proto jednotné a dostatečně ostré měřítko pro posouzení této problematiky.

2.*Problémy psychologie, motivace a míry bezúhonnosti provozovatelů.* Podle původu pornografického matariálu rozlišujeme

-*originální pornografický materiál velkých producentů;* z hlediska psychopatologického bývají obvykle velcí producenti bezproblémoví; jakožto velké komerční společnosti, snaží se upevnit svou bezproblémovou pozici a vyhýbat se prohřeškům proti zákonu; nezabývají se proto speciálními praktikami vyššího stupně s výjimkou občasné urinofilní (pissing) produkce; jejich originální materiály jsou často nelegálně kopírovány, příp. scanovány do počítačové podoby, kdy dochází k porušování autorských práv, která se pochopitelně vztahují i na pornografii; motivace oficiálních producentů je samozřejmě zištná; velcí producenti poskytují materiály se zvláště speciální náplní, placené pomocí bankovních karet klienta, ale také i zcela volně přístupné; přemíra grafiky na některých stránkách producentů, která zpomaluje přenos artefaktů, v některých případech i prodlevy nebo zdlouhavé vybavování zobrazení intimních míst na fotografiích, přivádí k domněnce určité shody jejich zájmů s provozovateli placené telefonní sítě;

-*pornografický materiál malých producentů;* malí producenti se zabývají spíše zájmovými skupinami a obecně nabízejí tvrdší pornografii; jejich produkce se objevuje hlavně na serverech spravovaných amatéry a zájmovými skupinami; nejsou zde výjimky volně přístupných případů zobrazování extrémního fetišismu (např. i malformací genitálií), výstředních bondáží (tortury, infibulace), bizaru (včetně simulace krvavých praktik), zoofilie, někdy i dětské pornografie; lze se ještě zmínit o vydávání pornokomixů, které zvláště v sadomasochistické podobě poskytují pozoruhodný studijní psychopatologický materiál; motivace v tomto případě je obdobná jako u předchozí kategorie producentů, snad navíc s tím, že v některých případech jsou žádány sponzorské příspěvky z řad dobrovolných dárců;

-*amatérské produkce,* kterým bývají věnovány speciální sekce na pornografických serverech; amatéři si také zakládají vlastní servery, vyměňují si materiály, sdělují zkušenosti apod.; amatérská produkce je mimořádně variabilní - od erotiky po extrémně tvrdé praktiky; je zajímavé, že v některých případech bývá komerční pornografie deklarována jakožto „amatérská„; motivace amatérských producentů bývá většinou nezištná; v poslední době se vyskytují též různé fotomontáže a dodatečné úpravy digitálních záznamů pornografických materiálů; většinou jde o detailizaci (podrobnější pohled), invalidizaci (znetvoření modelu), skandalizaci (mixáž s obličejem známé osobnosti), intususcepci (vkliňování kreseb, cizích i vlastních), resignování (změny značek producenta) pomocí speciálních grafických editorů; aberantní jedinec může tak poměrně snadno realizovat své představy.

3.*Problémy spojené s konzumací artefaktů.* Lze se domnívat, že normálně saturovaný jedinec nedozná žádné újmy shlédnutím i těch mimořádně extrémních porno-produktů, které se mohou na Internetu vyskytnout. Bohužel, existují však osoby, u nichž určité psychické následky by mohly vzniknout. Mohou to být děti, mladiství, či osoby sexuálně nesaturované, psychopati apod. Názory občanů na otázky excitace či tlumení sexuálních aktivit (mnohdy společensky značně nebezpečných) na základě shlédnutých porno-materiálů se různí. Jde jistě

o velmi individuální záležitosti, které nelze nijak globálně pojímat. Přinejmenším může u nedospělého jedince vzniknout, byť jistě dočasně, určitá nezdravá závislost na vyhledávání těchto artefaktů. A to s některými důsledky známými z oblasti drogových závislostí, jako je zanedbávání běžných denních povinností, školní docházky, finanční únik (zvýšené náklady za často celodenní či celonoční sledování Internetu) atd. Internet totiž poskytuje pohodlný a takřka anonymní přístup k těmto artefaktům s možností využití výhod maximálního soukromí např. v domácím prostředí. Některé rádoby seriozní firmy předřazují erotickým stránkám určitá varování, že vstup mohou odklepnout jen osoby starší 18-ti let, či osoby, které se necítí být frustrovány materiály erotické povahy. Prohlášení podobného typu jsou však asi tak účinná, jako různé okrasné nápisy „za odložené svršky se neručí„, umístěné poblíž míst právě k odkládání určených.

4.*Otázky prevence* jsou nejčastěji diskutovány v souvislosti s akceptováním určitých omezení přístupů k informacím se sexuální tématikou. Systémy, které zabraňují přístupu mládeži, či osobám bez zájmu o podobný druh materiálů, jsou založeny na dobrovolných konvencích. V praxi to znamená, že tyto systémy sice existují (nebo je v některých zemích vyžaduje zákon), ale ve skutečnosti neexistují prostředky následné kontroly. Technicky se omezení realizuje adjunkcí speciálního programu k prohlížeči, který pak zamezuje přístup k jistým předem nastaveným místům (negativní pojetí), nebo naopak umožňuje pohyb jen po určitých adresách (pojetí pozitivní). Podoba serveru je limitována zákony země, kde se server nachází, ale prohlížení či stáhnutí artefaktů podléhá úpravám země, kde uživatel právě žije. Vzhledem k objemu datových transakcí je velkým problémem podobnou aktivitu monitorovat. Až na naprosté výjimky několika soudních postihů, panuje stav velké liberality až anarchie. Platí, že čím stabilnější je existence serveru a čím více se majitel nebo správce snaží s pornografií obchodovat, tím více respektuje zákony a další veřejné požadavky. Dobrovolně se nechává registrovat u ratingových organizací, používá různých upozornění apod. Malé a dočasně vznikající firmy naproti tomu nerespektují prakticky žádné zásady. V případě stížností nebo žaloby prostě stránku zruší a na jiném místě ve světě založí jinou. O ochraně vložením *varovné vstupní stránky* jsme se již zmínili.V některých případech jde snaha provozovatelů tak daleko, že uživatel stvrzuje, že nebude žalovat správce serveru. Jiným způsobem ochrany jsou opatření pomocí *ratingových systémů,* na základě nichž se uživatel může předem dovědět, jak „tvrdá„ je která stránka. Např. jeden z nejrozšířenějších amerických systémů hodnotí artefakty podle míry násilí, formy presentování nahoty, míry sexu a jazykové vytříbenosti slovních projevů. V kontextu kulturních vzorců starého kontinentu lze však pochybovat o tom, že by pomocí tohoto systému mohlo jít o seriozní řešení otázek hodnocení materiálů na Internetu.

Lokálně účinnými, avšak z hlediska svobody projevu a přístupu k informacím diskutabilními, mohou být určitá omezení činnosti zaměstnanců s Internetem na pracovištích. Zaměstnavatel tím chce většinou docílit lepšího využívání pracovní doby, případně též úspor na telefonních poplatcích. Rozumný zaměstnavatel však vždy ponechá určitý prostor svým pracovníkům k relaxaci a odpočinku, což je žádoucí zejména tam, kde se kladou vysoké nároky na psychiku a duševní činnost.

Jisté možnosti prevence skýtá také státní daňová politika, vhodně modifikovaná k usměrnění, či útlumu nežádoucích pornografických aktivit.

5.*Otázky represe* by měly být vždy jen v rukou kvalifikovaných orgánů k tomu školených. Téměř všichni policejní specialisté se shodují v tom, že represe implikované delikty v prostředí Internetu jsou poměrně problematické, ať zdůvodnitelností, či svým rozsahem, praktickou proveditelností, tak i účinností. Týkají se především dětské pornografie, porušování autorských práv, nedovolených průniků, skandalizací veřejně činných osob apod. Nesnadnost práce represivních orgánů dokládá tento případ, který se stal v roce 1999 u nás. Pro usnadnění práce si jeden pracovník policie soukromě (bez vědomí nadřízeného) vytvořil webovou stránku s výzvou uživatelům Internetu , aby ho upozornili na případný výskyt dětské pornografie. Původ stránky byl podroben nezávislému policejnímu šetření, protože se nevědělo, zda nejde o výtvor psychopata. Po vyjasnění případu se policie od této aktivity svého pracovníka plně distancovala. O postihu pornografie na Internetu platí dále jinak v podstatě to, co již bylo řečeno dříve v souvislosti s jinou trestnou činností.

Kategorizace produkce jako vodítko k řešení problémů. Problémy s pornografií na Internetu podle uvedených problémových okruhů nelze řešit paušálním přístupem, nýbrž výlučně posuzováním konkrétních případů. Zdá se, že z hlediska kriminálních aspektů jsou textové pornografické projevy (povídky, reportáže, eseje apod.) nejméně problematické. Závažnější situace je u frekventovanějších forem, tedy především u presentace fotosnímků. Někteří velcí producenti se chlubí databázemi erotických fotografií o rozsahu statisíců položek. Z nich pak na Internet vybírají denně nebo v určitých časových intervalech kolekce označované často také jako galerie. Tyto fotografie bývají posuzovány zpravidla podle zobrazených subjektů (zejména věku aktérů), podle extrémů v zobrazené situaci (póz, prostředí, doplňků, pomůcek, praktik) a celkového dojmu (vyzývavosti, vulgarity). Zobrazovanými subjekty jsou většinou ženy všech typů (včetně extrémně obézních), věku (i velmi vysokého) a barvy pleti (exotických typů). Rovněž se vyskytují také kolekce s homosexuální i transsexuální tématikou. V souvislosti s doplňky a pomůckami se lze setkat v krajním případě s určitými přechodně získanými tělesnými malformacemi či trvalým (někdy snad i vrozeným) znetvořením. Nesmírně velká škála existuje v zobrazování různých situací až po realizace extrémních fantazií ponižujících lidskou důstojnost. Vše při pózách modelů až po neobvykle vyzývavé polohy (např. různé otevřené V-pózy, artistické kreace aj.) v soukromí i na veřejnosti, v interiérech i exteriérech.

Erotická produkce. U erotických materiálů nezobrazujících koitus nelze zcela jednoznačně hovořit o pornografii. To platí zejména pro tzv. soft-erotiku, která navíc respektuje ve značné míře i estetická měřítka. Sem patří i zobrazování celebrit, tedy známých osobností, hlavně zpěvaček a hereček. Určité problémy představují presentace těch snímků mladých dívek (školaček), které vzbuzují podezření na porušení zákona. Zde však mnohdy není zcela zřejmé, zda nejde např. o legální modelky s tzv. komplexem Lolity. Bezproblémové se zdají být i zobrazované doplňky (zpravidla ne více než ozdobný piercing na genitálu), či pomůcky a situace neurážející standardní vkus či lidskou důstojnost.

Formy pornografie problematické z hlediska trestního postihu. Obyčejná pornografie presentovaná na Internetu jako tzv. tvrdá pornografie (hardcore) zobrazuje většinou koitus v nejrůznějších polohách, včetně homosexuálních praktik, avšak nikoliv bizarní či jinak abnormální techniky. Tvorba i presentace těchto materiálů by měla být činěna s dobrovolným souhlasem aktérů starších 18-let, což producenti mnohdy dotvrzují. Na Internetu se lze setkat i s *ritualizovanou pornografií* naznačující neobvyklé praktiky formou hry (rituálu). Sem lze řadit fetišismus (aktéři s různými doplňky zavěšenými na těle, či oblečení do speciálních latexových či gumových obleků), předstírané sadomasochistické praktiky (bondáž, bičování, kartáčování) a s tím související a dobrovolně snášené ponižování lidské důstojnosti subjektů (zpravidla dominami). Dále se zde vyskytují jiné méně extrémní praktiky - např. vaginofilní (veggies, fisting), klinický sex (včetně zobrazení gynekologických nástrojů), gerontofilní aktivity, *voyeurské aktiviy* se snímky pořizovanými bez vědomí fotografovaných osob atd. V tomto případě nemusí jít o materiály agresivní či jinak abnormální povahy, které mohou dokonce respektovat i určité estetické zásady. Poměrně řídce zastoupené bývají snímky nehygienických nebo krvavých praktik vytvářené se souhlasem protagonistů. Patří sem např. koprofilie (praktiky označované jako kaviár), koprofagie, urinofilie, tvrdé sadistické praktiky, včetně krvavých (nikoliv ireverzibilních) apod. Na serverech s lehčími formami pornografie bývají tyto artefakty zařazovány nejčastěji do kategorie bizarních praktik. Jak tvrdí celkem ve shodě specialisté z nejrůznějších styčných oborů i zemí, postih většiny aktivit ve spojení s těmito formami pornografie je značně problematický. A to, jak z hlediska viny producenta, zprostředkovatele či konzumenta (poptávky), tak i inhibitorů negativních stránek společenského a technického pokroku, kteří toto vše umožňují. Samozřejmě, že legální proces postihu by měl nastoupit vždy, pokud orgány činné v trestním řízení dospějí k názoru, že v konkrétním případě byl porušen zákon.

Extrémně tvrdou pornografii na Internetu lze charakterizovat aktivitami, které hraničí s porušováním zákona nebo jej přímo porušují. Specialisté sem jednoznačně řadí dětskou pornografii, zejména tvrdou s explicitním koitem s nedospělým partnerem nebo jinými praktikami ukájení (cunnilingus, felace aj.). Je ovšem problematické, zda sem zařadit i jinak obyčejné snímky nahých dětí, např. při opalování, koupání, pobytu na plážích apod. Rozhodně sem však patří incest. Ovšem na incest proklamovaný pouhým textem pod obrázkem obyčejného koitu dospělých osob mohou být již názory poněkud jiné. Do extrémně tvrdých praktik lze zahrnout i nekrofilii, nekrosadismus (presentované někdy jako hororový sex) či praktiky natáčené a předkládané jako násilné (konkrétně znásilnění jako takové, tortury apod.). Trestní postih u artefaktů se sexuálním násilím může však být rovněž problematický s odkazem na analogie násilí beztrestně veřejně presentované téměř denně na televizních obrazovkách. Zde záleží asi opět na posouzení stupně společenské nebezpečnosti v jednotlivých případech. Na japonských serverech vedle poměrně krutých praktik (provazových bandáží), se vyskytuje dosti často dětská pornografie, ale s tím, že nejsou zobrazovány pohlavní orgány aktérů. V některých případech jsou tato místa dokonce retušována. I když principiální postih presentace extrémně tvrdých artefaktů v mnoha podobných konkrétních případech může být jasný, zpravidla ztroskotá na praktických

problémech realizovatelnosti, tak jak jsme o nich hovořili již dříve. Některé servery se vyznačují postupným zvyšováním tvrdosti nabízené pornografie. Mnohdy jinak běžnou produkci legálních vydavatelů přebírají (často s rizikem postihu za porušení autorského práva) a řadí ji do tvrdšího kontextu, např. vytvářením určitých dějových sekvencí nebo pouhým doplněním (též i vulgárních) komentářů.

Internetoví piráti. O zajímavé psychologii některých počítačových pirátů jsme se zmínili již dříve. Také na Internetu, vzhledem k povaze informací zde se vyskytujících, zejména pak jejich neomezené reprodukovatelnosti, jsou piráti typem delinkventů, kteří mohou uskutečňovat své aktivity v duchu zásady „bohatým brát a chudým dávat„. U běžných uživatelů bez přílišných skurpulí jsou pak velmi populární. Jde zpravidla o výjimečně schopné osoby, které na základě speciálních programů a hlavně svých znalostí pronikají do specializovaných serverů krytých hesly, kódy uživatelských kont, či jinými zámky. Odtud pak získávají materiály a kódy pro další nekalou činnost. *Pirát z přesvědčení* zastává názor, že informace patří všem. Za nemravné nepovažují volné presentování pornografie, nýbrž vymáhání peněz za její zpřístupňování. Jejich názory jsou často v souladu s filozofií odmítání globalizace světa, kapitalistického společenského zřízení, či alespoň přehnané komercionalizace. Proto ukradený software, počítačové hry či pornografické artefakty zpřístupňují široké veřejnosti nejčastěji prostřednictvím ilegálních serverů, kde mohou též uvádět seznamy přístupových hesel, nebo utajených lokací. Ve smyslu obvyklých právních úprav ve většině zemí jde přitom o porušování autorských práv, příp. dalších zákonných ustanovení.

Organizovaní piráti a nebezpečnost jejich aktivit. Internetoví piráti se v poslední době sdružují do uzavřených skupin, které kontrolují a regulují průniky na servery s pornografickou tématikou, aby nedocházelo k jejich přetěžování a posléze rušení. Členství v těchto *elitních komunitách pirátů* je ostře střeženo, přístup pro nováčky je možný po dodání dosud neznámého hesla na server, který je na seznamu vyhlášených. Organizovaní piráti disponují pokročilými informačními technologiemi a hlubokými znalostmi z oblasti programování a výpočetní techniky vůbec. Jejich činnost může v budoucnu překročit lokální rámec zájmové či rekreační specializace a hraničit tak s velmi nebezpečným organizovaným zločinem. Mohou paralyzovat ochranné systémy důležitých serverů s neblahými společenskými důsledky. Internet představuje totiž pro různé zájmové subkultury, včetně těch, co porušují zákon, vynikající prostor pro přenos a směnu nejrůznějších materiálů i operativních informací za dostatečně garantované anonymity. Pirátské aktivity v oblasti internetové pornografie jsou rozsáhlé. Lze je považovat za jednu z nejliberálnějších i nejnebezpečnějších činností na Internetu. Totiž, jakmile by byla přijata jakákoliv společensky nutná omezení (a nikoliv jen v oblasti pornografie), mohou se situace ujmout piráti. Proti těmto opatřením pak postavit nelegální aktivity na svých těžko identifikovatelných serverech a nabízet zakázané komukoliv, včetně aktivit sloužících expanzi organizovaného zločinu. Vše alespoň po určitou dobu, dokud nebudou nuceni své aktivity modifikovat nebo ukončit z obavy o odhalení. Vzhledem k

mimořádným technickým možnostem a znalostem organizovaných pirátů je šance na jejich dopadení poměrně malá.

Celkově lze říci, že v naší společnosti, snad i vzhledem k historicky podmíněnému odmítání ortodoxních církevních předsudků a pruderií, pojímáme již tradičně problematiku sexu, erotiky i pornografie s velkou mírou tolerance. To platí samozřejmě i o artefaktech v prostředí Internetu. Mnohdy ovšem občané reagují, např. ve sdělovacích mediích, již na pouhé vybočení ze vžitých kulturně-morálních vzorců s požadavkem represivního řešení bez opory v právní úpravě. Z toho ovšem nelze ještě vyvozovat závěry o deformaci či anulování přirozených principů právního povědomí občanů o nutnosti postihu těch případů, kdy dochází k faktickému porušování platných zákonů. Protože Internet není zatím prostředkem, který by u nás ještě plně zdomácněl, je nutno klást velký důraz na osvětovou činnost ve vztahu k *počítačovému právnímu vědomí* stále širšího okruhu obyvatelstva.

**

Na závěr zdůrazněme otázku mnohdy zbytečné *kriminalizace aktivit spojených s výpočetní technikou*. Při represivním postihu pachatele počítačové kriminality je nutno nejdříve zjistit, zda konkrétní osoba své konání nepostavila na dobré vůli, ať jakkoli pochybné. Dále je třeba zvažovat, zda k dosažení nápravy nestačí prostředky např. obchodního zákoníku, a je nutno sáhnout k tvrdšímu zákonu trestnímu. Z běžné praxe je vidět, že si mnozí v naší zemi zvykli na to, že zákon lze obcházet podle potřeb vlastního prospěchu, bez ohledu na ostatní. Pak musí nastoupit žádoucí prosazení zákona a nekompromisní postup vůči osobám, které ho porušují, podle zásady „padni komu padni„. I tím lze naplnit alespoň zčásti generálně preventivní účinek našeho právního systému vůči počítačové kriminalitě.

Pokud jde o aktuální boj se softwarovým pirátstvím, je třeba adekvátně vnímat a posuzovat extrémní postoje a aktivity, které se v poslední době vyskytly zřejmě ve spojitosti s konkurenčním bojem některých organizací. Nutno odmítat skutky, které vedou ke globálním generalizacím zkratkově charakterizujícím uživatelskou veřejnost jako národ zlodějů, udavačů, či zastánců falešné solidarity.

Literatura

Abrams,M.D.,Podell,H.J.: Tutorial Comp.and Network Security. Comp.Soc.Press, Washington 1987

Aktuální otázky práva autorského, práv průmyslových a práva soutěžního, sborník. UK, Praha, 1995

Ameriku ohrožují počítačoví piráti. Kriminalistická společnost 2/1997

Arkin,S.S. a.coll.: International Corporate Security of Computers, MBC, N.York, 1991

Austen,J.: Praktické příklady vyšetřování počítačové kriminality. Krim.společnost 3/1991

Až 70 procent software je v ČR využíváno nelegálně. Metro 6/10/1998

Bainbridge,D.I.: Introduction to Computer Law. Pitman, London 1993

Baker,R.F.: Avoiding Virus Infections. California Lawyer 6/1992, p.45

Baudyš,P.: Viry a červi. Internet, COMPUTERWORLD 26/97

Bečvář,J.: Loupeživý hacker. Internet WWW, 1998

Bellach,B.M.,Borning,A.: Hypotéza o perseveranci při páchání trest.činů. Kriminalistika 2/1993

Beneš,A.,ml.,Matyáš,V.,ml.: Víceúrovňová bezpečnost. Internet, COMPUTERWORLD 32/97

Bequal,A.: Computer Related Crime. Strasbourg. CE, 1990

Best,R.A.,Picquet,D.Ch.: Computer Law and Software Protection. McFarland, London 1993

Bímová,A.: Některé charakteristiky pachatelů počítačové kriminality, Čs.kriminalistika 1/1991

Bímová,A.: Počítačová kriminalita a naše doba, IDG, Praha,1990

Boháček,M.: Autorskoprávní ochrana a počítačové programy. Průmyslové vlastnictví 1/1995

Boháček,M.: Počítačové programy a novela autorského zákona. Systém integrace 4/1996

Boháček,M.: Právní ochrana počítačových programů. Systémová integrace 1/1995

Boháček,M.a kol.: Právo průmyslovéhoa jiného duševního vlastnictví. VŠE, Praha 1994

Boj proti softwarovému pirátství. Informace Úřadu pro zahraniční styky, 8/98

Bologna,J.: Computer Crime. Data processing and Communications Security, 2/1986, p.30-32

Bomba z Internetu zranila švédské studenty. Kriminalistická společnost 2/1997

Budka,I. a kol.: Základy činnosti kriminální policie, Policejní akademie ČR, Praha 1997

Budka,I.: ECNA a SOCIO-software pro zpravodajskou kriminální službu. Kriminalistika 4/1994

Bůh má vlastní e-mailovou adresu. Kriminalistická společnost 2/1997

Cailolois,R.: Struktura a klasifikace her, Analogon, 6/1992, s.1-5

Cejp,M.,Osmančík,O.,Scheinost,M.: Druhy a formy organizovaného zločinu. IKSP, Praha 1996

Collier,P.: Crime and the Computer, M.Wasik,Univ.Press,Oxford 1991. Brit.Journal of Criminology 1/93

Computer Crime. Criminal Justice Resours Manual. U.S.Dep.of Justice, 1979

Computer Crimes. High-Tech Theft. Paladin Press. Boulder 1990

Cooper,J.A.: Computer-Security Technology. Lexington Books, Lexington 1984

Cyriax,O.: Zamyšlení nad Encyklopedií zločinu. Kriminalistická společnost 3/1996

Česká republika špatně střeží duševní vlastnictví. Metro 8/10/1998

Dastych,J.: Elektronický obchod s paragrafy. Internet WWW, 1998

Dastych,J.: Morální aspekty softwarového pirátství. Internet WWW, 1998

Dastych,J.: Piráti. Internet WWW, 1998

Dastych,J.: Pirátské vody na WWW. Internet WWW, 1998

Dastych,J.: Počítačová kriminalita, Internet WWW, 1998

Dastych,J.: Softwarové pirátství. Policista 2/1998

De Mulder,R.,Kleve,P.: Centre for Computer and Law. EU Rotterdam. Čas.pro práv.vědu a praxi 6/94

De Mulder,R.,Kleve,P.: The New Computer Crime Act in the Netherlands. IKSP 1994.

Deidel,D.: Computerkriminalität in den kapitalist. Industrielandern, Staat u.Recht, 2/1988, s.65-67

Denning,P.J.: Stopping Computer Crimes. American Scientist 1/1990, p.10

Dijk,J.J.M.,Mayhevová: Kriminální viktimizace v industrializovaném světě. IKSP 1992

Dočkal,J.: Bezpečnost databází. Internet, COMPUTERWORLD 25/97

Dočkal,J.: Bezpečnost počítačové sítě. Internet, COMPUTERWORLD 4/98

Dooley,A.: Crime Time, Copmuterworld 5/1989, s.30-32

Dreier,T.: The Intrnat.Development of Copyright Protect.for Comp.Programs.HESL. Lehman a T.,1993

Drgonec,J.: Počítačová kriminalita podle práva platného v SR. Právny obzor 2/1993

Drgonec,J.: Počítačová kriminalita. Justičná revue 8-9/1991

Drumm,H.E.: Copyrighting Computer Programs. C.Boardman, New York 1984

Resumé

Perspektiva neustále rostoucího významu informačních technologií, nepřehledný rozsah informací o kriminalitě páchané ve spojitosti s počítači, rozptýlený po často již méně dostupných pramenech a konečně i zcela nové aspekty tzv. informační kriminality byly motivem k sestavení tohoto kompendia. Jsou zde pojednány názory specialistů nejen k počítačové kriminalitě samé, ale i k úzce souvisejícím otázkám počítačové bezpečnosti, prevence a represe, speciálně pak ke strategii a taktice boje s počítačovou kriminalitou. Kromě toho je věnována též pozornost novým poznatkům a metodám v oblasti chování a studia osobnosti pachatele počítačové kriminality. Text je členěn celkem do deseti kapitol, tyto pak na oddíly s bloky a odstavci obsahujícími alespoň zhruba kompaktní problematiku. V závěru práce je uveden seznam literatury zahrnující tituly, z nichž bylo čerpáno.

Příloha č. 1

Slovníček základních počítačových výrazů a zkratek

Název	Výklad	Význam
2	too, to = příliš, pro ap.	Užívá se v hackerském slangu, např. *2morrow* = tomorrow, 2*me* = to me.
4	for(e) = pro	Užívá se v hackerském slangu, např. *b4* = before.
!	negace	Užívá se v hackerském slangu. Např.: *!expected* = *unexpected*.
&c	atd. (et cetera)	Užívá se v hackerském slangu.
@-party	schůzka uživatelů Internetu	Užívá se v hackerském slangu.
[]	nejistota	Užívá se v hackerském slangu. Př.: *Al[f[ph]]a* může být *Alfa* nebo *Alpha*.
<ethnic>		Užívá se v hackerském slangu namísto označení etnické skupiny, zejména ve vtipech (není-li známo kdo je na druhé straně).
<G>	Big grin - úsměšek, výraz smíchu nebo ironického mínění	Užívá se v hackerském slangu, též: -)))) nebo :->
A Binary digit	binární číslice	Buď 0 nebo 1. Nejmenší prvek počítačového programu. 8 bitů = 1 byte.
aaa	přes všechna rizika (against all risks)	Užívá se v hackerském slangu.
ACK	Jsi tam? (Acknowledge)	Užívá se v hackerském slangu. Př.: *ACK NAK* Jsi tam? Ne nejsem.
ActiveX		Standard Microsoftu pro připojitelné, okamžitě použitelné OLE komponenty přes Internet.
advTHANKSance	Předem díky (thanks in advance)	Užívá se v hackerském slangu.
afaik	pokud vím (as far as I know)	Užívá se v hackerském slangu.
aka	alias, známý také jako... (also known as)	Užívá se v hackerském slangu.
angry fruit salad	nepřehledná struktura programu	Užívá se v hackerském slangu.
aos	jedno po druhém (ad one and do no skip)	Užívá se v hackerském slangu.

Applet		Jméno třídy aplikací, navržených a vyvinutých pro Internet. Říká se jim applety, protože to nejsou úplné aplikace, ale pouze části velkých aplikací. Jsou to aplikační moduly, používané na web stránkách, vyvinuté v Javě, ActiveX nebo jako přídavé moduly (plug-ins).

armor-plated	neprůstřelný program	Užívá se v hackerském slangu.
as blind as a bat	slepý jako patrona	Užívá se v hackerském slangu. *B-I* = slepecké brýle.
as daft as a brush	blbý jako tágo	Užívá se v hackerském slangu. Př.: <: blbec, :-] další blbec.
asap	co nejrychleji	Užívá se v hackerském slangu, ale též běžně v korespondenci (as soon as possible).
automagicall	proces probíhá, avšak poněkud záhadně - nevím jak jsem toho docílil	Užívá se v hackerském slangu.
awhfy	Je to pořád ještě legrace? Myslíš to vážně? (are we having fun yet?)	Užívá se v hackerském slangu.
B	be = být	
Backslash	lomítko	Jiný výraz pro "\".
Baud	Bits At Unit Density	Jednotka přenosové rychlosti rovná počtu změn stavu nebo podmínek za vteřinu. Hodnota v baudech obvykle říká počet bitů, přenesených za jednu vteřinu.
Bits	bity, A Binary digit	Buď 0 nebo 1. Nejmenší prvek počítačového programu. 8 bitů = 1 byte.
BPS	Bits-Per- Second	Jednotka rychlosti (bity za vteřinu), jak rychle se přemísťují data z jednoho místa na druhé. 28,8K modem dokáže přenést 28.800 bitů za vteřinu.
Brute force attack	útok hrubou silou	Způsob zjišťování hesel, kdy crackovací program zkouší všechny existující kombinace, až najde skutečné heslo. Tento způsob může být časově velmi náročný, ale nese jistotu, že dříve nebo později bude správné heslo odhaleno.

Byte		Základní jednotka, se kterou pracuje počítač. Je to skupina binárních číslic, obvykle 8, které se často používají ke zobrazení jednoho znaku.
C	see = vidět	Užívá se v hackerském slangu např. *CU* = see you, naviděnou.
Cat	kočka	Jiný výraz pro "@", slang.
CGI	Common Gateway Interface	Konvence mezi implementátory HTTP serverů, jak integrovat skripty styčných prvků (gateways) a programů, napsaných v jednom z mnoha populárních jazyků: C, C++, Perl, TCL nebo jako shell skript. [viz HTTP].

Název	**Výklad**	**Význam**
Client	klient, program	Program, který požaduje služby od jiných programů (serverů), které mohou, nebo nemusí být umístěny na stejném fyzickém počítači.
Client/ Server		Vzor aplikační architektury, která zdůrazňuje modularitu a komponentový přístup. Třívrstvá klient/server architektura se skládá ze tří hlavních částí. Jsou to: prezentační vrstva, funkční vrstva a datová vrstva. V současnosti je to převládající model návrhu aplikací. Dvouvrstvý klient/server model dělí aplikace pouze na dvě složky, a to buď na: vrstvu prezentačně/funkční a vrstvu datovou nebo na vrstvu funkčně/datovou a vrstvu prezentační.
com	commercial	Doména na Internetu USA - komerční.
Compression	omprese	Technika zhuštění a prezentace obrazu, textu, audia nebo jakéhokoli jiného média malým počtem bitů. Používá se pro zrychlení Internetových přenosů obrázků a videa, pro kopírování nebo vzdálené prohlížení. Komprimace objektu si vynucuje v místě určení dekomprimaci do původní nebo velmi podobné podoby.
Cookie	koláček sušenka	Informace o uživateli, o počítači uživatele a o výsledné stránce, kterou sebou nese HTTP požadavek. Tato informace se na webovské stránce, ani nikde jinde, obvykle nezobrazuje; je dostupná pouze přes programátorské rozhraní.

cracker	lámač, křupač	Nabourávač do systémů, za hranicí zákona, zloděj a škodič dat. Laická veřejnost většinou nevnímá rozdíl mezi crackery a hackery (viz též) a označuje všchny crackery slovem hacker.
cz	www.__.cz	Doména na Internetu ČR (pozor cr=Costarica).
DCE	Distributed Computing	Environment. Standard, založený na RPC a definovaný nadací Open Software Foundation, pro distribuované aplikace.
Denial of service	druh útoku proti NT	Spočívá v paralyzování nějaké služby na pracovní stanici nebo serveru.
DES	Data Encryption Standard	Standard pro šifrování dat. Šifrovací algoritmus pro ochranu neklasifikovaných počítačových dat. Není povolen pro národní bezpečnost nebo pro klasifikované dokumenty. Tento algoritmus není dovoleno exportovat mimo území USA.

Název	**Výklad**	**Význam**
Dictionary attack	slovníkový útok	Crackovací program zkouší jako možné heslo všechna slova v určitém slovníku. Je to metoda rychlá, ale neskýtá jistotu úspěchu. Zaleží to na rozsahu slovníku a na tom, zda objekt útoku je zabezpečen jednoduchým heslem.
DME	Distributed Management Environment	Soubor služeb pro řízení a správu aplikací v DCE.
Domain Name	jméno domény	Unikátní jméno, které identifikuje Internetovský uzel (např.: ctgroup.com). Má vždy dvě nebo více částí oddělených navzájem tečkami. Část vlevo od tečky je nejkonkrétnější, část vpravo nejobecnější
edu	education	Doména na Internetu USA - vysoké školy, vzdělávací instituty, nekomerční.
E-mail	elektronická pošta	Zprávy, obvykle textové, které posílá jedna osoba druhé pomocí počítače. Zprávu lze automaticky poslat na velké množství adres.

Encryption	šifrování (enkripce)	Proces, při kterém se převádí prostý text na ekvivalentní číselný text pomocí kódu nebo se ke zprávě připojují kontrolní symboly, pro potřeby generování kódu detekce a opravy chyby. Dále je to metoda utajení a zabezpečení dokumentů, přístupových hesel nebo integrity informací mezi zúčastněnými stranami.
Firewall	ochranný val	Spojení HW a SW povolující pouze autorizovaný přístup k funkcionalitě na druhé straně „zdi“.
Gateway	brána	HW nebo SW mechanismus, který provádí převod mezi dvěma různými protokoly. Libovolný mechanismus, zprostředkovávající přístup k funkcionalitě nebo datům jiného systému.
GIF	Graphics Interchange Format	Typ souboru, který se používá k posílání komprimovaného obrazu standardního formátu.
Glass-Stiegel Act	Glass-Stiegelův zákon	Zákon, který odděluje banky od obchodování a obchodníky od bankovnictví.
Gopher		Internetovský protokol, který přímo přecházel WWW, vytvořen byl na universitě v Minnesotě. Je to jednodušší systém než HTTP Webu.

Název	**Výklad**	**Význam**
hacker	průnikář, sekač	Nabourávač do systémů, na samé hranici zákona, hackerská etika však zakazuje jakkoli datům škodit (srov. cracker). Původně označoval termín hacker jen člověka s větší zálibou v programování, který nejevil snahu pronikat do systémů či škodit jiným počítačovým sítím.
hackspeak	hekerská řeč	Dorozumívají se prostřednictvím klávesnice, proto zkracují výrazy - viz příklad : *ACK NAK (Jsi tam? Ne nejsem!).*
Home Page	domovská stránka	První HTML (HyperText Markup Language) stránka, kterou uživatel vidí na World Wide Web uzlu. Představuje obraz společnosti nebo jednotlivých projektů, podávaný uživatelům Internetu. [viz HTML].

HTML	HyperText Markup Language	Jazyk pro psaní a čtení Webových stránek. Na rozdíl od běžných textových dokumentů, HTML je univerzální pro PC, Macintosh i UNIX.
HTTP	HyperText Transfer Protocol	Standard dekódování v počítačové komunikaci přes Internet pro předávání dokumentů na webu.
HW	hardware	Hmotně-technická podstata počítače.
Hyperlink		Cesta mezi dvěma dokumenty, která uživateli umožňuje kliknout na určité slovo na obrazovce a tím se přenést do požadovaného místa kdekoli na Internetu.
Hypertext		V zásadě libovolný text, který obsahuje „linky“ na jiné dokumenty - slova, grafiku nebo fráze v řádku dokumentu, které může čtenář vybrat a tak se dostat k dalšímu dokumentu, který se mu pak zobrazí.
Intranet		Privátní síť, která využívá stejné softwarové standardy jako Internet, ale která má další HW a SW omezující externí přístupy.
IP spoofing		Poměrně složitá hackerská technika, kdy hackerův počítač předstírá IP adresu někoho jiného, aby se dostal k neautorizovaným informacím. Je to použitelné zejména u systému UNIX a jemu podobným.
IPX	Internet Packet Exchange	Nižší síťový protokol používaný Novellem při provozování jeho populárního síťového software.
ISP	Internet Service Provider	Firma, která tím, že poskytne rozhraní na páteř Internetu, umožňuje společnostem i jednotlivcům připojení na Internet.

5

Název	**Výklad**	**Význam**
Java	speciální programovací jazyk pro Internet	Jazyk vyvinutý firmou Sun Microsystems. Je to jazyk podobný C++. Užívá se především pro vývoj Internetových aplikací. Používá se k vytváření appletů pro web stránky i samostatných Internetovských aplikací. Je to vývojový jazyk a prostředí pro Internet.

JPEG	Joint Photographic Experts Group	Komprimovací algoritmus jak pro barevný tak i černobílý digitální obraz, „přirozených“ výjevů skutečného světa.
Keylogger	speciální program	Program zaznamenávající stisknuté klávesy. Všechny klávesy, které uživatel na daném systému stiskne, jsou zaznamenány do textového souboru, který si pak může hacker přečíst. Pro NT je asi nejlepší *Invisible keylogger for NT*, který dokáže zaznamenávat bez vědomí uživatele klávesy i během přihlašování.
LAN	Local Area Network	Decentralizovaný hrozen propojených počítačů.
MIME	Multipurpose Internet Mail Extensions	Standard jak posílat zprávy více adresátům, multimediální a binární data s využitím celosvětového Internetového systému elektronické pošty, např. obrázky, audio, textové dokumenty, programy nebo prosté textové soubory.
MPEG	Moving Picture Experts Group	Standard navrhovaný ISO, pro kompresi animovaných obrázků digitálního videa a audia. Původně byla během definičního procesu MPEG-2 plánována aplikace pro veškeré přenosy videa profesionální kvality.
Multitasking	Multiúkol	Zpracování většího počtu úloh počítačem najednou.
NetBuse	speciální program	Program na dálkovou kontrolu počítače.
NT	počítačová síť	Propojení většího počtu počítačů pomocí ústředního počítače, serveru.
OLE	Object Linking and Embending	Odvětvový standard, vyhlášený Microsoftem, pro objektově orientované zpracování a komunikaci.
Packet sniffer	produkt z oblasti hackerských programů	Zachytávač packetů, lze pomocí něho zachytávat veškerou síťovou komunikaci, ke které je zřízen fyzický přístup. Zachytávání packetů je určeno však pouze pro pokročilé, kteří se dokonale vyznají v síťové komunikaci.
Password cracker	speciální program	Program určený k luštění hesel, např. pro WinNT je to L0phtcrack. Password crackery používají buď metodu Brute force nebo Dictionary attacku, viz též.
Páteřové vedení - Backbone		Vysokorychlostní linka nebo soubor propojení, které tvoří hlavní průchod sítí.

Pevná linka		Telefonní linka vyhrazená pro klienta bez přerušení spojení. Jde o úsporu času při navazování spojení a výhodnější poplatky za vytížení linky.
PGP	Pretty Good Privacy	Metoda šifrování dat, umožňující lidem bezpečně komunikovat na Internetu.
Phreaker	hacker telefonních sítí	Jedinec, který se zabývá neoprávněným pronikáním do telefonních systémů. Většinou tím sleduje profit, méně často jiné osobní uspokojení (např. při určitých sexuálních úchylkách).
POP	Přístup na Internet Point of Presence	Termín, používaný poskytovateli Internetových služeb pro označení zeměpisných lokalit a počtu jejich přístupů na Internet.
POP-3	Post Office Protocol 3	Standardní protokol využívaný aplikacemi Internetové pošty.
Port		Vstupní a výstupní součást HW počítače.
Port scanner	speciální testovací program	Programy na testování otevřených portů; v dnešní době už se však příliš nepoužívají. Asi nejlepším příkladem Port Scanneru pro NT je YAPS.
PPP	Point-to-Point Protocol	Nejznámnější protokol, umožňující počítači použít pro navázání TCP/IP spojení normální telefonní linku a modem a dostat se tudíž na Internet. V těchto případech nahrazuje PPP postupně SLIP.
Provider	poskytovatel	Poskytovatel připojení k síti.
Proxy Server		Server uchovávající často hledané dokumenty, může být umístěn ve vaší lokální síti, nebo přímo ve vašem počítači.
SAM	Security account manager	Databáze, ve které se uchovávají například hesla uživatelů. Hesla v NT se např. nacházejí adresáři c:\winnt\repair a c:\winnt\config a v registrech.
Search Engine	vyhledávač	Internetovská aplikace, která pomáhá uživateli nalézt Internetovské dokumenty a uzly, obsahující určité informace. Tento vyhledávač má dva systémové prostředky: registraci a vyhledávání. Nové uzly se zaregistrují, indexují a zařadí do katalogu ve vnitřní databázi vyhledávače. Pokud uživatel požaduje dokumenty nebo uzly, obsahující určitá slova nebo fráze, prohledá se nejprve tato databáze, zda neobsahuje příslušné stránky a podle toho vyhledávač reaguje.
Server	ústřední počítač sítě	Umožňuje vzájemné propojení počítačů a provoz takové sítě počítačů.
sk		Doména Internetu Slovenska (pozor sr=Surinam, sl=Sierra Leone) .
Slash	lomítko (též slosh)	Jiný výraz pro "/".

Název	Výklad	Význam
Stroke	lomítko	Jiný výraz pro "/".
Strudel	štrůdl	Jiný výraz pro "@", slang.
SW	software	Podstata "náplně" počítače umožňující jeho provoz, systémy programů.
TCP/IP	Transmission Control Protocol/Internet Protocol	Standard, konektově orientovaný, plně duplexní protokol host-host, užívaný pro komunikaci v počítačových sítích s přepínáním paketů, jako je Internet.TCP těsně koresponduje s ISO Open Systems Interconnection-Reference Modelem (OSI-RM) Vrstva 4 (Transportní vrstva).
Telnet		Softwarové služby, které jsou součástí většiny operačních systémů, umožňující uživateli vstupovat do systému, jako kdyby používal terminál daného systému.
Trojan	speciální kamuflážní program	Program, který je zdánlivě určen pro jinou činnost než kterou ve skutečnosti realizuje. Například trojan zvaný *Picture.exe*. Když bývá otevřen, zobrazí nějaký obrázek, ale mezitím instaluje *NetBuse*, což je program na dálkovou kontrolu počítače.
U	you = ty	Užívá se v hackerském slangu, např. *4u* = for you.
UNIX		Operační systém vyvinutý ve spolupráci MIT a AT&T, který používají a podporují téměř všichni dodavatelé. UNIX využívá jako standardní komunikační protokol TCP/IP, což z něj činí jeden z nejoblíbenějších operačních systémů pro Internet.
URL	Uniform Resource Locator	Obecné jméno libovolného souboru, který lze přenést web protokolem. Týká se to těchto typů souborů: FTP, HTTP a Gopher.
Vyhledávač		Program umístěný na serveru, který prohledává ostatní servery. Takto lze najít jakékoli heslo obsažené ve všech textových stránkách na WWW. Program je zpravidla seřadí odkazy podle výskytu hledaného slova.
Web Page		HTML dokument na webu.
Web Server		HW a SW vybavení, z něhož může Internet (nebo Intranet) číst a zobrazovat dokumenty přes přenosový protokol hypertextů (HTTP). Soubory mohou být audio klipy, video, grafické nebo textové.

Wordlist	speciální seznam slov	Seznam slov pro použití s password crackerem, většinou abecedně uspořádaný . Je nutný pro dictionary attack. Čím větší wordlist, tím větší je šance na rozluštění hesla. Bývá používán o rozsahu až 30 i více MB.

8

Název	**Výklad**	**Význam**
World Wide Web	WWW	Mechanismus, vyvinutý Timem Berners-Leeem pro fyziky CERNu, aby mohli sdílet dokumenty přes Internet. Web umožňuje uživatelům přístup k informacím ve všech systémech na celém světě, které používají k identifikaci souborů a systémů URL (Uniform Resource Locators) a hypertextové linky pro pohyb mezi soubory ve stejném nebo v různých systémech.
WWW	World Wide Web	Obecně uznávaná zkratka pro World Wide Web, také web nebo W3.
Yahoo!		Jeden z nejpopulárnějších vyhledávačů uzlů. Tento uzel má vlastní databázi Internetovských uzlů rozdělenou kvůli efektivnějšímu vyhledávání podle kategorií.
YAPS	Port scanner pro NT	Program pro testování otevřených portů.
zavináč	@	Hovorový výraz pro symbol @, nejčastěji ve významu oddělovače v adresách internetové elektronické pošty.

Příloha č. 2

POČÍTAČOVÁ KRIMINALITA

STRUČNÝ PŘEHLED

{1} Dastych, Jiří: INTERNET, http://hysteria.sk/udc/bw.html, 1999.

Rozčlenění počítačové kriminality v kontextu trestního zákona ČR podle autora přehledu {1}

Autor přehledu {1}, jako policejní specialista na počítačovou kriminalitu, vychází z aktuálnosti daného tématu, ale upozorňuje, že jím podané informace nemusí být v souladu s pojetím některých dalších odborníků.

Přímá a nepřímá počítačová kriminalita

Rozlišujeme *přímou a nepřímou* počítačovou kriminalitu.

Přímou počítačovou kriminalitou je např.

-ilegální výroba počítačové techniky (hardware) kopírující cizí vzory,

-ilegální kopírování programů (např. software), tj. počítačové pirátství,

-neoprávněné užívání práce počítačů (krádeže strojového času),

-ničení a poškozování počítačů a programů (počítačové sabotáže),

-neoprávněné získávání informací z databází.

Nepřímou počítačovou kriminalitou je např.

-vkládání lživých dat do počítačového systému,

-měnění výsledků počítačového zpracování dat,

-měnění programu.

Některé z těchto forem počítačové kriminality jsou praktikovány i zločineckými organizacemi při zahlazování vlastní kriminality, při vytváření podmínek pro praní špinavých peněz i pro další trestnou činnost. Počítače mohou být významným prostředkem i na úseku hospodářské kriminality při zkracování daní a jiné nekalé činnosti. Někteří autoři vylučují z počítačové kriminality ty trestné činy, v nichž počítač figuruje pouze jako předmět útoku, věc, tedy jeho krádež a poškození, pokud ovšem

útok nesměřuje k technickému nebo programovému vybavení počítače. Pro zjednodušení vynechávají i čistě softwarové pirátství, ačkoliv jistě představuje značný problém.

Skutky řazené pod počítačovou kriminalitu

Pod pojem počítačové kriminality mnozí autoři řadí následující skutky:

1. Útok na počítač, program, data, komunikační zařízení.

Zde se prolínají dvě roviny - útok na fyzický objekt počítače nebo jeho příslušenství (odcizení, poškození) a útok na informace v počítači uložené.

2. Neoprávněné užívání počítače či komunikačního zařízení.

Patří sem např. počítání "cizích" úloh na počítači, používání programů nebo komunikačních zařízení, které náleží někomu jinému, bez jeho vědomí a souhlasu.

3. Neoprávněný přístup k datům, získání utajovaných informací (počítačová špionáž) nebo jiných informací o podniku, výrobě, osobách atp.

Nestačí pouhý průnik do databází, nýbrž musí dojít k neoprávněnému zneužití získané informace.

4. Změna v programech a datech (okrajově i v technickém zapojení počítače či komunikačního zařízení).

Sem patří

-změna programu a dat jinými programy - obvykle viry nebo přímými zásahy programátora (což je časté např. při tzv. počítačových defraudacích),

-méně běžné úpravy v zapojení nebo jiném atributu technického vybavení počítače či komunikačního prostředku.

5. Zneužívání počítačových prostředků k páchání jiné trestné činnosti.

Manipulace s počítačovými daty má pro pachatele určité výhody, např.

-vymazání či přemazání údajů na magnetickém mediu je podstatně snazší než v papírových dokladech a nezanechává prakticky žádné stopy,

-méně zasvěcený člověk (zákazník, někdy i povrchní kontrolor aj.) z psychologického hlediska považuje výsledky z počítače a priori za správné a více jim důvěřuje,

-při nedostatečně zabezpečeném systému lze spoléhat v souvislosti s neoprávněnými manipulacemi na určitou míru anonymity.

6. Podvody páchané v souvislosti s výpočetní technikou.

Pachatel již předem vytváří program, který mu má později usnadnit jeho trestnou činnost.

Softwarová krádež

Softwarovou krádeží rozumíme kopírování software bez povolení vlastníka copyrightu. Formy softwarových krádeží jsou různé, např. neautorizované vytváření duplikátů, neautorizované kopírování programů pro vlastní užití a prodej software chráněného autorskými právy či copyrightem ve tvaru blízkém originálu, uložení na pevný disk počítače dealerem nad rámec dohody s vlastníkem software atd.

Zjednodušené členění

Při určitém zjednodušení lze počítačovou kriminalitu rozdělit do dvou základních skupin na

-delikty, kde počítač (program, data atd.) je nástrojem zločince,

-delikty, kde počítač (program, data atd.) je cílem zločinného útoku.

Porovnání klasifikace materiálu *Rady Evropy* s ekvivalenty v našem trestním zákoně

Rada Evropy	Česká Republika
počítačové podvody	podvod - par. 250, 250a
počítačové falzifikace	
poškozování počítačových dat a programu	poškozování a zneužití záznamu na nosiči informací - par. 257a
počítačová sabotáž	sabotáž - par. 97, obecné ohrožení par. 179 - 180, poškozování cizí věci par. 257
neoprávněný přístup	neoprávněné užívání cizí věci - par. 249
neoprávněný průnik	neoprávněné užívání cizí věci - par. 249
neoprávněné kopírování autorsky chráněného programu	porušování autorského zákona - par. 152
neoprávněné kopírovaní topografie	porušování autorského práva - par. 152, porušování práv k vynalezu a průmyslovému vzoru - par. 151 (dále také podle zák. č. 529/91 Sb. o ochraně topografií počítačových výrobků)
změna v datech nebo počítačových programech	poškození a zneužití záznamu na nosiči informaci - par. 257a
počítačová špionáž	vyzvědačství - par. 105, ohrožení státního tajemství - par. 106, ohrožení hospodářského tajemství - par. 122, ohrožení služebního tajemství - par. 173
neoprávněné užívání počítače	neoprávněné užívání cizí věci - par. 249
neoprávněné užívání autorsky chráněného programu	porušování autorského zákona - par. 152

{1} Dastych, Jiří: INTERNET, http://hysteria.sk/udc/bw.html, 1999.

Příloha č. 3

Informační a počítačová bezpečnost

Aktuálnosti po uzávěrce literatury

Nová technologie likviduje viry

Pod názvem Striker32 uvedla firma Symantec nejpokročilejší technologii zjišťování a opravy virů navrženou pro boj s rostoucí hrozbou komplexních 32-bitových virů ve Windows. Technologie, zahrnutá v produktech Norton AntiVirus, pracuje na základě virtuálního "čisticího prostoru", v němž podezřelý program může běžet, zatímco Striker32 analyzuje, zda je program infikován. Infikovaný soubor je bezpečně izolován používáním tzv. karantény a funkce Scan and Deliver umožňuje poslat soubor přes internet do Výzkumného antivirového centra Symantecu. Program umí analyzovat a během několika minut i vyléčit komplexní viry, jako např. W32 Bolzano, považovaný za nejrozsáhlejší rodinu virů ve Windows. **Nejnovější varianty tohoto viru nelze nalézt tradiční antivirovou technologií, protože se samy mění a "pohřbívají" hluboko uvnitř spustitelných souborů Windows, přičemž schovávají všechny znaky infekce.** Striker32 umí zjistit viry bez ohledu na to, kde se nacházejí nebo jak skrývají své programové instrukce.
Hospodářské noviny, 19.10.1999,

Kybernetická válka proti zločinu

Bezpečí britských občanů se od letošního října zvýšilo, a to díky nové internetové službě Crimestoppers. Každý, kdo něco ví o zločincích či jiných pachatelích trestných činů, může využít elektronické pošty a zcela anonymně sdělit vše, co ví. **Navíc mu tato služba veřejnosti na nic nepřijde, neboť lze použít spojení na účet volaného, takže účet za telefon se mu nezvýší.**
Jak píše BBC News, již nyní britská policie obviňuje na základě internetových informací průměrně čtrnáct lidí denně a jednou za dvanáct dní prý dopadne i vraha. Ministr vnitra Jack Straw tuto novou službu vřele uvítal. "Boj proti zločinům není jen věcí vlády a policie. Chce to partnerství, které vyžaduje podporu od každého," dodal.
Crimestoppers zaručují informátorům naprostou anonymitu, mohou totiž, pokud chtějí, využívat zvláštní server, který e-mailovou adresu odesílatele neregistruje.
Také proslulý Scotland Yard má podobnou službu, a informace na jeho e-mail proudí z celého světa. Na základě zprávy z Nizozemska obvinil v Londýně muže z vraždy.
Mip, Hospodářské noviny, 19.10.1999,

Islámští hackeři řádí

Jen několik hodin poté, co minulý týden pákistánské ozbrojené síly svrhly demokraticky zvolenou vládu Naváze Šarífa, se takzvaná Islámská skupina hackerů dala do **převratu internetového.** Nabourala se do oficiálních webových stránek vlády provincie Pandžáb, odkud sesazený premiér Šaríf pochází, a umístila na nich urážky tohoto státníka. Prý mu to svržení patří, protože je "bez mozku a bez vlasů". Naopak jsou vynášeni elitní parašutisté, kteří mají na puči největší zásluhu, jako ryzí hrdinové.
Stejně tak rychle z internetu zmizely oficiální stránky násilně odstraněné ústřední pákistánské

vlády, ministerstva zahraničí i ministerstva obchodu.
Islámští hackeři si již své **ostruhy získali** v letošním **vojenském konfliktu** mezi Pákistánem a Indií o vládu nad Kašmírem. Vnikli na webovskou stránku indické armády a podsunuli na ni zprávy o údajných zvěrstvech indických bezpečnostních sil páchaných proti kašmírskému civilnímu obyvatelstvu. Stranu pateticky věnovali "všem kašmírským bratřím, kteří trpí brutálním útlakem indické armády".
Převrat vedl také k tomu, že **Pákistánci ze všech koutů světa zavalili schránku elektronické pošty BBS New Online** tisíci názory na tento čin ozbrojených sil své země. **Většinou prý puč schvalují.**
Mir, Hospodářské noviny, 19.10.1999,

Bankovní úředník zakládal fiktivní konta a vybíral úroky

Z neexistujících peněz vybral úroky dnes již bývalý zaměstnanec českobudějovické pobočky Union banky, kterého policie před šesti týdny obvinila z podvodu a umístila do vazby.
České Budějovice - Nikoliv o devět, jak uváděli vyšetřovatelé, ale o tři milióny korun připravil údajně osmadvacetiletý pracovník Union banky v Českých Budějovicích letos od dubna do července svého zaměstnavatele. Vedení tohoto peněžního ústavu včera poprvé zveřejnilo detailní výsledky svého vnitropodnikového šetření.
Obviněný zaměstnanec podle generálního ředitele Union banky Jiřího Babiše **využil svých výborných znalostí podnikového informačního systému** a založil několik fiktivních kont na jména neexistujících firem. Celkem tak měl **vytvořit reálně neexistující sumu** v celkové výši okolo 220 milionů korun. "**Z těchto peněz pak vznikly úroky, které obviněný přesunul na jiná konta a fyzicky vybral**," uvedl Babiš. **Než podvod podle něj odhalila vnitropodniková kontrola, obohatil se tak bankovní úředník na úkor zaměstnavatele o tři miliony koru**n.
Generální ředitel UB zároveň **nevyloučil**, že zadrženému **pachateli mohli vědomě či nevědomě pomáhat i další zaměstnanci** českobudějovické pobočky, jejichž míru viny ukáže další vyšetřování. "**Vnitřní kontrola v českobudějovické pobočce nebyla tak důsledná, jak stanoví naše normy**," řekl Babiš. Přesto bylo podle něj odhalení pachatele jen otázkou času.
Mluvčí banky Josef Řeřicha tvrdí, že v případě odhaleného podvodu nešlo o chybu autorizovaného systému, který používají i další bankovní domy v čechách i v zahraničí.
"**Jedná se ve větší míře o shodu náhod, kterou však náš kontrolní systém nakonec odhalil**," uvedl Řeřicha. **Ani toto lidské selhání se však vzhledem k přijatým opatřením podle něj už nemůže v budoucnu opakovat.**
Kes, Lidové noviny, 8.10.1999, www.lidovenoviny.cz

Policie: Někteří hackeři ničí stránky také na objednávku a za peníze

Někteří **čeští hackeři pracují na objednávku za peníze.** Na veletrhu informačních technologií Invex-Computer v Brně to řekl Jiří Dastych z policejního prezidia. Činnost hackerů mění v ČR podobu. V minulosti měla prvky exhibicionistického dětinského zesměšňování, nyní je cílem stále více osobní zisk, uvedl.
"**Víme, že jsou lidé, kteří nabízejí anonymně svoje služby a za peníze jsou ochotni ničit cizí webové stránky a nabourávat se do různých databází**. Za útoky se může skrývat konkurenční boj různých firem nebo touha získat cizí informace," poznamenal.
Za chybu pokládá, že některé **podniky útoky na své stránky a počítačové sítě úmyslně**

nehlásí, aby nepřišly o klienty a neměly negativní reklamu. Policie nemůže chránit někoho, kdo o to sám nemá zájem, dodal Dastych. Mezi nejslavnější hackery v ČR patří CzERT, který se před lety naboural do stránek ministerstva zdravotnictví a upravil je na stránky Ministerstva smrti Čínské republiky. Doplnil je také radami, jak nejlépe spáchat sebevraždu. Podařilo se mu proniknout i na stránky české pobočky americké firmy Hollywood Classic Entertainment i společnosti MaMedia a dalších firem. V roce 1996 pozměnil například i internetovou stránku Union banky, kterou přejmenoval na Ruin banku**. "CzERT již dlouho o sobě nedal vědět a myslím si, že své aktivity přesunul jinam**," doplnil Dastych.
Problémy s hackery mají i policisté v USA. Např. loni obsadili stránku The New York Times, aby vyzvali k propuštění počítačového zločince Kevina Mitnicka.
Den, 7.10.1999,

Kriminalisté vytvořili tým proti softwarovým pirátům

Ministerstvo vnitra a policejní prezídium vyčlenilo zvláštní prostředky na vybavení speciálního pracoviště pro odhalování softwarové kriminality.
"Naši specialisté pracují nejen na policejním prezídiu, ale také na všech stupních řízení. Je logické, že nejlepší vybavení mají v Praze, ale i jednotlivá krajská a okresní ředitelství mají vyčleněné policisty, kteří se touto formou kriminality zabývají. Tým má zatím zhruba poloviční stav, ale postupně bude doplněn," řekl včera na veletrhu Invex computer v Brně policejní prezident Jiří Kolář. Podle jeho slov **má tým všechny podmínky pro svou práci a jedinou překážkou, jak získat ty nejlepší počítačové experty, jsou platy, které jim policie může dát**.
Vytvoření koncepce účinného boje proti softwarovému pirátství je jednou z podmínek, které si klade Evropská unie pro budoucí začlenění ČR do svých struktur.
Kg, Právo, 8.10.1999,

Paralela klasického a počítačového zločinu

Zloději aut jsou vždy o krok dále než jejich výrobci X Hackeři jsou vždy o krok dále než výrobci informačních technologií i bezpečnostních.
Zloději vozidel nebo jejich vykradači jsou organizovaní a jejich důvtip a šikovnost často vyzraje i nad moderním a složitým bezpečnostním zařízením X Organizovaní hackeři s vyšší inteligencí vítězí nad provozní slepotou výrobců.
Na každý ochranný prostředek si zloději aut rychle najdou protizbraň X Jakmile se nová bezpečnostní technologie vypustí do světa, začíná závod o její prolomení. U komerčně nasazených technologií se zatím vždy našel způsob, jakým konkrétní mechanismus ochrany překonat.
Zloději si troufnou i na nejmoderněji vybavený vůz, jenž výrobce mnohdy označuje za neodcizitelný, MF Dnes, 9.10.1999,

Ministerstvo vnitra a policie na Invexu 99

Existuje kriminalita na Internetu, jejíž pachatelé využívají anonymity tohoto moderního média k nabídce nelegálního zboží, šíření nezákonných textů a fotografií (extremismus, rasismus, dětská pornografie) a **k neoprávněnému získávání nebo poškozování cizích informací.**
Odhalováním této trestné činnosti a poskytováním odborné pomoci ostatním útvarům

kriminální policie se zabývá **skupina informační kriminality, která vznikla v květnu 1999** v rámci Ředitelství služby kriminální policie Policejního prezidia.
Truschka Samuel, Veřejná správa 99/40, www.mvcr.cz/vespra

IDA (Interchange of Data between Administrations)

Systém bezpečnostních funkcí a jejich vlastností. Pro řadu aplikací závisí použití sítě na zajištěné úrovni bezpečnosti a funkcí. tyto funkce by měly být pro uživatele pokud možno transparentní a měly by obsahovat minimum úsilí a současně zajišťovat odsouhlasenou úroveň bezpečnosti. Bezpečnostní funkce lze rozdělit do mnoha kategorií, jak uvádějí autoři systému.
COMPUTERWORLD, 9.10.1999.

Počítačové viry způsobují ročně ztráty až dvacet miliard dolarů

Počítačové viry způsobí na celém světě ročně škody až dvacet miliard dolarů. Za antivirové programy se naproti tomu letos utratí 800 milionů dolarů.
"Nastal znatelný posun k virům, které se šíří pomocí elektronické pošty," řekl na brněnském veletrhu Invex mluvčí firmy AEC Tomáš Přibyl**. Letošní nové viry označil za drzé, rozesílající samy sebe. Podle něho však nejsou viry schopny aktivace pouhým otevřením e-mailové zprávy**, ale nebezpečí znamená otevření příloh a dokumentů.
"Zásadou je vždy nevěřit nikomu a ničemu," dodal s tím, že odborníci už zachytili viry i na Windows 2000, které ještě nejsou na trhu.
ČTK, MFDnes 9.10.1999, www.idnes.cz

Neznámý pachatel prodává informace o sporožirových účtech České spořitelny

PRAHA- Jména, adresy, zůstatky na účtu, údaje o finančních operacích a jiné osobní informace o majitelích sporožirových účtů u České spořitelny nabízí neznámý pachatel. Uvedl to včera internetový server iDNES. Soukromé údaje dvou a půl milionů klientů bankovního ústavu nabídla minulý týden některým firmám neznámá osoba. Jako důkaz pravdivosti nabídky uvedl autor příklady výpisů z účtu čtyř náhodně vybraných klientů z července letošního roku. Kromě jejich osobních údajů se v nich lze dočíst, kde dotyčný pracuje, kolik vydělává, kdy platil inkaso, kam posílal peníze a jaký byl na konci měsíce zůstatek jeho konta. Ty údaje naprosto odpovídají. Jsem z toho v šoku. Vy teď vlastně o mě víte úplně všechno, reagoval jeden ze čtyř zveřejněných klientů František F. z Prahy. Podle České spořitelny však mohou klienti zůstat klidní. Údaje našich klientů jsou zabezpečeny naprosto standardně, sdělil mluvčí bankovního ústavu Pavel Jiroušek, který se o záležitosti dozvěděl z médií. V tuto chvíli neumím říct, jestli údaje, které mají média, jsou pravdivé, dodal. Pokud se informace potvrdí, mimo bankovního tajemství mohou být vážně ohroženy i peníze střadatelů. Při výběru hotovosti není totiž potřeba doklad totožnosti, stačí jen karta k účtu a podpis podle vzoru.
Poznámka autora: Pachatel, pracovník v oblasti zpracování dat České spořitelny, byl policií do čtrnácti dnů odhalen a předán k dalšímu šetření orgánům činným v trestním řízení.
*Tento článek byl nalezen fulltextem M.I.A. (*http://fulltext.mia.cz*)*

Vláda odmítla návrh zákona o elektronickém podpisu

PRAHA 6. prosince 1999 (ČTK) - Vláda odmítla poslanecký návrh zákona o elektronickém podpisu pro jeho „nesystematické zpracování a vnitřní rozpory“. ČTK to během jednání kabinetu řekl jeho mluvčí Libor Rouček. Autoři předlohy chtěli umožnit elektronické obchodování a větší využívání internetových služeb. Zákon měl zrovnoprávnit dokumenty v „papírové“ a elektronické podobě.

Návrh předložila skupina poslanců několika stran vedená místopředsedou Unie svobody Vladimírem Mlynářem. Mezi autory patří i předseda klubu poslanců ČSSD Stanislav Gross. Mlynář ČTK řekl, že námitky ministrů pramení z neporozumění. Doufá, že Poslanecká sněmovna k návrhu přistoupí zodpovědněji a že u ní zákon nalezne podporu napříč politickým spektrem.

Ministři tvrdí, že návrh splňuje jen částečně účel, tedy používání elektronického podpisu. Není jim jasné, zda se má elektronický podpis týkat i jiných než soukromoprávních úkonů, například úkonů správních nebo trestních. Návrh podle nich neorganicky slučuje správní řízení a rozhodování se smluvními postupy, aniž přesně vymezil, na co se který postup vztahuje.

Z návrhu není vládě zřejmé postavení úřadu pro elektronické podpisy. Nejasné je podle ní právní postavení ověřovatele informací. Podle textu lze usuzovat, že jeho činnost bude podnikáním. Podle notářského řádu je však činnost notáře neslučitelná s jinými výdělečnými aktivitami s výjimkou těch, které zákon vymezuje.

Podle ministrů z návrhu nevyplývá jakým postupem se bude vydávat osvědčení: zda na základě smlouvy, nebo zda se na řízení bude vztahovat správní řád, takže by ověřovatel nebyl správním úřadem. Není zřejmé, zda při splnění předepsaných podmínek vzniká žadateli nárok. Na vydání osvědčení, jakou formou se osvědčení vydává a zda a jak je možné se domáhat vydání osvědčení v případě, že ověřovatel jeho vydání odmítne.

Návrhu dále vytýkají, že neupravuje proces ověřování elektronického podpisu. Za nejasné ministři považují i některé formulace, například „nezaměnitelný pseudonym“ či „zvláštní znaky oprávněné osoby.

Poznámka autora. V roce 2000 lze s určitým uspokojením akceptovat další, tentokrát pozitivní schvalovací vývoj této důležité právní normy. Nutno však mít na mysli, že praktické uplatňování elektronického podpisu bude podmíněno nejen principiálními a právními aspekty, nýbrž i ryze technickými podmínkami, jako např. integrací sítí, úpravou ochrany jednotlivých informačních systémů, zřizováním terminálových stánků pro komunikaci širší veřejnosti v rámci informačních sítí jednotlivých úřadů apod.

Počítačová kriminalita
Nástin problematiky
Kompendium názorů specialistů

Autor: RNDr. Stanislav Musil
Recenzenti: JUDr. Václav Nečada,
Ing. Lukáš Peterka.
Určeno: Pro odbornou veřejnost
Tiskárna: Vydavatelství Kufr – František Kurzweil
Naskové 3, Praha 5
Dáno do tisku: srpen 2000
Vydání: první
Náklad: 170 výtisků

www.kriminologie.cz

ISBN 80-86008-80-0