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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

Autor práce: Radek Benda

Studijní obor: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Roman Svatoš, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2014

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

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

.....

Děkuji vedoucímu bakalářské práce JUDr. Romanu Svatošovi, Ph.D. za cenné rady, připomínky a metodické vedení práce. Zároveň bych chtěl poděkovat mým spolužákům, kamarádům za zapůjčené materiály, bez kterých by bakalářskou práci nebylo možno dokončit a v neposlední řadě mé rodině za podporu a trpělivost.

ABSTRAKT

BENDA, R. *Počítačová kriminalita a její příčiny.* Bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2014. 64 s. Vedoucí bakalářské práce: JUDr. Roman Svatoš, Ph.D.

Klíčová slova: internet, nebezpečí, opatření, počítačová kriminalita, příčiny

Bakalářská práce se zaměřuje na počítačovou kriminalitu, jako jednu ze závažnějších kriminalit dnešní doby vůbec a to ve smyslu využívání internetu jako prostředku k jejímu páchání. V první části pojednává o tom, co počítačová kriminalita je, jaké jsou její příčiny i to, kde se vyskytuje. Popisuje různá nebezpečí při běžném prohlížení internetových stránek a současně se zmiňuje o druzích počítačové kriminality, jakož to trestné činnosti. Následující část uvádí některé metody odhalování a postupy v boji s počítačovou kriminalitou. Poslední díl bakalářské práce, se věnuje obětem počítačové kriminality a zároveň navrhuje různá preventivní opatření.

ABSTRACT

BENDA, R. *Computer crime and its causes.* Bachelor thesis. České Budějovice: The College of European and Regional Studies, o. p. s., 2014. 64 p. Supervisor: JUDr. Roman Svatoš, Ph.D.

Key words: internet, dangerous, software, computer crime, causes

This thesis focuses on cybercrime as one of the serious criminality of our time at all in the sense of using the Internet as a means for its commission. The first part discusses what cybercrime is, what its causes are, and where it occurs. Describes the various hazards during normal web browsing and also mentions the types of computer crime, and that crime. The following section provides some detection methods and practices in the fight against cybercrime. The last part of the thesis is dedicated to the victims of computer crime and sets out various preventive measures.

OBSAH

ÚVOD

Ve své bakalářské práci se zabývám počítačovou kriminalitou a jejími příčinami. Téma jsem si zvolil proto, že počítačová kriminalita je velice žhavým a aktuálním tématem současné společnosti, nejen v České republice, ale i ve světě. Zároveň počty počítačových trestných činů rapidně narůstají, vzhledem ke zvyšující se kvalitě výpočetní techniky. Dále bych si rád také rozšířil své znalosti o dané problematice.

Již jsme částečně, jak se říká jednou nohou, našlápli do nového světa. Do světa digitálního a digitalizace široké škály oblastí běžného života. S tímto světem se setkáváme všichni, bez rozdílu každodenně, prostřednictvím informačních technologií. Jako všude platí pravidla, ani digitální sféra není výjimkou, jen ta pravidla jsou jiná. Akcelerace rozvoje výpočetní techniky, šikovnost, inteligence a vynalézavost mladších generací, umožňuje spolu s ne zrovna ideální ochranou autorských práv, tato pravidla porušovat a tím se ocitat, buď na hraně zákona v lepším případě, anebo za hranou zákona v případě horším. Počítačová kriminalita, co do forem, je velice rozmanitá. Je potřeba si říci, jak lze počítačovou kriminalitu definovat, kde hledat ty hlavní důvody (příčiny) pro její páchání, jak ji řešit a především mít na paměti prevenci.

1 METODIKA A CÍL BAKALÁŘSKÉ PRÁCE

Vzhledem k rozmachu počítačové techniky a závislosti lidské populace na internetu bude téma počítačové kriminality čím dál více diskutovaným tématem i v budoucnosti. Zájem na odhalování příčin i samotné trestné činnosti mají snad všechny policejní orgány na světě, neboť počítačová kriminalita je v dnešní době tou nejrozšířenější a zasahuje téměř veškeré oblasti rozsahu finančních škod.

Otázka tedy zní, co je potřeba změnit, zdokonalit a udělat proto, aby byly škody co nejmenší a nejméně početné, jak, pokud to vůbec lze, zabránit výskytu této kriminality? Jaké jsou metody a postupy při odhalování pachatelů, možnosti bránění se proti tomuto druhu trestné činnosti? Všechny tyto otázky budou předmětem zkoumání a posuzování na základě odborné literatury, která je dosti hojně zastoupena jak v domácí tak zahraniční síti knih. Dobré výsledky v oblasti řešení počítačové kriminality, ochrana občanů a majetku s tímto spojených, jsou bezpochyby dlouhodobým cílem zástupců spravedlnosti i v České republice.

Hlavním cílem bakalářské práce je objasnění co je počítačová kriminalita, kde všude se s ní lze setkat, jak postupovat při objasňování a potírání této kriminality a zjištění příčin počítačové kriminality. Za vedlejší cíle pak navržení některých opatření, která by mohla vést k omezení výskytu počítačové kriminality.

2 POČÍTAČOVÁ KRIMINALITA JAKO POJEM

2.1 Definice počítačové kriminality všeobecně

Ty tam jsou doby, kdy zloděj musel fyzicky napadnout vyhlédnutou oběť, případně se s kuklou na hlavě vloupat za pomoci dynamitu, autogenu a dalších nezbytných nástrojů do banky. Dnes už se jde na podobné nezákonné aktivity jinak – moderně – za pomoci výpočetní techniky z tepla domova. Ke spáchání trestného činu bohatě postačí průměrný počítač, připojení k internetu, vypalovací mechanika a nějaké ty znalosti (jejich úroveň závisí na konkrétním trestném činu či přestupku) (MATĚJKA[1]).

Definovat jednoznačně pojem počítačová kriminalita není tak jednoduché, jelikož tato se váže na nejrůznější oblasti trestního práva, spojených různými vazbami s informačními technologiemi. Z hlediska obecné teorie trestního práva můžeme definovat následující skupiny znaků jednotlivých skutkových podstat:

- objekt trestného činu – za objekt trestného činu jsou považovány předměty ochrany trestním zákonem;
- předmět útoku – tím může být člověk, věc, ale i nehmotný majetek (právo, informace apod.);
- porušení předmětu útoku je účinkem trestného činu;
- objektivní stránka trestného činu – zahrnuje především tzv. obligatorní znaky, kterými jsou: jednání, následek a příčinný vztah mezi nimi (kauzální průběh);
- subjektivní stránka trestného činu – zahrnuje znaky týkající se psychiky pachatele (zavinění, pohnutka apod.) (MURČÁ[2]).

Pojem počítačová kriminalita byl definován mnoha autory různými způsoby. HOLCR[3] vidí počítačovou kriminalitu jako trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů. ZAPLETAL[4] zase počítačový trestný čin definoval, jako jednání namířená proti výpočetní technice, jejímu programovému vybavení a datům a informacím takto zpracovávaných. KUCHTA[5],[6] chápe počítačovou

[1] MATĚJKA, M. *Počítačová kriminalita*. Brno: Computer Press, 2002. s. 106-108.
[2] MURČÁ J. *Počítačová kriminalita* [online] 2009. Dostupné z WWW: <http://referaty.portik.cz/rubrika/informatika/pocitacova-kriminalita-0/>.
[3] HOLCR, K. a kol. *Kriminologie*. 1. Vydání Praha: Leges, 2008, s. 10-11.
[4] ZAPLETAL, J. a kol. *Kriminologie pro posluchače magisterského studijního programu.* Praha: PA ČR, 2002, s. 6-7.
[5] KUCHTA, J. a kol. *Kriminologie* I. Část, 1. Vydání Brno: MU, 1993, s. 12-13.

kriminalitu jako útoky na sběr, zpracování, přenos a uchování informací prostřednictvím výpočetní techniky. Počítačovou kriminalitou rozumíme trestné činy páchané prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení a databází výpočetní techniky. Může jít o následující typické způsoby páchání:

- neoprávněné zásahy do vstupních dat,
- neoprávněné změny v uložených datech,
- neoprávněné pokyny k počítačovým operacím,
- neoprávněné pronikání do počítačů, počítačového systému a jeho databází,
- napadení cizího počítače, jeho programového vybavení a souborů dat v databázích (KONRÁD[7]).

Pryč jsou doby, kdy se viry šířily převážně kopírováním z disket! S rozšířením internetu bohužel hrozba virové nákazy, ale i jiných nepříjemností, značně stoupla. Knížka srozumitelná každému uživateli ukáže, jak se účinnými softwarovými nástroji a dodržováním základních pravidel uchránit před viry, nevyžádanými e-maily (*spamem*), nechtěně instalovanými programy (*spywarem*), hackerskými útoky či síťovými podvody (*phishingem*) (KOCMAN[8]).

Veřejnost vnímá hacking jako výraz pro méně závažné trestné činy související např. s automobily. Výsledkem studie COLDWELLA[9] byla skutečnost, že studenti různým oborů vnímají hacking s různou vahou důležitosti. Zjistilo se, že poměrně málo studentů považuje hackery jako zločince, navíc ti v přírodních vědách jsou ještě méně znepokojeni, než jejich vrstevníci v IT vědách.

Zatímco v minulosti se počítačová kriminalita v našem průzkumu příliš neobjevovala, dnes patří mezi nejčastěji páchané hospodářské trestné činy (PwC[10]). Počítačová kriminalita je typickou formou organizované kriminality ve fázi tvorby zisku (KONRÁD[7]).

---

[6] KUCHTA, J., VÁLKOVÁ, H. a kol. *Základy kriminologie a trestní politiky*. 1. Vydání Praha: C. H. Beck, 2005, s. 11.

[7] KONRÁD a kol. *Metodika vyšetřování jednotlivých druhů trestných činů*. 1999 [online] Dostupné z WWW: <http://www.vakobobri.cz/e107_files/public/metodika_vysetrovani_jednotlivych_trestnych_cinu.doc>.

[8] KOCMAN, R., LOHNISKÝ, J. *Jak se bránit virům, spamu a spyware*. 1. Vydání Computer press 2005, s. 26-28.

[9] COLDWELL, R. A. Some social parameters of computer crime. *Australian computer journal*. 1990. Vol. 22. Issue 2. s. 43-46.

[10] PwC - *Počítačová kriminalita pod lupou, Celosvětový průzkum hospodářské kriminality, Česká republika*. 2011 [online] Dostupné z WWW: <www.pwc.cz/crimesurvey>.

Počítačová kriminalita je hospodářský trestný čin spáchaný pomocí počítače či internetu. Typickými příklady počítačové kriminality jsou šíření virů, nelegální stahování médií, *phishing* a *pharming* a krádeže osobních informací, jako jsou např. údaje o bankovním účtu. Nespadají sem běžné podvody, kdy je počítač používán jako vedlejší nástroj s cílem spáchat podvod. Zahrnujeme zde pouze takové hospodářské trestné činy, kde jsou počítač, internet nebo užití elektronických médií a zařízení hlavním, nikoliv náhodným, prvkem (PwC[9]) (OAK[11]).

Neexistují žádné přesné, spolehlivé statistiky o míře počítačové kriminality a výši ekonomických ztrát jejích obětí, částečně proto, že mnohé z těchto trestných činů zřejmě nejsou oběťmi detekovány či hlášeny na úřadech, a částečně také proto, že ztráty jsou prostě často obtížně vypočitatelné (STANDLER[12]).

Nikdo neposkytne žádnou záruku či doporučení, které zabrání možnosti stát se obětí počítačové kriminality, ale alespoň se může člověk stát nesnadnou obětí a tak si možná útočník vyhledá snadnější cíl (STANDLER[13]).

MATĚJKA[14] uvádí, že vše také pramení z osobního pohodlí, které nabízí židle u počítače. Snadněji je provedena krádež v elektronické bance než v té kamenné.

Výpočetní technika a komunikace samozřejmě skýtá nesčetné možnosti a výhody pro podniky, správy, školy i jednotlivce. Tuto výhodu nesmíme opomíjet (CELENTANO[15]).

Dalším kamenem úrazu naší společnosti je neznalost práva, která má za následek nezodpovědné bezstarostné jednání (kopírování softwaru, primárních dat, extremistické diskuse, nelegální pornografie atd.). Této neznalosti jde ruku v ruce nedokonalost samotné legislativy. Vzhledem k rychlému vývoji informačních technologií a kriminality nemohou zákonné normy pružně reagovat (HELLEBRANDOVÁ[16]).

Výbor Evropského parlamentu se pokusil definovat počítačovou kriminalitu následovně: "*Počítačová kriminalita je nelegální, nemorální a neoprávněné jednání*

[11] OAK, M. *Types of computer crimes*. 2008 [online] Dostupné z WWW: <http://www.buzzle.com/articles/types-of-computer-crimes.html.

[12] STANDLER, R. B. *Computer crime*. 2002 [online] Dostupné z WWW: <http://www.rbs2.com/ccrime.htm>.

[13] STANDLER, R. B. *Tips for avoiding computer crime*. 2012 [online] Dostupné z WWW: <http://www.rbs2.com/cvict.htm>.

[14] MATĚJKA, M. *Počítačová kriminalita*. Brno: Computer Press, 2002. s. 15-16.

[15] CELENTANO, L. Z., FARMER, J. J. *Computer crime*. A joint report. 2000 [online] Dostupné z WWW: <http://csrc.nist.gov/publications/secpubs/computer.pdf>.

[16] HELLEBRANDOVÁ, H. *Počítačová kriminalita.* Právnická fakulta Masarykovy univerzity v Brně. 2006. Bakalářská práce. Vedoucí práce Kratochvíl V. s. 20-21.

zahrnující užití dat získaných prostřednictvím výpočetní techniky nebo jejich změnu." (SVATOŠ[17])

Počítačová kriminalita podléhá členění dle zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších právních předpisů, (dále jen „TZk")[18] následovně:

- trestná činnost se speciální úpravou pro oblast počítačové kriminality:
  - neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 TZk

Jedná se o neoprávněný přístup k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací. Oproti § 257a původního trestního zákona, zde došlo k posunu, když je sankcionována již samotná neoprávněná manipulace či neoprávněný přístup k počítači. Původní skutková podstata je pak rozvedena a doplněna v odstavci 2, ve kterém se hovoří, že kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta.

  - opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZk

Tato nová skutková podstata umožňuje postihnout osoby, které v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) TZk vyrobí, dovezou, zpřístupní, opatří a jinak šíří a přechovávají zařízení to umožňující, nebo heslo či jiná data, díky kterým lze získat přístup k počítačovému systému nebo jeho části. Skutková podstata je velmi podrobně formulována, takže by měla zajistit postih všech forem neoprávněného jednání směřujícího ke spáchání tohoto trestného činu.

[17] SVATOŠ, R. *Kriminologie*. Plzeň: Aleš Čeněk, 2012. s. 190.
[18] Zákon č. 40/2009 Sb., trestní zákoník, v platném znění 2009. [online] In: Sbírka zákonů České republiky, 354-461. Dostupné z WWW: <http://zakony.centrum.cz/trestni-zakonik>.

Skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZk a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZk jsou v trestním zákoníku upraveny na základě Úmluvy o počítačové kriminalitě, Budapešť, ze dne 23. listopadu 2001 (SVATOŠ[19]).

- poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZk

Ustanovení postihuje toho, kdo z hrubé nedbalosti porušení povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté zničí, poškodí, pozmění nebo učiní neupotřebitelnými data uložená v počítačovém systému nebo na nosiči informací, nebo učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat a tím způsobí na cizím majetku značnou škodu. Za toto nedbalostní jednání hrozí pachateli trest odnětí svobody až na šest měsíců, zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty. Ještě přísněji bude potrestán ten, kdo takovým jednáním způsobil škodu velkého rozsahu, až dvě léta odnětí svobody.

- krádeže, poškození nebo zničení programu a dat na nosiči informací:
  - krádež dle § 205 TZk
  - poškození cizí věci dle § 228 TZk
  - poškození a ohrožení obecně prospěšného zařízení dle § 276 TZk
  - obecné ohrožení dle § 272 TZk
- neoprávněné užívání počítače:
  - neoprávněné užívání cizí věci dle § 207 TZk
  - porušení autorského práva dle § 270 TZk
  - podvod dle § 209 TZk
- neoprávněný přístup k utajovaným informacím – hackerství:
  - vyzvědačství dle § 316 TZk
  - ohrožení utajované informace dle § 317 TZk
- zneužití výpočetní techniky k jiné trestné činnosti.

Nová právní úprava by tak měla být v souladu s mezinárodními předpisy, zejména s Úmluvou o počítačové kriminalitě ze dne 23. 11. 2001, rámcovým rozhodnutím Rady

[19] SVATOŠ, R. Počítačová kriminalita. *Auspicia.* 2013, roč. X. č. 1, s. 171-178.

ES o útocích proti informačním systémům 2005/222/SVV ze dne 24. 2. 2005 a s usnesením Rady ES ze dne 28. 1. 2002 o společném přístupu a konkrétních krocích v oblasti síťové a informační bezpečnosti. Původní jediné ustanovení § 257a „poškození a zneužití záznamu na nosiči informací“ bylo podstatně rozšířeno a aktualizováno, aby tak konečně mohlo být adekvátně reagováno na specifickou počítačovou kriminalitu (HRUŠÁKOVÁ[20]).

2.2 Počítačová kriminalita ve světě

Rychlý rozvoj počítačové telekomunikační a další technologie vedl k růstu nových forem mezinárodní trestné činnosti, zejména počítačové kriminality. Počítačová trestná činnost nemá prakticky žádné hranice a dělá nebo může mít vliv na všechny země v tomto světě. Studie RAIE[21] může sloužit jako pracovní dokument, který pojednává o fenoménu, povaze a klasifikaci počítačové kriminality. Zpráva shrnuje práci v oblasti počítačové zločinnosti na mezinárodní úrovni, projednává potřebu propagace pro povědomí a uzákonění nezbytných právních předpisů v zemi, pro prevenci počítačové kriminality. Zpráva také uvádí další zdroje informací, pokud by měl někdo zájem. Svět počítačů je komplexní a nestabilní a díky tomu i výhledy do budoucna jsou až zlověstné, i realita je v nebezpečí. Nejlepší řešení by bylo držet se hesla – „lepší býti připraven, nežli zaskočen“.

Počítače a internet se staly důležitou součástí moderního života na celém světě. Mají vliv na komunikaci, finance a správu věcí veřejných. V té samé době vytvořila technologie jedinečné příležitosti k trestné činnosti a deviaci on- a off-line. V průběhu posledních dvou desetiletí rozšířil kriminologický výzkum své zaměření na řešení různých forem trestné činnosti a na použitelnost tradičních metod na její postih. Tomu se věnuje studie HOLTA[22], který počítačovému trestnému činu a metodám jeho studia věnoval mnohaletý výzkum.

Na začátku jednadvacátého století, než vzrostla síla on-line sociálních sítí, spekulovalo několik studií o pravděpodobné struktuře organizované počítačové trestné

[20] HRUŠÁKOVÁ, M. Vybrané majetkové trestné činy v novém trestním zákoníku ve srovnání s aktuální úpravou, se zaměřením na nedbalostní trestné činy. 2009. *Buletin advokacie*. Vol. 10. s. 73-77.
[21] RAI, G., DUBASH, R. K., CHAKRAVARTI, A. K. Computer related crimes. *Electronics information & planning*. 1998. Vol. 25. Issue 9. s. 478-490.
[22] HOLT, T. J., BOSSLER, A. M. An assessment of the current state of cybercrime scholarship. *Deviant behavior*. 2014. Vol. 35. Issue 1. s. 20-40.

činnosti. Práce YIPA[23] zkoumá strukturu organizované počítačové trestné činnosti na základě analýzy dat z internetu.

Obecně je počítačová kriminalita celosvětovým problémem bez výjimky (KIM[24], CARUCCI[25], MCCURDY[26], DHILLON[27], CARTER[28], GILL[29], HANSEN[30], MARSHALL[31], NICHOLSON[32]). Každý z autorů odborných publikací na ni nahlíží z jiného úhlu. Mnohé světové kapacity se jí zabývají všeobecně (KLEINDIENST[33], AUDAL[34], HUANG[35], ANONYMOUS[36], CRONAN[37], BAZELON[38], WALLACE[39], VOTH[40], DITZION[41], DILLON[42], BENSON[43], PERRITT[44], GILL[45], BARRETT[46],

[23] YIP, M., WEBBER, C., SHADBOLT, N. Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & society*. 2013. Vol. 23. Issue 4. s. 516-539.
[24] KIM, C., NEWBERGER, B., SHACK, B. Computer crimes. *American criminal law review*. 2012. Vol. 49. Issue 2. s. 443-488.
[25] CARUCCI, D., OVERHULS, D., SOARES, N. Computer crimes. *American criminal law review*. 2011. Vol. 48. Issue 2. s. 375-419.
[26] MCCURDY, J. L. Computer crimes. *American criminal law review*. 2010. Vol. 47. Issue 2. s. 287-329.
[27] DHILLON, G. SILVA, L., BACKHOUSE, J. Computer crime at CEFORMA: a case study. *International journal of information management*. 2004. Vol. 24. Issue 6. s. 551-561.
[28] CARTER, A. J., PERRY, A. Computer crimes. *American criminal law review*. 2004. Vol. 41. Issue 2. s. 313-365.
[29] GILL, P. Fighting computer crime – Report on the forensic team of the justice department of Basel. *Kriminalistik*. 2003. Vol. 57. Issue 6. s. 389-390.
[30] HANSEN, M. Crime and computers. *Aba journal*. 2002. Vol. 88. s. 24-25.
[31] MARSHALL, A. M., TOMPSETT, B. C. Spam 'n'chips – A discussion of internet crime. *Science & justice*. 2002. Vol. 42. Issue 2. s. 117-122.
[32] NICHOLSON, L. J., SHEBAR, T. F., WEINBERG, M. R. Computer crimes. *American criminal law review*. 2000. Vol. 37. Issue 2. s. 207-259.
[33] KLEINDIENST, K. T., COUGHLIN, T. M., PASQUARELLA, J. K. Computer crimes. *American criminal law review*. 2009. Vol. 46. Issue 2. s. 315-357.
[34] AUDAL, J., LU, Q., ROMAN, P. Computer crimes. *American criminal law review*. 2008. Vol. 45. Issue 2. s. 233-274.
[35] HUANG, X. M., RADKOWSKI, P., ROMAN, P. Computer crimes. *American criminal law review*. 2007. Vol. 44. Issue 2. s. 285-335.
[36] ANONYMOUS. Computer crime cases up in Northern Ireland. *Digital investigation*. 2006. Vol. 3. Issue 4. s. 189-189.
[37] CRONAN, T. P., FOLTZ, C. B., JONES, T. W. Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*. 2006. Vol. 49. Issue 6. s. 85-90.
[38] BAZELON, D. L., CHOI, Y. J., CONATY, J. F. Computer crimes. *American criminal law review*. 2006. Vol. 43. Issue 2. s. 259-310.
[39] WALLACE, R. P., LUSTHAUS, A. M., KIM, J. H. J. Computer crimes. *American criminal law review*. 2005. Vol. 42. Issue 2. s. 223-276.
[40] VOTH, D. Task force tackles computer crime. *IEEE software*. 2004. Vol. 21. Issue 4. 99-100 p.
[41] DITZION, R., GEDDES, E., RHODES, M. Computer crimes. *American criminal law review*. 2003. Vol. 40. Issue 2. s. 285-336.
[42] DILLON, S. A., GROENE, D. E., HAYWARD, T. Computer crimes. *American criminal law review*. 1998. Vol. 35. Issue 3. s. 503-547.
[43] BENSON, C., JABLON, A. V., KAPLAN, A. V., ROSENTHAL, M. E. Computer crimes. *American criminal law review*. 1997. Vol. 34. Issue 2. s. 409-433.
[44] PERRITT, H. H., CHARNEY, S., MILLER, G. P. Computer crimes now on the books: What do we do from here? *Temple law review*. 1997. Vol. 70. Issue 4. s. 1199-1226.
[45] GILL, M. S. Cybercops take a byte out of computer crime. *Smithsonuan*. 1997. Vol. 28. Issue 2. s. 114.
[46] BARRETT, D. J. Statistics and computer crime. *Computer*. 1996. Vol. 29. Issue 7. s. 14-14.

COOPER[47], HARBORT[48], RASKIN[49], COPLER[50], LOIA[51], TOMPSETT[52]), jiní se specializují na určité téma v rámci této rozsáhlé problematiky – legislativa (ANONYMOUS[53], ANONYMOUS[54], ANONYMOUS[55], SCHULTZ[56], KERR[57], ANONYMOUS[58], JACOBSON[59], BAKEWELL[60], HATCHER[61], HANCOCK[62]), vyšetřování (ZÁVRŠNÍK[63], ANONYMOUS[64], SCHULTZ[65], BROWKER[66], CHEN[67]), prevence, ochrana, devianti (NEVILLE[68], LEWIS[69], WIBLE[70], ANONYMOUS[71],

[47] COOPER, D., PFLEEGER, C. Statistics and computer crime – Reply. *Computer* 1996. Vol. 29. Issue 7. s. 14-14.
[48] HARBORT, S. Crime in cyberspace – New forms of time-specific computer crimes. *Kriminalistik*. 1996. Vol. 50. Issue 3. s. 194-198.
[49] RASKIN, X., SCHADACHPAIVA, J. Computer crimes. *American criminal law review*. 1996. Vol. 33. Issue 3. s. 541-573.
[50] COPLER, J. A. Computer crime: A crime fighter's handbook – Icove, D., Seger, K., VonStorch, W. *Online*. 1996. Vol. 20. Issue 1. s. 97.
[51] LOIA, V., MATTIUCCI, M., SENATORE, S., VENIERO, M. Computer crime investigation by means of fuzzy semantic maps. 2009. In: BaezaYates, R., Berendt, B., Bertino, E., Lim, E. P., Pasi, G. *International conferences on web intelligence*, Milan, Italy. Vol. 3. s. 183-186.
[52] TOMPSETT, B. C., MARSHALL, A. M., SEMMENS, N. C. Cyberprofiling: Offender profiling and geographic profiling of crime on the internet. *Workshop of the 1st int. Conf. on security and privacy for emerging areas in communication networks*. 2005. s. 23-26.
[53] ANONYMOUS. New UK komputer crime-related legislation passes. *Computers & security*. 2007. Vol. 26. Isme 1. s. 12-13.
[54] ANONYMOUS. Update on komputer crime-related legislation. *Computers & security*. 2006. Vol. 25. Issue 8. s. 561-561.
[55] ANONYMOUS. CSI/FBI survey results show computer crime losses are declining. *Computers & security*, 2006. Vol. 25. Issue 6. s. 399-400.
[56] SCHULZ, E. New clause in UK computer crime legislation would make big difference. *Computers & security*. 2006. Vol. 25. Issue 4. s. 243-243.
[57] KERR, O. S. Lifting the „fog" of internet suveillance: How a suppression remedy would change computer crime law. *Hasting law journal*. 2003. Vol. 54. Issue 4. s. 805-845.
[58] ANONYMOUS. New Taiwan criminal code articles make computer crime a felony. *Computers & security*. 2003. Vol. 22. Issue 6. s. 467-468.
[59] JACOBSON, H., GREEN, R. Computer crimes. *American criminal law review*. 2002. Vol. 39. Issue 2. s. 273-325.
[60] BAKEWELL, E. J., KOLDARO, M., TJIA, J. M. Computer crimes. *American criminal law review*. 2001. Vol. 38. Issue 3. s. 481-524.
[61] HATCHER, M., MCDANNELL, J., OSTFELD, S. Computer crimes. *American criminal law review*. 1999. Vol. 36. Issue 3. s. 397-444.
[62] HANCOCK, B. US department of justice computer crime legislation information site. *Computers & security*. 1998. Vol. 17. Issue 1. s. 8-9.
[63] ZÁVRŠNÍK, A. Computer crime and digital investigation. *Revija za kriminalistiko in kriminologijo*. 2008. Vol. 59. Issue2. s. 198-204.
[64] ANONYMOUS. Computer crime-related legislation moves forward in US congres. *Computers & security*. 2006. Vol. 25. Issue 6. s. 402-402.
[65] SCHULZ, E. Police change tactics to deal with computer crime victims. *Computers & security*. 2003. Vol. 22. Issue 5. s. 371-371.
[66] BOWKER, A. L., THOMPSON, G. B. Computer crime in the 21st century and its effect on the probation officer. *Federal probation*. 2001. Vol. 65. Issue 2. s. 18-24.
[67] CHEN, C. Y., LINDSAY, G. Viruses, attacks, and sabotage: It's a computer crime wave. *Fortune*. 2000. Vol. 141. Issue 10. s. 484-484.
[68] NEVILLE, K. Virtually criminal: Crime, deviance and regulation online. *Online information review*. 2008. Vol. 32. Issue 1. s. 121-122.
[69] LEWIS, B. C. Prevention of computer crime amidst international anarchy. *American criminal law review*. 2004. Vol. 41. Issue 3. s. 1353-1372.

HANCOCK[72], DUFF[73], HIGHLAND[74]), dětská pornografie (WANE[75]), ekonomika (BIEVER[76], SCHULTZ[77], SCHULTZ[78], WIGGINS[79]) atd.

V posledních letech ukázala řada výzkumů významné zvýšení hlášených případů počítačové kriminality a zneužívání. Tento nárůst je spojen s rostoucí pozorností vůči této problematice v médiích, což má za následek zvyšování veřejného vnímání problémů s IT, a může představovat i překážku pro přijetí technologií, jako je internet. Studie DOWNLANDA[80] se zabývá účinky počítačové kriminality a vychází z výsledků průzkumu, který provedla pro posouzení postoje veřejnosti a povědomí o této problematice. Důležitou roli ve formování individuálních názorů hrají hromadné sdělovací prostředky. Výsledky průzkumu ukazují, že individuální vědomí počítačové kriminality a zneužívání je vysoké a že je většina respondentů vnímá jako problém. Nicméně, vyjádřené názory, pokud jde o závažnost různých typů zneužívání (a potenciální motivací pro ně) byly variabilní. Kromě toho, povědomí o týrání je rozšířenější, než znalost souvisejících právních předpisů, které mohou být použity k prevenci a trestům. Výsledky také ukázaly významný potenciál pro multimediální zprávy, které ovlivňují názory v této oblasti a zdůrazňují důležitost zodpovědného přístupu s cílem posílit informovanost společnosti.

S rozvojem počítačové techniky dochází i ke zvýšenému zneužívání dat a informací, které jsou zpracovávány právě moderní informační technologií. Masové používání počítačů v různých podmínkách, s rostoucím využíváním telekomunikačních zařízení tak, že se zvýší počet uživatelů, poskytuje stále větší šance zlodějům,

---

[70] WIBLE, B. A site where hackers are welcome: Using hack-in contents to shape preferences and deter computer crime. *Yale law journal*. 2003. Vol. 112. Issue 6. s. 1577-1623.
[71] ANONYMOUS. Students face komputer crime penalties. *Computers & security*. 2003. Vol. 22. Issue 4. s. 275-276.
[72] HANCOCK, B. Who do you call for help with komputer crime? *Computers & security*. 1998. Vol. 17. Issue 2. s. 99-100.
[73] DUFF, L., GARDINER, S. Computer crime in the global village: Strategies for kontrol and regulativ – In defence of the hacker. *International journal of the sociology of law*. 1996. Vol. 24. Isme 2. s. 211-228.
[74] HIGHLAND, H. J. Fighting komputer crime. *Computers & security*. 1996. Vol. 15. Issue 1. s. 8-9.
[75] WANE, P. Child pornografy: Crime computers and society. *Information communication & society*. 2009. Vol. 12. Issue 8. s. 1264-1265.
[76] BIEVER, C. Revealed: the true cost of komputer crime. *New scientist*. 2005. Vol. 186. Isme 2505. s. 30-31.
[77] SCHULTZ, E. Variety of computer crime-related bills passed. *Computers & security*. 2004. Vol. 23. Issue 8. s. 626-626.
[78] SCHULTZ, E. Computer crime cost the UK 145 pound milion in 2002. *Computers & security*. 2003. Vol. 22. Issue 5. s. 370-371.
[79] WIGGINS, L. M. Corporate komputer crime: Collaborative power in numbers. *Federal probatik*. 2002. Vol. 66. Isme 3. s. 19-+.
[80] DOWNLAND, P. S., FURNELL, S. M., ILLINGWORTH, H. M., REYNOLDS, P. L. Computer crime and abuse: A surfy of public attitudes and awareness. *Computers & security*. 1999. Vol. 18. Issue 8. s. 715-726.

a nepovolaným osobám (*hacker*) prorazit ochranné kódy oprávněných uživatelů. Jejich zapojení do systému způsobuje mnoho škod a má nepředvídatelné následky. Studie SIMUNDICA[81] představuje moderní informační technologie na ochranu dat a informací se zvláštním důrazem na jejich právní ochranu. Využití moderních informačních technologií umožňuje sběr a zpracování velkého množství dat z různých oblastí lidské činnosti.

Technologický pokrok umožnil schopnost ukládání a načítání velkého množství dat, která nabízejí spojení pro každého, kdykoli a kdekoli. Doprovodným výsledkem těchto výhod je, že se zvýšila i firemní rizika. Vytvořila se infrastruktura, ve které se společnost sama o sobě může snadno stát obětí (WIGGINS[82]).

Informační systém (IS) je nedostatečně chráněn proti některým typům poškození nebo ztrát. Je však třeba se také věnovat rizikům představovaným „vyšší mocí", hackery a viry, případně nepoctivými zaměstnanci se záměrem provádění nějaké formy počítačové kriminality. V této souvislosti začala řada výzkumníků řešit, do jaké míry jsou si bezpečnostní manažeři vědomi rizika systémů (WILLISON[83]).

Počítač dnes již nefunguje jako izolované zařízení, nýbrž má roli multi-transformátoru. V obchodním světě je využíván k běžným obchodním transakcím a analýzám na zpracování a uvažování s informacemi o národní bezpečnosti. Počítačový trestný čin má za sebou dlouhou historii, již od roku 1930. "Kyberzločin " se v poslední době objevil v boji proti organizovanému, neoprávněnému nabourávání počítačových systémů u komerčních subjektů, finančních institucí, orgánů veřejné správy a dochází tak k úniku důvěrných informací především pod vidinou zisku (NG[84]).

Kyberzločin je často tradiční trestná činnost (např. podvody, krádeže identity, dětskou pornografie), provedená rychle a obrovskému množství potenciálních obětí. Dále se může jednat o neoprávněný přístup, poškození a rušení počítačových systémů. V reakci na hrozbu kybernetické trestné činnosti, je naléhavá potřeba reformovat metody a rozvíjet nadnárodní schopnosti policie. Mezinárodní odezva je stručně nastíněna v dokumentech Organizace spojených národů (v platnosti od září 2003)

[81] SIMUNDIC, S., FRANJIC, S., SUSIC, T. Databases and komputer crimes. Proceedings elmar – 2010. 2010. In: Grgic, M., Bozek, J., Grgic, S. *52nd international symposium ELMAR*, Zadar, Croatia. s. 195-201.

[82] WIGGINS, L. M. Corporate komputer crime: Collaborative power in numbers. *Federal probatik*. 2002. Vol. 66. Isme 3. s. 19-+.

[83] WILLISON, R., BACKHOUSE, J. Opportunities for komputer crime: considering systems risk from a criminological perspective. *European journal of informatik systems*. 2006. Vol. 15. Isme 4. s. 403-414.

[84] NG, D., TSUI, E. Knowledge – intensit collaboration to vombat cyber crime in the Asia Pacific Region. 2010. In: Tsui, E. *Proceedeings of the 7th international conference on intellectual capital, knowledge management and organisational learning*, China. s. 323-330.

a Rady inovativní úmluvy kyberzločinu v Evropě (v platnosti od července 2004) (BROADHURST[85]).

Existují různé formy páchání počítačové kriminality. V současné době se nejčastěji používá členění na přímou a nepřímou počítačovou kriminalitu.

Přímá počítačová kriminalita:

- útok na počítač, program, údaje komunikačního zařízení (počítačový vandalismus)
- neoprávněné použití počítačových programů a nelegální tvorba a rozšiřování kopií programů (počítačové pirátství)
- neoprávněné užívání počítače nebo komunikačního zařízení (krádež komunikačních služeb)
- neoprávněný přístup k údajům, získání utajovaných informací nebo jiných informací o osobách, činnosti atd. (počítačová špionáž)
- krádeže počítače, programů, údajů, komunikačního zařízení
- změny v programech a údajích
- šíření poplašných zpráv.

Nepřímá počítačová kriminalita:

- zneužívání počítačových prostředků na páchání jiné trestné činnosti
- počítačové bankovní krádeže a finanční machinace (fishing, pharming, *spoofing, MITM* – man in the middle) (SVATOŠ[86]).

[85] BROADHURST, R. Developments in the global law enforcement of cyber-crime. *Policing – an international journal of police strategies & management*. 2006. Vol. 29. Issue 3. s. 408-433.
[86] SVATOŠ, R. Počítačová kriminalita. *Auspicia.* 2013, roč. X. č. 1, s. 171-178.

3 PŘÍČINY POČÍTAČOVÉ KRIMINALITY

Příčin vzniku počítačové kriminality je bezpočet, ovšem uvádí se několik faktorů, které je charakterizují nebo pro ně připravují tzv. živnou půdu. Snad úplně první příčinou je **vznik samotného počítače**. Většina vynálezů stvořených s dobrými úmysly, mohou být nakonec zneužity k různým formám protiprávního jednání. Dalším postupem bylo **propojení více počítačů**, které umožnilo sdílení dat a komunikaci (JIROVSKÝ[87]), budoucí internet. Kyberprostor už od této chvíle jen narůstal, nekonečné množství informací, možností, svodů. V neposlední řadě je tu **rychlost**, s jakou může jedinec svůj nezákonný čin nebo útok spáchat. A kde by bylo lidstvo bez své **zvědavosti.** Ta v tomto případě hraje nemalou roli. Člověk si „to prostě chce vyzkoušet". Lákadlem je samozřejmě i **„anonymní" a pohodlné prostředí.** Lépe se provede trestný čin ze židle elektronicky, než fyzicky venku v kamenném obchodě či bance (MATĚJKA[88]). V neposlední řadě, co se týče pachatele, má tu svůj význam i pocit beztrestnosti, touha po adrenalinu či jistá osobní kompenzace ve vztahu k zaměstnavateli. Mezi další významné příčiny páchání počítačové trestné činnosti patří **vidina zisku**, který může být z takovéto činnosti nemalý a dále také relativně snadná **dostupnost.** Ta souvisí s životní úrovní současné společnosti, kdy téměř každá domácnost vlastní počítač s připojením na internet a její členové tráví v kybernetickém světě značnou část svého volného času. Pachatelům počítačových trestných činů značně usnadňuje práci **důvěra** samotného **uživatele**. Ten je přesvědčen o tom, že jeho se to netýká, jemu se to stát nemůže.

Internet je tak obsáhlá síť s tak obrovským **množstvím dat a rychlostí toku**, že je technicky nemožná jejich kontrola a zaznamenávání. V neposlední řadě je jednou z příčin páchání počítačových trestných činů i **nedokonalost v legislativě** a její **neznalost** v široké veřejnosti. Kolikrát běžný uživatel netuší, že páchá počítačový trestný čin nebo že mu napomáhá a jaký by ho za to mohl stihnout trest. Naopak mnohdy jsou si uživatelé vědomi svých nezákonných činů, avšak to se dostáváme zpět k domněnce, „mě se to netýká, mně nechytí, mně se to nemůže stát".

Ale proč zrovna trestný čin prostřednictvím počítače?

a) Trestný čin může být spáchán během několika sekund, aniž by se pachatel nacházel na místě činu,

[87] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 2007. Praha: Grada Publishing, a.s. s. 55-58.
[88] MATĚJKA, M. *Počítačová kriminalita*. Brno: Computer Press, 2002. s. 21-22.

b) Prostředky na páchání počítačové kriminality jsou legálně dostupné,
c) Zručnost na páchání této trestné činnosti a vědomosti jsou jednoduše dostupné,
d) Počítačová kriminalita způsobuje značné škody, které se někdy těžko kvantifikují,
e) Je vysoce latentní,
f) Má mezinárodní charakter, aniž by pachatel fyzicky překročil hranice,
g) Pro odhalování, dokumentování a dokazování jsou třeba erudovaní odborníci.

3.1 Historie počítačové techniky a internetu

Počítače v dnešní době významně ovlivňují náš život a i celou společnost. Jedná se o odvětví, které se výrazně rozvíjí a i do budoucna se počítá s jeho výrazným rozvojem. Co ale předcházelo tomuto rozvoji a proč vlastně počítače vznikly? Za primitivní způsoby počítání se dá považovat počítání pomocí prstů na ruce nebo počítání pomocí kamínků a jamek v písku. Z tohoto způsobu potom vznikly počítací desky. Nejstarší objevená deska pochází z ostrova Salamis z doby přibližně 300 let před naším letopočtem.

Z této desky vychází další počítací pomůcka, abacus (viz Příloha VI). Abacus, tak jak ho známe dnes, pochází přibližně z roku 1200 našeho letopočtu z Číny. Vedle abacusu existovaly i jiné počítací pomůcky, například logaritmické pravítko (viz Příloha V). První vynález mechanického počítacího stroje je připisován Blaise Pascalovi roku 1642. Přístroj se jmenoval Pascalina. Další mechanický počítací stroj vytvořil německý matematik G. W. von Leibniz v roce 1673. Byl to předchůdce moderní kalkulačky.

Snaha zjednodušit a zpřesnit výpočty vedla k práci na vývoji mechanického počítacího stroje (malý diferenční stroj) anglického matematika Charlese Babbage. Požadavek ke zrychlování počítání vedl ke vzniku dalších počítacích strojů. V USA vypsali soutěž na počítací stroj pro potřeby sčítání lidu. Tuto soutěž vyhrál se svým strojem H. Hollerith, který je považován za jednoho z otců IBM. Jeho stroj se jmenoval tabelátor.

Významným počítačem ve vývoji, který byl zkonstruován, byl v roce 1944 počítač MARK 1. Základním prvkem tohoto počítače bylo relé. Počítač MARK 1 zkonstruovali Howard Aiken a Grace Hopper. Počítač vznikl za spolupráce s firmou IBM, skládal se z 9000 relé, 497 mil drátů a celý vážil 5 tun. Jeho výpočetní výkon byl tři operace sčítání za sekundu a jeho nasazení bylo jasné – výpočet atomové bomby. Nakonec stroj pracoval plných 15 let.

Aby byla historie počítačů přehlednější, začal se vývoj počítačů rozdělovat na jednotlivé etapy – generace počítačů. Každá etapa je charakteristická nejen použitým hardwarem, ale i způsobem obsluhy, programováním počítače, vlastním softwarem, atd.

První počítačová generace je charakteristická tím, že počítače byly především vyvíjeny školami anebo na základě grantů od vlády. Počítače měly často výpadky i přesto, že byly v klimatizovaném prostředí. Typicky tyto počítače obsluhovaly velké týmy operátorů. Významným jevem této etapy je i pozvolné pronikání počítačů i do komerční sféry. Typickým zástupcem této éry je počítač ENIAC (Electronic Numerical Integrator And Computer) sestrojený v Bellových laboratořích.

Druhá počítačová generace začala kolem roku 1959 a její hlavní charakteristikou je použití tranzistorů na místo elektronek. Dalším rysem bylo zmenšování počítačů a zlevnění jejich výroby. V programování se začali objevovat programovací jazyky, což zpřístupnilo práci s počítačem více lidem. Typickým zástupcem této éry byl počítač IBM 650, který byl první počítačem, vyráběným hromadně, celkem se ho prodalo 1500 kusů.

Třetí počítačová generace spadá do let 1964 až 1970. Jejím hlavním znakem je použití integrovaného obvodu, který byl vynalezen roku 1959. K ukládání dat se používal magnetický disk. Z hlediska programů byl výrazný rozvoj operačních systémů a hlavně možnost práce více uživatelů na jednom počítači zároveň.

Čtvrtá generace počítačů, která probíhá od roku 1970 až dodnes by se dala charakterizovat neustálou miniaturizací integrovaných obvodů, v komerční oblasti hlavně rozšiřování i do oblastí, kde se dříve počítače vůbec nepoužívaly (HOLA[89]).

Počítače jsou dnes naprosto všude a spousta lidí si život bez nich nedokáže ani představit. U spousty z nich propukla a ještě propukne závislost na nich a tím i odtržení některých jedinců od všední tváře reality. Počítače zasáhly všechna odvětví od armády, bankovnictví, školství, vědu, zdravotnictví, po zábavní průmysl (filmy, oblíbené hry...) a mnoho dalších (WAST[90]).

Pro lepší přehlednost byla významná data uspořádána do tabulky 2.

[89] HOLA, V. *Historie a vznik počítačů*. 2002. [online] Dostupné z WWW: <http://utf.mff.cuni.cz/vyuka/OFY016/F2001/Hola/referat.html>.

[90] WAST. *Vznik a vývoj počítačů.* 2007. [online] Dostupné z WWW: <http://www.gamepark.cz/vznik_a_vyvoj_pocitacu_11279.htm>.

Tab. 2 Počítač od historie po současnost

rok	**událost**
1801	řídí Francouz Maria Jacquard tkalcovský stav pomocí děrné pásky.
1833	vyvíjí Angličan Charles Babage tzv."Analytical Engine" pracující s děrnými štítky. Po té se pokouší sestavit univerzálnější počítač pro složitější matematické operace, ale před dokončením bohužel umírá.
1938	inženýr Konrád Zus v Německu sestrojuje první mechanický počítač Z1.
1941	Konrad Zus zkonstruuje malý reléový automatický počítač Z4. Hitlera tento projekt ale nezaujme. Při jednom ze spojeneckých náletů je totálně zničen.
1943	Howard H. Aiken a jeho tým na Harvardské universitě uvádí do provozu reléový počítač zvaný Harvard Mark I.
1944	byl na univerzitě ve Filadelfii v státu Pensylvánie (USA) uveden do provozu ENIAC (Electronic Numerator Integrator And Computer) Byl řízen za pomocí elektronických impulsů a prováděl až 5 000 operací za sekundu. Spotřebu elektrické energie měl okolo **140 kW!** (jako tehdy celé město).
1945	John von Neumann sestavil a uvedl do provozu počítač MANIAC (Mathematical Analyser Numerical Integrator And Computer). Tento počítač byl mimo jiné použit k vývoji vodíkové bomby.
1946	další počítač ENIAC (Electronic Numerical Integrator and Computer) sestrojený na University of Pennsylvania byl první použitelný samostatný počítač na světě.
1948	byl poprvé předveden tranzistor, jehož komerční využití přišlo až v r. 1952
1951	je prvním sériovým počítačem elektronkový Univac firmy Remington.
1952	první byl sestaven počítač s tranzistory a s diodami ve Spojených státech a jmenoval se Tradic. Byl uveden do provozu počítač IAS, který se stal vzorem pro první počítač IBM 701 vyráběný ve velkých sériích.
1958	byl u nás (tehdy ČSSR) uveden do provozu první reléový počítač SAPO. Přišel Jack St. Clair Kilby (USA) s nápadem vyrobit celistvou součástku z kousku křemíku a na světě byl první tzv. integrovaný obvod. Kilbymu se podařilo vyrobit první čip.
1967	Angličan Norman Kitz sestavuje Anita Mark 8 – první elektronický osobní počítač. Přišel vynález systému LED

1971	zavádí americká firma Texas Instruments poprvé výrobu mikroprocesorů.
1976	byla vyvinuta první inkoustová tiskárna firmou IBM.
1977	později Bill Gates a Paul Allen oficiálně zakládají společnost Microsoft.
1981	uvádí na trh společnost IBM první PC s procesorem Intel 8088 s frekvencí 4,77 MHz s novinkou - operačním systémem MS-DOS.
1982	spatřilo světlo světa poprvé první CD v továrně v Hannoveru (Německo).
1983	se začíná používat disketa, která úspěšně nahrazuje dříve rozšířenou magnetofonovou pásku.
1984	se objevuje první osobní laserová tiskárna od f. Hewlett-Packard.
1985	Microsoft vyvine zdokonalenou verzi MS-DOS pro firmu IBM PC Windows 1.0.
1986	po investici National Science Foundation vzniká obrovská celosvětová počítačová sít. Základ internetu. V ČR až v roce 1992.
1988	přicházejí na trh první disky CD-R, cédéčka tak jak je známe.
1993	internet dostává dnešní podobu, tak jak jej znáte i vy.
1994	uvádí f. EPSON na světový trh první inkoustovou tiskárnu Stylus Color.
1996	hlásí příchod na trh první DVD s daleko větší kapacitou 4,38 GB (Digital Versatile Disk) disky, které dnes vytlačují (jsou cenově výhodnější) klasické CD-R.
1998	uvádí na trh firma Diamond Multimedia svůj první (světová premiéra) MP3 přehrávač.
2000	Microsoft přichází s Windows 2000.
2001	Microsoft přichází s Windows XP a časem se z XP stává nejvíce používaný operační systém na PC. Blu-ray Disc, je jméno další generace optických disků.
2003	firma Sony jako první představila Blu-Ray rekordér pro domácnost s označením BDZ-S77, který se začal první prodávat v Japonsku (stál 3800 dolarů). Médium o kapacitě 23GB se prodávalo za 30 dolarů.
2007	přichází Microsoft s Windows Vista.

Převzato a upraveno z WAST[91]:

[91] WAST. *Vznik a vývoj počítačů.* 2007. [online] Dostupné z WWW: <http://www.gamepark.cz/vznik_a_vyvoj_pocitacu_11279.htm>.

Co se týče internetu, jeho historie sahá až do rozmezí let 1950 až 1960. V té době dochází k výraznému rozvoji počítačů. Ukazuje se potřeba propojovat jednotlivé počítače a přenášet data z jednoho počítače do druhého.

V roce 1982 pak by definován ústřední komunikační protokol celého současného internetu. Tím se stal protokol TCP/IP. Tím se současně začíná mluvit i o Internetu. První internet byl čistě nekomerční a sloužil primárně k propojení univerzit a dalších výzkumných ústavů a pracovišť. V 80 a 90 letech dvacátého století se ale historie internetu posouvá dál a začínají se objevovat první komerční poskytovatelé internetových (datových) služeb.

Zhruba od poloviny 90 let pak dochází k velkému růstu celého internetu. Objevují se první služby, které již dnes považujeme za běžné a samozřejmé: elektronická pošta, instant messaging (IM, aplikace jako ICQ nebo Skype). Už tehdy existují první video hovory nebo video konference. Dochází také k velkému nárůstu webových stránek (WWW, World Wide Web), objevují se diskusní fóra, blogy a první sociální sítě.

V roce 2007 pak už přes internet proudí téměř 97 % všech informací (WAST[92]). A současnost je ještě více alarmující.

Dostupnost počítačové techniky a rychlost spáchání počítačového trestného činu jdou ruku v ruce s vidinou zisku. Ten je samozřejmě nemalý. V roce 2011 přišli lidé na celém světě o 110 miliard dolarů právě díky kybernetickému zločinu (PALEČEK[93]). Co se týče dostupnosti počítačové techniky, tak právě na internetu je nespočetné množství možností koupě všeho potřebného, čeho se k páchání počítačové trestné činnosti, a nejen jí, využívá, již od korunových položek.

Porovnání průměrného loupežného přepadení a průměrného kybernetického útoku z hlediska zisku, rizika, pravděpodobnosti dopadení, pravděpodobnosti odsouzení a výše trestu je patrná z přiložené tabulky č. 3 (WOJTOVIČ[94]).

---

[92] WAST. *Vznik a vývoj počítačů.* 2007. [online] Dostupné z WWW: <http://www.gamepark.cz/vznik_a_vyvoj_pocitacu_11279.htm>.

[93] PALEČEK, J. *Kybernetický zločin okrádá lidi po celém světě o 110 miliard dolarů ročně.* 2012 [online] Dostupné z WWW: <http://pcworld.cz/novinky/kyberneticky-zlocin-okrada-lidi-po-celem-svete-o-110-miliard-dolaru-rocne-4483>.

[94] WOJTOVIČ, J. *Kybernetická kriminalita – výnosný a rychle rostoucí byznys*. 2013 [online] Dostupné z WWW: <http://www.internetprovsechny.cz/kyberneticka-kriminalita-vynosny-a-rychle-rostouci-byznys/>.

Tab. 3 Porovnání průměrného loupežného přepadení a kybernetického útoku

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn či zabit.	Bez rizika fyzické újmy
Zisk	Průměrně 3 - 5 tisíc USD.	**Průměrně 50 - 500 tisíc USD.**
Pravděpodobnost dopadení	Dopadeno 50 - 60 % útočníků.	**Dopadeno cca 10 % útočníků.**
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků.	Z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je odsouzeno jen 50 %.
Trest	Průměrně 5 - 6 let, pokud pachatel při loupeži nikoho nezranil.	Průměrně 2 - 4 roky.

4 VÝSKYT POČÍTAČOVÉ KRIMINALITY

4.1 Situace v České republice

V České republice zaujímá počítačová kriminalita svou četností čtvrtou pozici (13 %). Přestože je tato hodnota pod průměrem regionu střední a východní Evropy (18 %) i celosvětově (23 %), předpokládá se, že se její podíl bude v následujících letech dále zvyšovat (viz příloha I, IV). 30 % českých společností se domnívá, že v následujícím roce bude s velkou pravděpodobností čelit počítačové kriminalitě. To ji, společně s korupcí a uplácením a zneužitím informací v obchodním styku, řadí mezi nejvíce obávané hospodářské trestné činy. Pro úplnost jsou přílohy II a III (viz přílohy), které demonstrují obavy týkající se počítačové kriminality v zemích střední a východní Evropy i celého světa. V případě ohrožení počítačovým trestným činem se české společnosti nejvíce obávají krádeže duševního vlastnictví (včetně krádeže dat), poškození dobrého jména společnosti a krádeže osobních údajů. Počítačový trestný čin byl tradičně vnímán jako nebezpečí přicházející z vnějšího prostředí. Průzkum však naznačuje změnu v tomto chápání: 21 % českých respondentů vidí toto riziko spíše jako vnitřní hrozbu, dalších 32 % dotazovaných považuje za stejně pravděpodobné, že útok přijde zevnitř nebo zvenku. V případě ohrožení počítačovým trestným činem se české společnosti nejvíce obávají krádeže duševního vlastnictví (71 %), včetně krádeže dat, poškození dobrého jména společnosti (72 %) a krádeže osobních údajů (74 %) (PwC[95]).

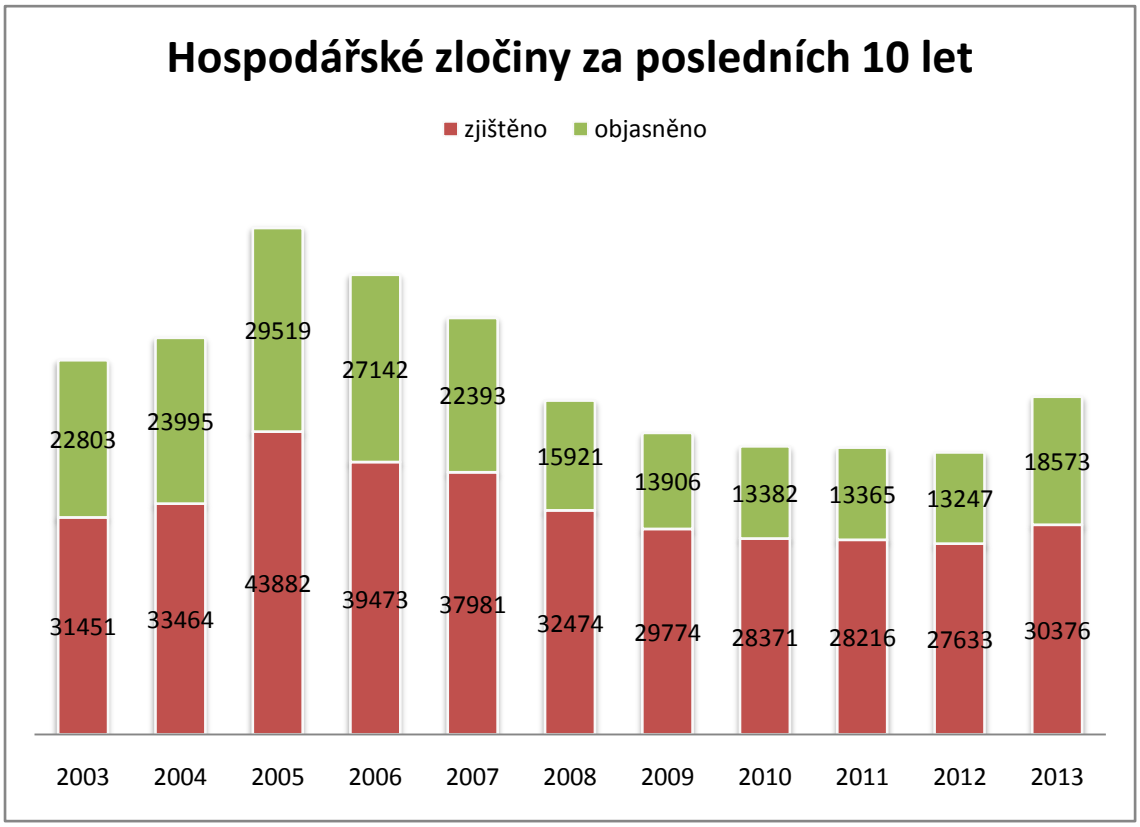
Pět nejčastěji se vyskytujících počítačových trestných činů se má následovně: pokud používáte program Malware (určený ke vniknutí nebo poškození počítačového systému od souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware), jste vystaveni počítačovému trestnému činu v masovém měřítku. Další je krádež identity. Zde je nejdůležitější zásadou nikdy nesdílet osobní informace! Opakované a stupňované obtěžování s využitím ICT (*Cyberstalking*) si většinou lidé zaviní sami neuváženým vkládáním osobních informací ať už na sociálních sítích, či kdekoli jinde na internetu. Takové obtěžování může dále přejít i v závažný trestný čin v realitě. Patří sem i dětská pornografie, která je obrovským tématem sama o sobě. A poslední z nejzávažnější pětice je SPAM (nevyžádané soubory, pošta). Mnozí z nás se s ní potýkáme denně a snažíme se přijít na účinnou obranu. Co můžeme udělat,

[95] PwC - *Počítačová kriminalita pod lupou, Celosvětový průzkum hospodářské kriminality, Česká republika*. 2011 [online] Dostupné z WWW: <www.pwc.cz/crimesurvey>.

abychom se udrželi v bezpečí? Obecně stačí použít „selský rozum“ před otevřením nějakého druhu souboru, abychom neohrozili bezpečnost počítače. Nikdy se nepřihlašujte do vašeho bankovního účtu na veřejném počítači, pokud si nejste absolutně jisti bezpečností. Neuveřejňujte zbytečně mnoho informací za svého soukromého života na sociálních sítích či kdekoli jinde na internetu. Chraňte tak sebe i své blízké (POT[96]).

Obrázek 1 demonstruje situaci v České republice za posledních 10 let v oblasti hospodářských trestných činů, kam počítačová kriminalita patří. Pro analýzu a vypracování grafu byla použita statistická data evidenčně statistického systému kriminality, (dále jen „ESSK“) z archivu Ministerstva vnitra.

Obr. 1: Hospodářské trestné činy v ČR za posledních 10 let.



Z grafu je v polovině sledovaného období patrný klesající trend v počtu hospodářských trestných činů, v posledním sledovaném roce opětný mírný vzrůst.

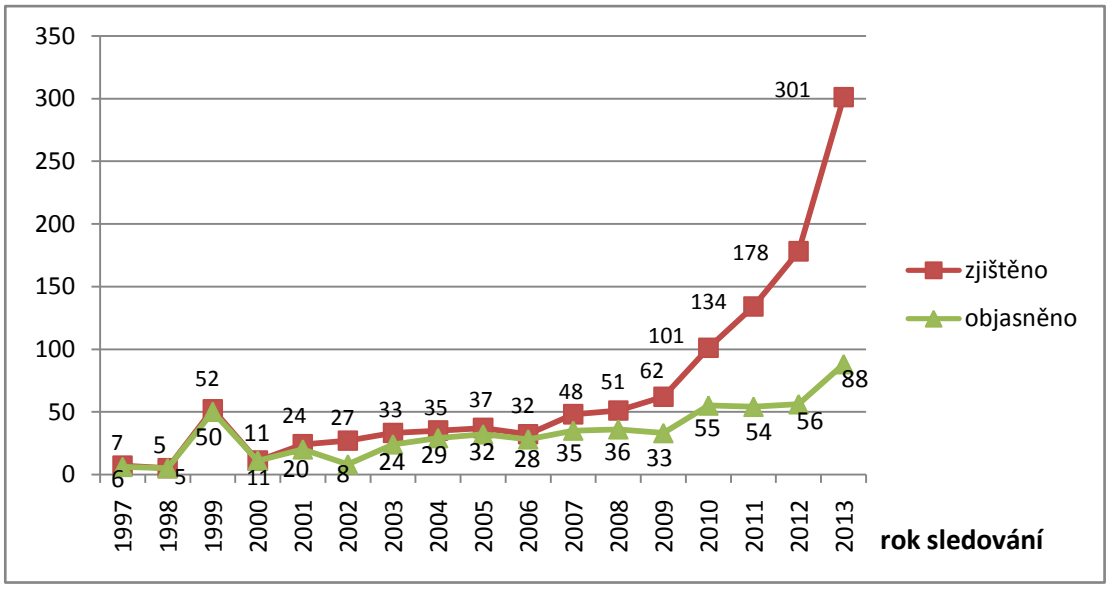
[96] POT, J. *Top five computer crimes & how to protect yourself from them*. 2010. [online] Dostupné z WWW: <http://www.makeuseof.com/tag/top-five-computer-crimes-protect/>.

Nejpravděpodobnější příčinou poklesu hospodářských trestných činů je v posledních letech konsolidace hospodářských vztahů, kdy po porevolučním přerozdělování státního majetku bez patřičné právní úpravy došlo v posledních letech k její precizaci.

Pokud jde o dynamiku počítačové kriminality, počet trestných činů prudce stoupá, viz následující obrázek č. 2. Na tomto místě je nutno upozornit na tu skutečnost, že počítačové trestné činy jsou jednou z položek náležící do hospodářských trestných činů, u kterých je trend opačný, klesající. Vzhledem k tomu, že počítačová kriminalita tvoří pouze malou část hospodářských trestných činů, tak vývoj hospodářských trestných činů v podstatě příliš neovlivní. Stoupající trend počítačové kriminality ovlivňuje i výpočetní technika, která se stále vyvíjí a zkvalitňuje a s tím se zvětšují i možnosti jejího zneužití. Zejména v posledních pěti letech je nárůst enormní. S podobným trendem je potřeba počítat i do budoucna. Tato skutečnost bude jistě umocněna i situací, kdy u policie nebude dostatek potřebných odborníků.

Na obr. č. 2 je zobrazen vývoj počítačové kriminality v období 1997 – 2013. Graf demonstruje pouze tři počítačové trestné činy dle § 230-232 TZk (neoprávněný přístup k počítačovému systému a nosiči informací, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti), avšak existuje i další počítačová kriminalita, která však není v ESSK blíže specifikována.

Obr. 2: Vývoj počítačové kriminality v ČR za posledních 16 let.



4.2 Potenciální pachatelé

Jedním z negativních jevů spojených se vznikem počítačů je nevyhnutelný vývoj počítačové kriminality. I když existuje mnoho trestných činů, které mohou být spáchány s pomocí počítačů, jeden z nejrozšířenějších je zvýšený výskyt neoprávněného přístupu do počítačových systémů. Kvůli nedostatkům v tradičním trestním právu, které dodnes přetrvávají, jsou přístupy přijaté jednotlivými státy téměř konzistentní (HUGHES[97]).

Počítačová kriminalita je poměrně nová oblast výzkumu v kriminologii a deviaci. Několik studií se zabývalo výskytem nelegálních počítačových úkonů a prakticky nikdo se nesnažil nabídnout teoretické vysvětlení pro chování. Ve své studii poskytuje SKINNER[98] údaje o životnosti nelegální počítačové aktivity ze vzorku studentů na univerzitě za poslední rok. Poznatky z této studie jsou užitečné pro pochopení toho, proč vysokoškoláci páchají protiprávní činy za pomoci počítače.

Pachatelé počítačové kriminality se člení na amatéry, kdy se většinou jedná o hackery, kteří pronikají do systémů a tím si zvedají sebevědomí, a na profesionály, kteří vykonávají trestnou činnost s využitím přístupů do IS v rámci pracovního zařazení (programátoři apod.) (SVATOŠ[99]). S rozvojem informačních technologií v posledních letech nastupuje nový fenomén, počítačová kriminalita. Pachatelé výpočetní techniku využívají pro její vysokou efektivitu v procesu zpracování informací (ANGERFELT[100]). Velmi často bývají pachateli trestné činnosti mladí lidé. Mezi základní rysy struktury kriminality mladých lidí patří zejména nedostatečná plánovitost trestné činnosti, neadekvátní jednání, virtuální realita, neschopnost odložit uspokojení potřeb, rozpoznávací a ovládací schopnost není zachována pod vlivem emocí, vandalismus, šikana, potřeba prostředků na obstarání drogy, tíhnutí k extremistickým hnutím, trávení času ve skupinách vrstevníků, dřívější zahajování sexuálního života atd. (SVATOŠ[101]). Nové informační technologie lidstvu v mnohém pomáhají, ale zároveň jsou však napadnutelné a snadno zneužitelné (SVATOŠ[99]). Počítačová kriminalita se stala celosvětovým problémem a nadále rychle roste, ale několik studií zkoumalo

[97] HUGHES, G. Computer crime – The liability of hackers. *Australian computer journal*. 1990. Vol. 22. Issue 2. s. 47-50.
[98] SKINNER, W. F., FREAM, A. M. A social learning theory analysis of computer crime among college students. *Journal of research in crime and deliquency*. 1997. Vol. 34. Issue 4. s. 495-518.
[99] SVATOŠ, R. *Kriminologie*. Plzeň: Aleš Čeněk, 2012. s. 189.
[100] ANGERFELT, B. Computer crimes – A study of different types of offenses and offenders. 1992. In: Gable, G. G., Caelli, W. J. *IT security: The need for international cooperation*. Vol. 15. s. 463-474.
[101] SVATOŠ, R. Mládež a extremismus v České republice. *Auspicia* 2013, roč. X č. 2. s. 113-122.

použitelnost obecné teorie kriminality k vysvětlování počítačové deviace. Pomocí souboru 2751 korejských mladíků zkoumala konkrétní studie, zda teorie nízkého sebeovládání může být užitečná jako teoretický rámec, vysvětlující počítačovou trestnou činnost (MOON[102]).

ROGERS[103] zkoumal psychologické charakteristiky, morální volby a agresivní manipulativní chování osob samostatně výdělečně činných. Studie se zúčastnilo 77 studentů v programu informačních technologií. Výsledky studie ukázaly, že jediná významná proměnná pro predikci deviantního chování byla *extroverze*.

Co se týče rozdílů mezi pohlavími v oblasti počítačové trestné činnosti, studie shodně ukazují, že chlapci jsou častěji než dívky zapojováni do různých typů počítačové kriminality. Aktuální studie testuje použitelnost obecné teorie kriminality při vysvětlování rozdílů mezi pohlavími v počítačové kriminalitě a hodnotí užitečnost teorie při vysvětlování počítačové trestné činnosti v rámci pohlaví (MOON[104]).

Organizace jsou dnes k počítačové trestné činnosti a podvodu spáchaného zaměstnancem více náchylné, než kdy předtím. Studie HAUGENA[105] prezentuje některé statistické údaje o růstu podvodů, faktorech, které je způsobují na pracovišti, jak podniky mohou chránit svůj majetek a běžné podvody spáchané s pomocí počítačů, technik a ovládacích prvků. Manažeři ve všech typech organizací musí být dobře informováni o jejich systému vnitřní kontroly a ujistit se, že má k dispozici dostatečnou kontrolu a rovnováhu na oddělení i proti zaměstnancům, kteří by se dopustili podvodného jednání. Žádná organizace není dnes imunní. Proto je nezbytně nutné, aby manažeři pochopili problémy, které mohou podvody způsobit a jak mohou chránit svou organizaci.

K většině počítačových trestných činů dochází, protože současný zaměstnanec je ničen ovládacími prvky. Tato práce analyzuje počítačové trestné činnosti vyplývající z důvodu porušování ochranných opatření ze strany zaměstnanců. Práce naznačuje, že by měly být zavedeny různé technické, procedurální a normativní kontroly, aby se

[102] MOON, B., MCCLUSKEY, J. D., MCCLUSKEY, C. P. A general theory of crime and computer crime: An empirical test. *Journal of criminal justice*. 2010. Vol. 38. Issue 4. s. 767-772.
[103] ROGERS, M. K., SEIGFRIED, K., TIDKE, K. Self-reported computer criminal behavior: A psychological analysis. *Digital investigation*. 2006. Sp. Issue. s. 116-12.
[104] MOON, B., MCCLUSKEY, J. D., MCCLUSKEY, C. P., LEE, S. Gender, general theory of crime and computer crime: An empirical test. *International journal of offender therapy and comparative criminology*. 2013. Vol. 57. Issue 4. s. 460-478.
[105] HAUGEN, S., SELIN, J. R. Identifying and controlling computer crime and employee fraud. *Industrial management & data systems*. 1999. Vol. 99. Issue 7-8. s. 340-344.

zabránilo nelegálním činům. Je potřeba zavést individuální odpovědnost za všechny potenciálně negativní akce (DHILLON[106]).

Některé studie se zaměřují na vliv vrstevníků na jednotlivce a jejich svádění k deviaci. Tímto tématem se literatura sice zabývá, ale metodicky je znemožněno vyvodit závěry o příčinné souvislosti. PATENOSTER[107] provedl experiment v laboratoři. Všech 91 účastníků mělo možnost podvádět kliknutí na až čtyři odkazy, které by jim poskytly možnost neoprávněně vydělat více peněz. Subjekty byly rozděleny na 2 skupiny, kontrolní a ve stavu „léčby". Výsledkem bylo, že žádný z účastníků v kontrolní skupině nepodváděl, naopak 38% účastníků ve stavu léčby ano. Závěrem lze konstatovat, že vliv skupiny může motivovat jednotlivce k deviaci. Nyní je potřeba se zabývat přesnými mechanismy.

4.3 Ekonomické dopady počítačových trestných činů

V roce 1996 činilo celosvětové ilegální kopírování softwaru 15.2 bilionů dolarů, se ztrátou 5.1 miliard dolarů konkrétně v Severní Americe. Některé zdroje uvádějí celkové ztráty díky softwarové kriminalitě více než 4.7 trilionů dolarů. Ve firemním prostředí nebo podnikání, musí mít každý počítač svoji vlastní sadu originálního softwaru a příslušného počtu manuálů. Je nezákonné, aby podnik koupil jednu sadu originálního softwaru a použil tento software na více než jednom počítači nebo jej půjčoval, kopíroval či jinak distribuoval z jakéhokoliv důvodu bez předchozího písemného souhlasu výrobce softwaru. Mnoho softwarových manažerů se zabývá dodržováním právních předpisů spolu s řízením aktiv a náklady na jejich organizaci. Mnoho firem zapojuje své právní oddělení a lidské zdroje v souvislosti s distribucí softwaru a licencemi (NICOLESCU[108]).

Zisky z počítačové kriminality předčily zisky z drog (MORÁVEK)[109].

Počítačová kriminalita se v posledních několika letech proměnila ve vzkvétající byznys, který vydělává miliardy dolarů. Už dávno neplatí všeobecně zažitá představa

[106] DHILLON, G., MOORES, S. Computer crimes: theorizing about the enemy within. *Computer & security*. 2001. Vol. 20. Issue 8. s. 715-723.
[107] PATERNOSTER, R., MCGLOIN, J. M., NGUYEN, H., THOMAS, K. J. The causal impact of exposure to deviant peers: An experimental investigation. *Journal of research crime and deliquency*. 2013. Vol. 50. Issue 4. s. 476-503.
[108] NICOLESCU, C. Economic consequences of software crime. *Romania within the EU: Oportunities, requirements and perspectives*. 2007. Vol. 1. s. 303-307.
[109] MORÁVEK D. *Zisky z počítačové krominality předčily zisky z drog.* 2010. [online] Dostupné z WWW: <http://www.podnikatel.cz/clanky/zisky-z-pocitacove-kriminality-predcily-drogy/>.

hackera jako teenagera, který z nudy či škodolibosti rozesílá počítačové viry, nebo se pokouší vlámat do informačních systémů firem a úřadů. Dnešní kriminalita je vysoce organizovaná, internetoví zločinci se úzce specializují, čile mezi sebou obchodují a vyměňují si zkušenosti. A jejich hlavním motivem není uspokojení vlastního ega, ale peníze. Cílem či obětí počítačového trestného činu se může stát prakticky kdokoliv – internetoví podvodníci zkoušejí nachytat jak běžné uživatele, tak firmy. Neexistují žádné oficiální statistiky trestné činnosti na internetu a liší se i odhady bezpečnostních firem a analytiků, kolik si vlastně podvodníci vydělají. Jisté však je, že se jejich zisky pohybují v miliardách dolarů. Například centrum FBI pro stížnosti na internetovou kriminalitu přijalo v loňském roce jen ve Spojených státech přes 250 tisíc oznámení a celkové škody vyčíslilo na čtvrt miliardy dolarů. Takto ohlášených trestných činů je přitom jen zlomek. Škody, které počítačová kriminalita napáchá, jsou ale ještě větší, než kolik sami podvodníci vydělají. V důsledku krádeží dat a kybernetické kriminality lze odhadovat, že firmy loni utrpěly ztráty duševního vlastnictví v hodnotě více než bilion dolarů (SIEBERT[110]).

[110] SIEBERT M. *Počítačová kriminalita: byznys za miliardy.* 2009 [online] Dostupné z: WWW: <http://euro.e15.cz/profit/pocitacova-kriminalita-byznys-za-miliardy-895968>.

5 OBJASŇOVÁNÍ A POTÍRÁNÍ POČÍTAČOVÉ KRIMINALITY

Úmluva o počítačové kriminalitě (dále jen „Úmluva“) byla přijata Výborem ministrů rady Evropy na jeho 109. zasedání dne 8. listopadu 2001 a následně byla dne 23. listopadu 2001 v Budapešti otevřena k podpisu. V současné době Úmluvu podepsalo 47 států (Albánie, Arménie, Rakousko, Ázerbájdžán, Belgie, Bosna a Hercegovina, Bulharsko, Chorvatsko, Kypr, Dánsko, Estonsko, Finsko, Francie, Gruzie, Německo, Řecko, Maďarsko, Island, Irsko, Itálie, Lotyšsko, Lichtenštejnsko, Litva, Lucembursko, Malta, Moldávie, Černá hora, Nizozemí, Norsko, Polsko, Portugalsko, Rumunsko, Srbsko, Slovensko, Slovinsko, Španělsko, Švédsko, Švýcarsko, Makedonie (FYROM), Turecko, Ukrajina, Spojené království, Kanada, Japonsko, Jihoafrická republika, Spojené státy americké), přičemž 36 států (Albánie, Arménie, Rakousko, Ázerbájdžán, Bosna a Hercegovina, Bulharsko, Chorvatsko, Kypr, Dánsko, Estonsko, Finsko, Francie, Gruzie, Německo, Maďarsko, Island, Itálie, Lotyšsko, Litva, Malta, Moldávie, Černá hora, Nizozemí, Norsko, Portugalsko, Rumunsko, Srbsko, Slovensko, Slovinsko, Španělsko, Švýcarsko, Makedonie (FYROM), Ukrajina, Spojené království, Japonsko, Spojené státy americké) uložilo ratifikační listiny. Česká republika Úmluvu podepsala 9. února 2005 na základě usnesení vlády ze dne 6. října 2004 č. 968. Úmluva vstoupila v platnost dne 1. července 2004. Cílem Úmluvy je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními technologiemi (Senát pČR[111]).

S rychlým růstem počítačových a síťových systémů v posledních letech je zde patrný odpovídající vzestup počítačové trestné činnosti. Kyberzločin má mnoho podob a získal si velkou pozornost v médiích. Čili prioritou se stává informační bezpečnost. Za účelem boje proti kybernetické kriminalitě je potřeba získat trestní důkazy

[111] Senát parlamentu ČR, Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě, 2013 [online] Dostupné z WWW: <http://www.senat.cz/xqw/webdav/pssenat/original/66810/56264>.

z počítačových systémů. Toto se zcela liší od shromažďování konvenční důkazů v trestním řízení a může to zmást i vyšetřovatele. WANG[112] nabízí řešení na ochranu proti počítačové trestné činnosti prostřednictvím implementace softwarových nástrojů do počítačových systémů. Tímto způsobem ti, kdo se trestných činů v kybernetickém prostoru dopouštějí, mohou být snadněji dopadeni.

Kyber technologie je velmi složitá a internet je stále více používán jako místo pro páchání trestné činnosti za pomoci osobních počítačů. Přestože počítačové vyšetřování je stále v raných fázích svého vývoje, rostoucím využíváním internetu se zvýšila i nutnost „digitálního vyšetřování“. Přístup ke zlepšení vyšetřování v počítačové trestné činnosti je navržen ve třech fázích: nezávislé ověřování digitálních stop, odpovídající informace z různých zdrojů a příprava platných argumentů. IP - adresa a čas strávený na internetu jsou klíčové pro identifikaci podezřelého hned na začátku. Neexistuje však žádná záruka, že vždy bude vše prokázáno, vyšetřovatelé by se měli snažit ze všech sil, aby se zabránilo pochybám, musí najít další stopy a důkazy pro ověření svého podezření (KAO[113]).

Vzhledem k nadále zvyšující se trestné činnosti v oblasti počítačů vyvinuly některé kontrolní orgány specializované pracovní skupiny k řešení daných problémů. Vzhledem k relativní novosti není však zcela jasné, jak nejlépe postupovat s největší efektivitou. Výzkum na národní úrovni poskytuje určitou představu, pokud jde o požadavky v oblasti vymáhání práva při řešení počítačové kriminality a navrhl hlubší šetření o současném stavu. Některé otázky se zabývaly typy počítačových trestných činů, které se nejčastěji vyskytují. Předpokládá se, že výsledky budou sloužit jako základ pro srovnání národních výsledků (HINDUJA[114]).

Útoky počítačových zločinců mohou být potenciálně stejně škodlivé pro národní infrastrukturu jako útoky kybernetických teroristů. Účinná bezpečnostní protiopatření v boji proti počítačové trestné činnosti se vyrovnají těm, kterých se využívá k ochraně proti potenciálním hrozbám kybernetického terorismu a informační války. Nicméně, bezpečnostní organizace opakovaně uvádějí, že mnoho, ne-li většina, počítačových útoků se vyskytuje především proto, že hostitelský operační systém neměl dostatečnou ochranu. Hackeři sdílejí informace o chybách v zabezpečení prostřednictvím

[112] WANG, S. J. Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer standards & interfaces*. 2007. Vol. 29. Issue 2. s. 216-223.
[113] KAO, D. Y., WANG, S. J. The IP address and time in cyber.crime investigation. *Policing-An international journal of police strategies & management*. 2009. Vol. 32. Issue 2. s. 194-208.
[114] HINDUJA, S. Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing-An international journal of police strategies & management*. 2004. Vol. 27. Issue 3. s. 341-357.

neformálních skupin napojených přes internet. Toto poskytuje útočníkům výhodu využívat hostitelovy slabiny (WILSON[115]).

Existuje relativně nový nástroj pro tzv. „počítačové otisky prstů" používaný v trestné činnosti. Nástroj využívá skenování sítě a identifikační zařízení k získání otisku počítače přes internet. Otisk obsahuje identifikační údaje o operačním systému, *bannery*, výčty služeb. Jsou diskutovány také právní otázky, týkající se používání počítačových otisků prstů při vyšetřování trestných činů (NOVOTNÝ[116]).

WANG[117] se zabývá relevancí problémů zákona o počítačové trestné činnosti a elektronických důkazů. Dále poukazuje na některé problémy a pojednává o charakteristice počítačové kriminality, vývoji situace a problémech informační bezpečnosti. Dále jsou oblastí zájmu elektronické důkazy právní platnosti, elektronický sběr důkazů a elektronická evidence.

Právní systémy ve většině zemí se potýkají s problémy v návaznosti na vývoji počítačové společnosti, včetně vymáhání práva lidí. Soudy obecně nemají příliš mnoho znalostí o tom, co se děje. Někdy může být obtížné definovat nebo rozhodnout, zda čelíme počítačové trestné činnosti nebo lidské chybě, neúmyslné nebo úmyslné (SAARI[118]).

Intenzivním vývojem se počítačový trestný čin rozšířil do všech oblastí (VONGRAVENREUTH[119]). Ochrana orientovaná na společnost si vymohla právní podporu v průběhu posledních 30 let. Poskytuje inovační strategie k identifikaci a boji s problémy kriminality prostřednictvím partnerství a spolupráce komunit. Úspěch této obranné strategie vedl k přijetí nových programů ve virtuálním boji proti počítačovému trestnému činu. Je zřejmé, jak může takový program fungovat nebo jaké faktory ovlivňují jeho použití v terénu (BOSSLER[120]).

---

[115] WILSON, C. Holding management accountable: A new policy for protection against computer crime. Proceedings of the IEEE 2000 national aerospace and electronics conference: *Engineering tomorrow*. 2000. s. 272-281.

[116] NOVOTNÝ, J., SCHULTE, D., MÁNES, G., SHENOI, S. Remote computer fingerprinting for cyber crime investigations. In: DeCapitaniDiVimercati, S., Ray, I., Ray, I. *Data and applications security XVII. Status and prospects*. 2004. Vol. 142. s. 3-15.

[117] WANG, X. G. Research on relevant problems of computer crime and electronic evidence. 2013. In: Chang, T. 2012 *International conference on education reform and management innovation*, China. Vol. 5. s. 486-491.

[118] SAARI, J. Legal response to a computer crime – retrospect of a mere chance case. *Computer security*. 1993. Vol. 37. s. 369-373.

[119] VONGRAVENREUTH, G. F. IT-security and computer crime. *Wirtschaftsinformatik*. 1992. Vol. 34. Issue 4. s. 419-424.

[120] BOSSLER, A. M., HOLT, T. J. Assessing officer perceptions and support for online community policing. *Security journal*. 2013. Vol. 26. Issue 4. s. 349-366.

BEDNAR[121] se zabýval možnostmi forenzních vyšetřovatelů, jak se chovat ve vztahu ke spolupráci, rozhodování, komunikaci a koordinaci. Forenzní vyšetřovatel by měl mít dovednosti a podporu, aby byl schopen reagovat na příslušné hrozby.

Rozsah forenzní vědy a forenzních technik bude muset být rozšířen na pomoc při stíhání počítačové kriminality, s ohledem na růst těchto trestných činů a nové právní úpravy v podobě zákona (COLLIER[122]).

Bohužel stále existují země, jako např. Zimbabwe, kde neexistuje žádný zákon, který by potíral počítačovou kriminalitu. Díky tomu je zde potenciál pro obrovský nárůst počítačové kriminální činnosti, která nebude potrestána. Současné zákony nejsou dostatečně obsažné, aby zamezily počítačové trestné činnosti (CHIMHENO[123]).

Studie SOMA[124] zkoumá neschopnost extradičního práva rychle reagovat na změny v trestním právu! To je problematické zejména s ohledem na právní předpisy v oblasti počítačové trestné činnosti, která se neustále vyvíjí.

Existuje úmluva, která se zabývá zejména porušováním autorských práv, dětskou pornografií, jakož i trestnými činy souvisejícími s bezpečností sítí, včetně hledání počítačových systémů a odposlechu (POUNDER[125]).

Základní formy boje s kriminalitou se týkají otázek výchovy, prevence, sofwarového auditu, represe, působnosti policie a dalších orgánů činných v trestním řízení (SVATOŠ[126]).

[121] BEDNAR, P. M., KATOS, V., HENNELL, C. Cyber-crime investigations: Complex collaborative decision making. 2008. In: Tryfonas, T., Thomas, P. (ed.) *Third international annual workshop on digital forensics and incident analysis: WDFIA* 2008, Proceedings. s. 3-11.
[122] COLLIER, P. A., SPAUL, B. J. A forensic methodology for countering computer crime. *Artificial intelligence review*. 1992. Vol. 6. Issue 2. s. 203-215.
[123] CHIMHENO, R. M., DEHGHANTANHA, A. Framework for cyber crime law implementation in Zimbabwe. *Third international conference on computer engineering and technology*, Malaysia. 2011. s. 613-618.
[124] SOMA, J. T., MUTHER, T. F., BRISSETTE, H. M. L. Transnational extradition for computer crimes_ Are new treaties and laws needed? *Harvard journal on legislation*. 1997. Vol. 34. Issue 2. s. 317-371.
[125] POUNDER, C. The counsil of Europe cyber-crime convention. *Computer & security*. 2001. Vol. 20. Issue 5. s. 380-383.
[126] SVATOŠ, R. Počítačová kriminalita. *Auspicia*. 2013, roč. X. č. 1, s. 171-178.

6 DRUHY OBĚTÍ

Odjakživa byly hlavně děti snadnou kořistí pro pachatele jakékoli trestné činnosti, hlavně pro svou důvěřivou povahu, naivitu a nezkušenost. Děti oplývají přirozenou zvědavostí a dychtivostí zkoušet stále nové věci. Toto zkoušení a poznávání jim dnes velmi usnadňuje internet. Pachatelé internetové kriminality to vědí a dokážou toho patřičně využít (HULANOVÁ[127], ALEXANDER[128]).

Z psychologického hlediska se stal internet prostředkem interpersonální komunikace, který může významně ovlivňovat lidské rozhodování, chování, postoje a emoce. Internet je dnes vstupní branou do obrovského virtuálního světa plného informací a znalostí, jejichž použití je prakticky neomezené. Zvláště dnešním dětem nabízí internet velké množství úžasných výhod, jako jsou přístupy ke vzdělávacím materiálům, publikacím, možnosti on-line přátelství, kamarádů, koníčků, her a další on-line zábavy. Děti z těchto výhod a možností dokážou velmi často profitovat zcela jinak než jejich rodiče. Internetová generace dětí je tady (HULANOVÁ[129]).

Jako příklad lze uvést dotazníkové šetření provedené VELIČKOVOU (2009) v květnu 2009. Studijní skupina obsahovala 1562 respondentů, z toho:

- 1329 (94%) dotazovaných dětí ve věku do 17 let má přístup na internet ze svého domova
- 836 (63%) dotazovaných dětí ve věku do 17 let má počítač s internetem ve svém pokoji
- 785 (56%) dotazovaných dětí ve věku do 17 let používá internet denně,
- 346 (24%) skoro denně a pouze 16 (1%) méně než jednou měsíčně
- Pouze 387 (27%) osob, které se o dotazované děti starají, vědí, jaké stránky jejich dítě na internetu navštěvuje
- 101 (7%) dotazovaných dětí ve věku do 17 let si myslí, že setkávání se osobně s lidmi, které znají jen přes internet, není nikdy nebezpečné

Aby se zabránilo internetové *viktimizaci*, je bezpodmínečně nutné učit děti zásadám bezpečného používání internetu a to od chvíle, kdy k němu poprvé usednou (HULANOVÁ[127]).

[127] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha: Triton, 2012. s. 31-39.
[128] ALEXANDER, M. Listen: Computer crime victims speak. *Datamation*. 1995. Vol. 41. Issue 23. s. 183-211.
[129] HULANOVÁ, L. Internet jako dobrý pomocník, ale zlý pán. In: Medřická, J. (ed.) *Sborník příspěvků z konference Pražské linky důvěry „Poskytování krizové pomoci – výměna zkušeností a know-how"*. 2012. Vydalo Centrum sociálních služeb Praha. s. 23-29.

Česká republika je po Estonsku druhou zemí, kde jsou děti a dospívající nejvíce vystaveni riziku sledování pornografie na internetu (*EU Kids Online 2009*[130]*).* Tvrdá a deviantní pornografie může negativně ovlivnit formování mladé osobnosti, její prožívání a chování. Pod vlivem uvedených materiálů může být narušeno vnímání obecných sexuálních norem a souvisejících hodnot. Současné děti jsou ovlivňovány médii a reklamou. Vidí nerealistické hrdiny a krásky. A jak mohou proti tomu bojovat rodiče? Všechny operační systémy disponují možnostmi rodičovské kontroly, prostřednictvím kterých lze blokovat některé webové stránky, na které dítě přistupuje ze svého účtu (DOČEKAL[131]).

[130] EU Kids Online 2009-11, final report [online] Dostupné z WWW: <http://www.lse.ac.uk/home.aspx>.
[131] DOČEKAL, D., ECKERTOVÁ, L. *Bezpečnost dětí na internetu*. Brno: Computer Press, 2013. s. 1-21.

7 NAVRŽENÍ PREVENTIVNÍCH OPATŘENÍ

Myšlenka, že je lépe učinit preventivní opatření než poté napravovat škody, není novinkou, nýbrž je v dnešní době vysoce aktuálním tématem. Je zcela jasné, že účinnou možností boje proti počítačovému trestnému činu je prevence – ochrana počítačů a počítačových systémů. Kromě prevence právní lze aplikovat preventivní ochranu za pomoci prostředků hardware a software (různé klíče, hesla apod.). V tomto směru je potřeba přistupovat k preventivním opatřením globálně a začít u jedince. Je nutné zapojit širokou veřejnost formou **preventivní výchovy** již na základních školách, dál výchova operátorů, programátorů a dotčených osob a uživatelů. Výchova je jeden z nejdůležitějších faktorů prevence. Dále je potřeba zajistit maximální kontrolu a komplexní zabezpečení nejen ve středním a vysokém školství a následně ve firmách povinně školit zaměstnance, kteří přicházejí do styku s výpočetní technikou. Pomocníkem v této oblasti může být i medializace, kdy je široká veřejnost informována o tomto typu zločinu, může odhalit samotný útok, případně při osobním napadení patřičně reagovat. Oproti tomu pachatel by si mohl uvědomit svůj morální prohřešek a zachovat se důstojně.

Nezbývá než souhlasit, že policie a další orgány činné v trestním řízení nemají v boji s počítačovou kriminalitou snadnou roli. Policie bude ve skutečnosti vždy o něco pozadu. Jejím úkolem se tak stává udržet tento odstup minimální. Úspěšnost dopadení pachatele závisí nejen na technickém vybavení policie a na důkladném ohledání místa činu, ale i na znalostech a zkušenostech orgánů činných v trestném řízení (SVATOŠ[132,133]). Pachatelé počítačových trestných činů jsou ve většině případů vzdělaní lidé, středoškolsky nebo vysokoškolsky, v informačních či technických oborech, a tak budou vždy o krok napřed. Je nutné mít stále na paměti příčiny, důvody a motivy, z kterých je takový zločin páchán: snadná dostupnost výpočetní techniky v domácím i pracovním prostředí; připojení počítače k síti, kde proudí obrovské množství dat nepředstavitelnou rychlostí; rychlost spáchání trestného činu; zvědavost potenciálního pachatele, jeho anonymita, touha po dobrodružství, pomsta; důvěra uživatele; „děravá“ legislativa a nedostatečná informovanost v této oblasti.

Jak ale vůbec kontrolovat počítačovou kriminalitu?

- V oblasti represe:

[132] SVATOŠ, R. *Počítačová kriminalita*. Auspicia 2013, roč. X. č. 1, s. 171-178.
[133] SVATOŠ, R. *Kriminologie*. Plzeň: Aleš Čeněk, 2012. s. 189-199.

- Postih pachatelů dle trestního zákoníku.
- Zkvalitnit vzdělávání policejních orgánů v oblasti počítačové kriminality, zavést povinné vzdělání v této oblasti v rámci základní odborné přípravy.
- Zvýšení počtu pracovníků specialistů u Policie ČR.
- Kvalitní výpočetní technika.
- Spolupráce policie se zahraničím.

❖ V oblasti prevence:

- Působení na subjekty, které přicházejí do styku s výpočetní technikou (výchova pachatelů, vedení k odpovědnosti, zvyšování právního vědomí)
- Organizační opatření směřující k zpřehlednění činnosti (ochrana hesly, uchovávání paměťových médií, zákaz práce s chráněnými daty v době oprav, vymezení práce s chráněnými daty, opatření evidující činnost)
- Přímá ochrana výpočetní techniky (spolehlivé operační systémy, procedury zaznamenávající činnost, testovací programy, odstraňování zbytkových informací, zabezpečovací programy, šifrovací systémy, ochrana počítačových sítí) (SVATOŠ[134])

Situace ve světě je podobná situaci v České republice, v některých zemích např. třetího světa zcela chybí potřebná legislativa. Problematikou počítačové kriminality se zabývá policie, orgány činné v trestním řízení a v neposlední řadě i bezpočet vědců a výzkumníků, kteří se snaží vynalézt stále účinnější a důmyslnější řešení na ochranu dat, dopadení pachatelů, preventivní opatření atd. zde je uváděno ve zkratce několik z nich. Práce BACKHOUSE[135] například analyzuje problémy, které přináší vznik počítačové trestné činnosti a možných cest pro jeho kontrolu a řízení. Rozebírá různé přístupy ke studiu kriminality. Na základě těchto navrhuje výzkumnou perspektivu pro správu firemní počítačové trestné činnosti.

V rámci počítačové kriminality se s rostoucí popularitou internetu formují nové typy trestné činnosti. Zločin je komplexní, utajovaný a způsobuje obrovské sociální

[134] SVATOŠ, R. *Počítačová kriminalita*. Auspicia 2013, roč. X. č. 1, s. 171-178.
[135] BACKHOUSE, J., DHILLON, G. Managing computer crime: A research outlook. *Computer & security*. 1995. Vol. 14. Issue 7. s. 645-651.

škody. LIU[136] ve své studii vysvětluje definici počítačové kriminality a její hlavní typy, konkrétně v Číně, poukazuje na prevenci počítačové kriminality a trestání pomocí právních předpisů, kritizuje současnou situaci a předkládá návrhy (SOON[137]).

Schopnost předvídat počítačovou trestnou činnost se stává stále důležitější. Práce BROWNA[138] popisuje metodu pro zjištění preference počítačových zločinců. Zjištěné preference mohou být použity pro přímou ochranu počítačových systémů proti stávajícím útokům nebo na stavbu simulace budoucích útoků.

Povaha distribuce internetu vyžaduje, aby bezpečnostní otázky byly řešeny prostřednictvím spolupráce veřejných i soukromých subjektů. Studie HUEYE[139] zkoumá jeden aspekt role, kterou veřejnost může a má hrát v oblasti kybernetické bezpečnosti: civilní ochrana internetu. Zejména zkoumá motivy a jednání občanů, kteří pravidelně využívají své počítačové dovednosti k identifikaci, sledování a shromažďování informací o aktivitách podezřelých pachatelů trestných činů.

Kyberzločinem se obvykle rozumí přístup přes počítač bez svolení či řádného povolení vlastníka, modifikace nebo zničení počítačových dat. Na vyšším postu je kyberterorismus. Teroristické akce v kyberprostoru může být provedena nejen jedincem nebo teroristickou skupinou, ale může tu útočit i jeden stát proti druhému. Díky tomu se kyberterorismus neliší od jiného druhu terorismu. Specifická povaha hrozby se může pohybovat od odmítnutí služby odposlechu, podvodu, sabotáže a krádeže duševního vlastnictví a osobních informací. Studie SEKGWATHE[140] má za cíl poskytnout široký přehled o výzvách, kterým čelí svět v počítačové trestné činnosti. Neposledním cílem je odhalování a stíhání počítačové kriminality a otázka, jak země třetího světa drží krok s neustále se měnící technologií.

Policejní útvary a jiné donucovací orgány neustále analyzují obrovské množství dat trestních incidentů, aby lépe pochopily trestný čin v jejich jurisdikcích, identifikovaly významné změny v úrovni kriminality, plánovaly komunitní a sousedské

[136] LIU, H. Y. The network era of computer crime punishment and prevention research. 2012. In: Hu, J. *2nd international conference on applied social science*, Malaysia. Vol. 2. s. 161-166.
[137] SOON, C. T. Asean – computer crime and corrective action – A status-report. 1992. In: Gable, G. G., Caelli, W. J. *IT security: The need for international cooperation*, Singapore, Proceedings paper. Vol. 15. s. 23-33.
[138]BROWN, D. E., GUNDERSON, L. F. Using clustering to discover the preferences of computer criminals. IEEE transactions on systems man and cybernetics part A – *Systems and humans*. 2001. Vol. 31. Issue 4. s. 311-318.
[139] HUEY, L., NHAN, J., BROLL, R. Uppity civilians and cyber-vigilantes: The role of the general public in policing cybe-crime. *Criminology & criminal justice*. 2013. Vol. 13. Issue 1. s. 81-97.
[140] SEKGWATHE, V., TALIB, M. Cyber crime detection and protection: Third world still to cope-up. 2011. In: Yonazi, J. J., Sedoyeka, E., Ariwa, E., ElQawasmeh, E. *E-technologies and networks for development*, Tanzania. Vol. 171. s. 171-181.

reakce na trestné činy, za účelem vyšetřování a zatčení pachatele. Studie BROWNA[141] představuje systém vyvinutý na University of Virginia. Kromě propojení trestné činnosti podle místa, času a způsobu, tento systém dokáže rozpoznat významné změny v oblasti trestné činnosti a předvídat budoucí hrozby.

Počítačová forenzní technologie by v otázkách prevence mohla chránit data a informace před hackery. Přestože se jedná o nový obor, byl učiněn velký pokrok při vyšetřování počítačové kriminality na ochranu informací a dat. Byly vyvinuty výkonné nástroje pro zpracování důkazů. Studie AKHTERA[142] klade důraz na roli počítače v trestné činnosti a poskytuje vodítko pro práci s počítačem v této roli. Výsledky mohou být použity k vývoji postupů pro hodnocení digitálních důkazů a vyšetřování trestných činů za pomoci počítače.

Ve společnosti, kde informace představují jedno z nejcennějších aktiv podniků, je nutný holistický přístup k řízení bezpečnosti informačních systémů a je nezbytná prevence. Správně čelit počítačové trestné činnosti vyžaduje teorie, metody a techniky různých disciplín souvisejících s technickou, formální a neformální částí informačního systému. Cílem je více se zaměřit na lidské chování, a tím lépe pochopit počítačovou trestnou činnost (ME[143]).

Ať už se čeští či zahraniční vědci a výzkumníci věnují jakémukoli tématu v rámci řešené počítačových trestných činů, ať jsou to různé typy ochrany, spolupráce veřejných a soukromých subjektů nebo firemní počítačová trestná činnost, mým názorem je, že stěžejní je prevence. Je lepší býti připraven, nežli zaskočen. A prvopočátek prevence spatřuji v rané výchově dětí, kterým je tak dán základ slušného chování. Určitým nástrojem je samozřejmě legislativa, která je dle mého názoru v naší republice na slušné úrovni.

[141] BROWN, D. E., GUNDERSON, L. E., EVANS, M. H. Interactive analysis of computer crimes. *Computer*. 2000. Vol. 33. Issue 8. s. 69-+.
[142] AKHTER, F. E-commerce security: The categorical role of computers in forensic online crime. 2008 In: Yang, C. C., Chen, H., Chan, M., Chang, K., Lang, S. D., Chen, P. S., Hsien, P., Zeng, D., Wang, F. Y., Carley, K., Mao, W., Zhan, J. *Intelligence and security informatics, proceedings*, Taiwan. Vol. 5075. s. 298-303.
[143] ME, G. L., SPAGNOLETTI, P. Situational crime prevention and cyber-crime investigation: the online pedo-pornography case study. *Eurocon 2005*. 2005. Vol. 1-2. s. 1064-1067.

ZÁVĚR

Hlavním cílem práce bylo objasnění co je počítačová kriminalita, jak postupovat při objasňování a potírání této kriminality, zjištění příčin počítačové kriminality a navrhnutí opatření, které by tyto příčiny mohla alespoň částečně eliminovat.

Čili co je počítačová kriminalita? Stručnou definicí, se kterou si dovolím se ztotožnit, by mohlo být, že počítačová kriminalita je hospodářský trestný čin spáchaný pomocí počítače či internetu a podléhá členění dle trestního zákoníku: trestná činnost se speciální úpravou pro oblast počítačové kriminality, krádeže, poškození nebo zničení programu a dat na nosiči informací, neoprávněné užívání počítače, neoprávněný přístup k utajovaným informacím (hackerství), zneužití výpočetní techniky k jiné trestné činnosti. V rámci práce bylo odcitováno 17 literárních pramenů, tuzemských i zahraničních, které svým způsobem definují počítačovou kriminalitu. Vzhledem k tomu považuji tento cíl práce za splněný.

Dalším bodem ve stanovených cílech práce, který považuji za splněný, bylo, jak postupovat při objasňování a potírání tohoto typu kriminality. Zde bych uvedl dva nástroje, které považuji za prioritní. A to je výchova; jak výchova rodičovská a školní, tak i výchova zaměstnanců – programátorů, operátorů, IT techniků. A druhým nástrojem je „neprůstřelná“ legislativa, která bohužel jak u nás, tak i ve většině států celého světa chybí. Pokud nebude k dispozici účinný pevný legislativní nástroj, je velice těžké stavět na nestabilním základě a potírání počítačových zločinů není opravdu jednoduché. V současné době se využívá kromě legislativy například získávání důkazů z počítačových systémů – ověřování digitálních stop, informace z různých zdrojů a příprava platných argumentů. V USA například ustanovily kontrolní orgány specializované pracovní skupiny k řešení problémů ohledně počítačové kriminality. Často je obtížné definovat a rozhodnout, jestli se jedná o počítačový trestný čin nebo lidskou chybu, úmyslnou či neúmyslnou.

Jedním z hlavních cílů práce bylo zjistit příčiny počítačové kriminality a navrhnout opatření k jejich alespoň částečné eliminaci. Nejzásadnějších příčin vzniku počítačové kriminality je mnoho. Vznik samotného počítače byl tou úplně první. Následně přišlo propojení dvou a více počítačů a internet. Jistým lákadlem pro potenciálního pachatele je rychlost, s jakou může být takovýto čin proveden a v neposlední řadě je lidská zvědavost. Mít tu možnost si to „vyzkoušet“ možná i bez počátečního špatného úmyslu, jen ze zvědavosti. Velkou výhodou je skutečnost, že

u toho pachatel může sedět doma, nebo kdekoli jinde ve světě, na židli, v pohodlí a zahánět nudu, rozproudit adrenalin. V dnešní době je počítačová technika dostupná téměř každému, kdo projeví zájem. Vidina zisku tu hraje též nemalou roli. Počítačová kriminalita se v posledních letech změnila ve vzkvétající byznys, který vydělává miliardy dolarů.

Co dál, jak se postavit problému? Je potřeba začít u „člověka“ a jeho informovanosti, výchovy. Prioritou se stává informační bezpečnost. Nejdůležitějším opatřením je prevence. Stále důležitější se stává schopnost předpovídat počítačovou trestnou činnost. Je nutné zpřesnit i legislativní zázemí řešené problematiky, zajistit spolupráci veřejných i soukromých subjektů. Firmy musejí mít schopné manažery a IT techniky pro ochranu svých firemních dat. Velkým společnostem nepřicházejí hrozby jen zvenku, ale hrozí jim i od vlastních zaměstnanců. Z čehož plyne další rada – vybírat uvážlivě důvěryhodné zaměstnance na důležité posty.

Ze statistických údajů za posledních 16 let vyplývá, že se počty trestných činů spáchaných za pomoci počítače rapidně zvyšují. Nadále je potřeba zlepšovat spolupráci policie a veřejnosti. Veřejnost se již učí takovéto činy hlásit, ovšem nedostatečné množství odborníků v řadách Policie ČR snižuje objasněnost počítačových trestných činů. Je nezbytností dodržovat jak represivní opatření, tak i ta preventivní. Pokud tedy shrneme „dobré“ rady, primární je prevence, doporučuji stavět na pevné legislativě, celoživotním vzdělávání a výchově občanů od raného věku, vychovávání spolehlivých odborníků v oblasti IT, důmyslné ochraně především softwaru, mezinárodní spolupráci a v neposlední řadě i lidském rozumu.

SEZNAM POUŽITÉ LITERATURY

Literární zdroje

1. AKHTER, F. E-commerce security: The categorical role of computers in forensic online crime. 2008 In: Yang, C. C., Chen, H., Chan, M., Chang, K., Lang, S. D., Chen, P. S., Hsien, P., Zeng, D., Wang, F. Y., Carley, K., Mao, W., Zhan, J. *Intelligence and security informatics*, proceedings, Taiwan. Vol. 5075. ISSN 0302-9743. ISBN 978-3-540-69136-5.
2. ALEXANDER, M. Listen: Computer crime victims speak. *Datamation*. 1995. Vol. 41. Issue 23. ISSN 0011-6963.
3. ANGERFELT, B. Computer crimes – A study of different types of offenses and offenders. 1992. In: Gable, G. G., Caelli, W. J. *IT security: The need for international cooperation*. Vol. 15. ISSN 0926-5473. ISBN 0-444-89699-6.
4. ANONYMOUS. Computer crime cases up in Northern Ireland. *Digital investigation*. 2006. Vol. 3. Issue 4. ISSN 1742-2876.
5. ANONYMOUS. Computer crime-related legislation moves forward in US congres. *Computers & security*. 2006. Vol. 25. Issue 6. ISSN 0167-4048.
6. ANONYMOUS. CSI/FBI survey results show computer crime losses are declining. *Computers & security*, 2006. Vol. 25. Issue 6. ISSN 0167-4048.
7. ANONYMOUS. New Taiwan criminal code articles make computer crime a felony. *Computers & security*. 2003. Vol. 22. Issue 6. ISSN 0167-4048.
8. ANONYMOUS. New UK komputer crime-related legislation passes. *Computers & security*. 2007. Vol. 26. Isme 1. ISSN 0167-4048.
9. ANONYMOUS. Students face komputer crime penalties. *Computers & security*. 2003. Vol. 22. Issue 4. ISSN 01674048.
10. ANONYMOUS. Update on komputer crime-related legislation. *Computers & security*. 2006. Vol. 25. Issue 8. ISSN 0167-4048.
11. AUDAL, J., LU, Q., ROMAN, P. Computer crimes. *American criminal law review*. 2008. Vol. 45. Issue 2. ISSN 0164-0364.
12. BACKHOUSE, J., DHILLON, G. Managing computer crime: A research outlook. *Computer & security*. 1995. Vol. 14. Issue 7. ISSN 0167-4048.

13. BAKEWELL, E. J., KOLDARO, M., TJIA, J. M. Computer crimes. *American criminal law review*. 2001. Vol. 38. Issue 3. ISSN 0164-0364.
14. BARRETT, D. J. Statistics and computer crime. *Computer*. 1996. Vol. 29. Issue 7. ISSN 0018-9162.
15. BAZELON, D. L., CHOI, Y. J., CONATY, J. F. Computer crimes. *American criminal law review*. 2006. Vol. 43. Issue 2. ISSN 0164-0364.
16. BEDNAR, P. M., KATOS, V., HENNELL, C. Cyber-crime investigations: Complex collaborative decision making. 2008. In: Tryfonas, T., Thomas, P. (ed.) *Third international annual workshop on digital forensics and incident analysis*: WDFIA 2008, Proceedings. ISBN 978-0-7695-3362-9.
17. BENSON, C., JABLON, A. V., KAPLAN, A. V., ROSENTHAL, M. E. Computer crimes. *American criminal law review*. 1997. Vol. 34. Issue 2. ISSN 0164-0364.
18. BIEVER, C. Revealed: the true cost of komputer crime. *New scientist*. 2005. Vol. 186. Isme 2505. ISSN 0262-4079.
19. BOSSLER, A. M., HOLT, T. J. Assessing officer perceptions and support for online community policing. *Security journal*. 2013. Vol. 26. Issue 4. ISSN 0955-1662.
20. BOWKER, A. L., THOMPSON, G. B. Computer crime in the 21st century and its effect on the probation officer. *Federal probation*. 2001. Vol. 65. Issue 2. ISSN 0014-9128.
21. BROADHURST, R. Developments in the global law enforcement of cyber-crime. *Policing – an international journal of police strategies & management*. 2006. Vol. 29. Issue 3. ISSN 1363-951X.
22. BROWN, D. E., GUNDERSON, L. E., EVANS, M. H. Interactive analysis of computer crimes. *Computer*. 2000. Vol. 33. Issue 8. ISSN 0018-9162.
23. BROWN, D. E., GUNDERSON, L. F. Using clustering to discover the preferences of computer criminals. *IEEE transactions on systems man and cybernetics part A – Systems and humans*. 2001. Vol. 31. Issue 4. ISSN 1083-4427.
24. CARTER, A. J., PERRY, A. Computer crimes. *American criminal law review*. 2004. Vol. 41. Issue 2. ISSN 0164-0364.
25. CARUCCI, D., OVERHULS, D., SOARES, N. Computer crimes. *American criminal law review*. 2011. Vol. 48. Issue 2. ISSN 0164-0364

26. COLDWELL, R. A. Some social parameters of computer crime. *Australian computer journal*. 1990. Vol. 22. Issue 2. 144 p. ISSN 0004-8917.
27. COLLIER, P. A., SPAUL, B. J. A forensic methodology for countering computer crime. *Artificial intelligence review*. 1992. Vol. 6. Issue 2. ISSN0269-2821.
28. COOPER, D., PFLEEGER, C. Statistics and computer crime – Reply. *Computer*. 1996. Vol. 29. Issue 7. ISSN 0018-9162.
29. COPLER, J. A. *Computer crime: A crime fighter's handbook – Icove*, D., Seger, K., VonStorch, W. Online. 1996. Vol. 20. Issue 1. ISSN 0146-5422.
30. CRONAN, T. P., FOLTZ, C. B., JONES, T. W. Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*. 2006. Vol. 49. Issue 6. ISSN 0001-0782.
31. DHILLON, G. SILVA, L., BACKHOUSE, J. Computer crime at CEFORMA: a case study. *International journal of information management*. 2004. Vol. 24. Issue 6. ISSN 0268-4012.
32. DHILLON, G., MOORES, S. Computer crimes: theorizing about the enemy within. *Computer & security*. 2001. Vol. 20. Issue 8. ISSN 0167-4048.
33. DILLON, S. A., GROENE, D. E., HAYWARD, T. Computer crimes. *American criminal law review*. 1998. Vol. 35. Issue 3. ISSN 0164-0364.
34. DITZION, R., GEDDES, E., RHODES, M. Computer crimes. *American criminal law review*. 2003. Vol. 40. Issue 2. ISSN 0164-0364.
35. DOČEKAL, D., ECKERTOVÁ, L. *Bezpečnost dětí na internetu*. Brno: Computer Press, 2013. 224 s. ISBN 978-80-2513-804-5.
36. DOUBRAVA, J. *Počítačová kriminalita (trestněprávní a kriminologické aspekty).* Univerzita Palackého v Olomouci, Právnická fakulta. 2011. Diplomová práce. 55 s.
37. DOWNLAND, P. S., FURNELL, S. M., ILLINGWORTH, H. M., REYNOLDS, P. L. Computer crime and abuse: A surfy of public attitudes and awareness. *Computers & security*. 1999. Vol. 18. Issue 8. ISSN 0167-4048.
38. DUFF, L., GARDINER, S. Computer crime in the global village: Strategies for kontrol and regulativ – In defence of the hacker. *International journal of the sociology of law*. 1996. Vol. 24. Isme 2. ISSN 0194-6595.
39. GILL, M. S. Cybercops take a byte out of computer crime. *Smithsonuan*. 1997. Vol. 28. Issue 2. ISSN 0037-7333.

40. GILL, P. Fighting computer crime – Report on the forensic team of the justice department of Basel. *Kriminalistik*. 2003. Vol. 57. Issue 6. ISSN 0023-4699.
41. HANCOCK, B. US department of justice computer crime legislation information site. *Computers & security*. 1998. Vol. 17. Issue 1. ISSN 0167-4048.
42. HANCOCK, B. Who do you call for help with komputer crime? *Computers & security*. 1998. Vol. 17. Issue 2. ISSN 0167-4048.
43. HANSEN, M. Crime and computers. *Aba journal*. 2002. Vol. 88. ISSN 0747-0088.
44. HARBORT, S. Crime in cyberspace – New forms of time-specific computer crimes. *Kriminalistik*. 1996. Vol. 50. Issue 3. ISSN 0023-4699.
45. HATCHER, M., MCDANNELL, J., OSTFELD, S. Computer crimes. *American criminal law review*. 1999. Vol. 36. Issue 3. ISSN 0164-0364.
46. HAUGEN, S., SELIN, J. R. Identifying and controlling computer crime and employee fraud. *Industrial management & data systems*. 1999. Vol. 99. Issue 7-8. ISSN 0263-5577.
47. HELLEBRANDOVÁ, H. *Počítačová kriminalita*. Právnická fakulta Masarykovy univerzity v Brně. 2006. Bakalářská práce. Vedoucí práce Kratochvíl V. 42 s.
48. HIGHLAND, H. J. Fighting komputer crime. *Computers & security*. 1996. Vol. 15. Issue 1. ISSN 0167-4048.
49. HINDUJA, S. Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing-An international journal of police strategies & management*. 2004. Vol. 27. Issue 3. ISSN 1363-951X.
50. HOLCR, K. a kol. *Kriminologie*. 1. Vydání Praha: Leges, 2008, s. 403. ISBN 978-80-8078-206-1.
51. HOLT, T. J., BOSSLER, A. M. An Assessment of the Current State of Cybercrime Scholarship. 2014. *Deviant Behavior*. Vol. 35. Issue 1. ISSN 0163-9625
52. HRUŠÁKOVÁ, M. Vybrané majetkové trestné činy v novém trestním zákoníku ve srovnání s aktuální úpravou, se zaměřením na nedbalostní trestné činy. 2009. *Buletin advokacie*. Vol. 10. 118 s.
53. HUANG, X. M., RADKOWSKI, P., ROMAN, P. Computer crimes. *American criminal law review*. 2007. Vol. 44. Issue 2. ISSN 0164-0364.

54. HUEY, L., NHAN, J., BROLL, R. 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. 2013. *Criminology & Criminal Justice*. Vol. 13. Issue 1. ISSN 1748-8958.
55. HUGHES, G. Computer crime – The liability of hackers. *Australian computer journal*. 1990. Vol. 22. Issue 2. ISSN 0004-8917.
56. HULANOVÁ, L. Internet jako dobrý pomocník, ale zlý pán. In: Medřická, J. (ed.) *Sborník příspěvků z konference Pražské linky důvěry „Poskytování krizové pomoci – výměna zkušeností a know-how“.* 2012. Vydalo Centrum sociálních služeb Praha. 217 s.
57. HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.
58. CHEN, C. Y., LINDSAY, G. Viruses, attacks, and sabotage: It's a computer crime wave. *Fortune*. 2000. Vol. 141. Issue 10. ISSN 0015-8259.
59. CHIMHENO, R. M., DEHGHANTANHA, A. Framework for cyber crime law implementation in Zimbabwe. *Third international conference on computer engineering and technology*, Malaysia. 2011. ISBN 978-0-7918-5973-5.
60. JACOBSON, H., GREEN, R. Computer crimes. *American criminal law review*. 2002. Vol. 39. Issue 2. ISSN 0164-0364.
61. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 2007. Praha: Grada Publishing, a.s. 284 s.
62. KAO, D. Y., WANG, S. J. The IP address and time in cyber.crime investigation. *Policing-An international journal of police strategies & management*. 2009. Vol. 32. Issue 2. ISSN 1363-951X.
63. KERR, O. S. lifting the „fog“ of internet suveillance: How a suppression remedy would change computer crime law. *Hasting law journal*. 2003. Vol. 54. Issue 4. ISSN 0017-8322.
64. KIM, C., NEWBERGER, B., SHACK, B. Computer crimes. *American criminal law review*. 2012. Vol. 49. Issue 2. ISSN 0164-0364.
65. KLEINDIENST, K. T., COUGHLIN, T. M., PASQUARELLA, J. K. Computer crimes. *American criminal law review*. 2009. Vol. 46. Issue 2. ISSN 0164-0364.
66. KOCMAN, R., LOHNISKÝ, J. *Jak se bránit virům, spamu a spyware*. 1. Vydání Computer press 2005, s. 152, ISBN 9788025107935.
67. KUCHTA, J. a kol. *Kriminologie* I. Část, 1. Vydání Brno: MU, 1993, s. 135. ISBN 80-210-0616-1.

68. KUCHTA, J., VÁLKOVÁ, H. a kol. *Základy kriminologie a trestní politiky*. 1. Vydání Praha: C. H. Beck, 2005, s. 568. ISBN 80-7179-813-4.
69. LEWIS, B. C. Prevention of computer crime amidst international anarchy. *American criminal law review*. 2004. Vol. 41. Issue 3. ISSN 0164-0364.
70. LIU, H. The Network Era of Computer Crime Punishment and Prevention Research. 2012 In: HU, J. *2nd International Conference on Applied Social Science* (ICASS 2012) Location: Kuala Lumpur, MALAYSIA, FEB 01-02, 2012, Vol. 2. Proceedings paper. ISBN: 978-1-61275-006-4
71. LOIA, V., MATTIUCCI, M., SENATORE, S., VENIERO, M. Computer crime investigation by means of fuzzy semantic maps. 2009. In: BaezaYates, R., Berendt, B., Bertino, E., Lim, E. P., Pasi, G. *International conferences on web intelligence*, Milan, Italy. Vol. 3. ISBN 978-1-4244-5331-3.
72. MARSHALL, A. M., TOMPSETT, B. C. Spam 'n'chips – A discussion of internet crime. *Science & justice*. 2002. Vol. 42. Issue 2. ISSN 1355-0306.
73. MATĚJKA, M. *Počítačová kriminalita*. Brno: Computer Press. 2002. 120 s. ISBN 80-7226-419-2.
74. MCCURDY, J. L. Computer crimes. *American criminal law review*. 2010. Vol. 47. Issue 2. ISSN 0164-0364.
75. ME, G. L., SPAGNOLETTI, P. Situational crime prevention and cyber-crime investigation: the online pedo-pornography case study. *Eurocon 2005*. 2005. Vol. 1-2. ISBN 1-4244-0049-X.
76. MOON, B., MCCLUSKEY, J. D., MCCLUSKEY, C. P., LEE, S. Gender, General Theory of Crime and Computer Crime: An Empirical Test. 2013. *International Journal of Offender Therapy and Comparative Criminology*. Vol. 57. Issue 4. ISSN 0306-624X
77. MUSIL, S., *Počítačová kriminalita.* Praha: Kufr, 2000. 298 s. ISBN 80-86008-80-0.
78. NEVILLE, K. Virtually criminal: Crime, deviance and regulation online. *Online information review*. 2008. Vol. 32. Issue 1. ISSN 1468-4527.
79. NG, D., TSUI, E. Knowledge – intensit collaboration to vombat cyber crime in the Asia Pacific Region. 2010. In: Tsui, E. *Proceedeings of the 7th international conference on intellectual capital, knowledge management and organisational learning*, China. ISBN 978-1-906638-84-9.

80. NICOLESCU, C. Economic consequences of software crime. Romania within the EU. *Oportunities, requirements and perspectives*. 2007. Vol. 1. ISBN 978-973-739-428-6.
81. NICHOLSON, L. J., SHEBAR, T. F., WEINBERG, M. R. Computer crimes. *American criminal law review*. 2000. Vol. 37. Issue 2. ISSN 0164-0364.
82. NOVOTNÝ, J., SCHULTE, D., MÁNES, G., SHENOI, S. Remote computer fingerprinting for cyber crime investigations. In: DeCapitaniDiVimercati, S., Ray, I., Ray, I. *Data and applications security XVII. Status and prospects*. 2004. Vol. 142. ISSN 1571-5736. ISBN 1-4020-8069-7.
83. PATERNOSTER, R., MCGLOIN, J. M., NGUYEN, H., THOMAS, K. The Causal Impact of Exposure to Deviant Peers: An Experimental Investigation. 2013. *Journal of Research in Crime and Delinquency*. Vol. 50. Issue 4. ISSN: 0022-4278
84. PERRITT, H. H., CHARNEY, S., MILLER, G. P. Computer crimes now on the books: What do we do from here? *Temple law review*. 1997. Vol. 70. Issue 4. ISSN 0040-2974.
85. POUNDER, C. The counsil of Europe cyber-crime convention. *Computer & security*. 2001. Vol. 20. Issue 5. ISSN 0167-4048.
86. RAI, G., DUBASH, R. K., CHAKRAVARTI, A. K. Computer related crimes. *Electronics information & planning*. 1998. Vol. 25. Issue 9. ISSN 0304-9876.
87. RASKIN, X., SCHADACHPAIVA, J. Computer crimes. *American criminal law review*. 1996. Vol. 33. Issue 3. ISSN 0164-0364.
88. ROGERS, M. K., SEIGFRIED, K., TIDKE, K. Self-reported computer criminal behavior: A psychological analysis. *Digital investigation*. 2006. Sp. Issue. ISSN 1742-2876.
89. SAARI, J. Legal response to a computer crime – retrospect of a mere chance case. *Computer security*. 1993. Vol. 37. ISSN 0926-5473. ISBN 0-444-81748-4.
90. SEKGWATHE, V., TALIB, M. Cyber Crime Detection and Protection: Third World Still to Cope-Up. 2011. In: YONAZI, J. J., SEDOYEKA, E., ARIWA, E., ELQAWASMEH, E. *E-Technologies and network for development*. Book Series: Communications in Computer and Information Science. Vol. 171. Proceedings Paper. ISSN: 1865-0929, ISBN: 978-3-642-22728-8
91. SCHULTZ, E. Computer crime cost the UK 145 pound milion in 2002. *Computers & security*. 2003. Vol. 22. Issue 5. ISSN 0167-4048.

92. SCHULTZ, E. Variety of komputer crime-related bills passed. *Computers & security*. 2004. Vol. 23. Issue 8. ISSN 0167-4048.
93. SCHULZ, E. New clause in UK computer crime legislation would make big difference. *Computers & security*. 2006. Vol. 25. Issue 4. ISSN 0167-4048.
94. SCHULZ, E. Police change tactics to deal with computer crime victims. *Computers & security*. 2003. Vol. 22. Issue 5. ISSN 0167-4048.
95. SIMUNDIC, S., FRANJIC, S., SUSIC, T. Databases and komputer crimes. Proceedings elmar – 2010. 2010. In: Grgic, M., Bozek, J., Grgic, S. *52nd international symposium ELMAR*, Zadar, Croatia. ISSN 1334-2630. ISBN 978-953-7044-11-4.
96. SKINNER, W. F., FREAM, A. M. A social learning theory analysis of computer crime among college students. *Journal of research in crime and deliquency*. 1997. Vol. 34. Issue 4. ISSN 0022-4278.
97. SOMA, J. T., MUTHER, T. F., BRISSETTE, H. M. L. Transnational extradition for computer crimes_ Are new treaties and laws needed? *Harvard journal on legislation*. 1997. Vol. 34. Issue 2. ISSN 0017-808X.
98. SOON, C. T. Asean – computer crime and corrective action – A status-report. 1992. In: Gable, G. G., Caelli, W. J. *IT security: The need for international cooperation*, Singapore, Proceedings paper. Vol. 15. ISSN 0926-5473. ISBN 0-444-89699-6.
99. SVATOŠ, R., *Kriminologie*. Plzeň: Aleš Čeněk, 2012. 290 s. ISBN 978-80-7380-389-6.
100. SVATOŠ, R. Mládež a extremismus v České republice. *Auspicia*. 2013, roč. X, č. 2. 208 s. ISSN 1214-4967.
101. SVATOŠ, R. Počítačová kriminalita. *Auspicia*, 2013, roč. X, č. 1. 260 s. ISSN 1214-4967.
102. TAN, Y., QI, Z., WANG, J. Applications of Association Rules in Computer Crime Forensics. 2012. In: GUO, J. *Mechatronics and applied mechanics*. Vol. 157-158. Proceedings Paper. ISSN: 1660-9336 ISBN: 978-3-03785-380-1
103. TOMPSETT, B. C., MARSHALL, A. M., SEMMENS, N. C. Cyberprofiling: Offender profiling and geographic profiling of crime on the internet. *Workshop of the 1st int. Conf. on security and privacy for emerging areas in communication networks*. 2005. ISBN 0-7803-9468-2.

104. VELIČKOVÁ, L. *Internetová kriminalita zaměřená proti dětem*. Praha, 2009. 142 s. Univerzita Karlova, Filozofická fakulta, Katedra psychologie. Diplomová práce.

105. VONGRAVENREUTH, G. F. IT-security and computer crime. *Wirtschaftsinformatik*. 1992. Vol. 34. Issue 4. ISSN 0937-6429.

106. VOTH, D. Task force tackles computer crime. *IEEE software*. 2004. Vol. 21. Issue 4. ISSN 0740-7459.

107. WALLACE, R. P., LUSTHAUS, A. M., KIM, J. H. J. Computer crimes. *American criminal law review*. 2005. Vol. 42. Issue 2. ISSN 0164-0364.

108. WANE, P. Child pornografy: Crime computers and society. *Information communication & society*. 2009. Vol. 12. Issue 8. ISSN 1369-118X.

109. WANG, S. J. Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer standards & interfaces*. 2007. Vol. 29. Issue 2. ISSN 0920-5489.

110. WANG, X. G. Research on relevant problems of computer crime and electronic evidence. 2013. In: Chang, T. 2012 *International conference on education reform and management innovation*, China. Vol. 5. ISBN 978-1-61275-049-1.

111. WIBLE, B. A site where hackers are welcome: Using hack-in contents to shape preferences and deter computer crime. *Yale law journal*. 2003. Vol. 112. Issue 6. ISSN 0044-0094.

112. WIGGINS, L. M. Corporate komputer crime: Collaborative power in numbers. *Federal probatik*. 2002. Vol. 66. Isme 3. ISSN 0014-9128.

113. WILLISON, R., BACKHOUSE, J. Opportunities for komputer crime: considering systems risk from a criminological perspective. *European journal of informatik systems*. 2006. Vol. 15. Isme 4. ISSN 0960-085X.

114. WILSON, C. Holding management accountable: A new policy for protection against computer crime. *Proceedings of the IEEE 2000 national aerospace and electronics conference: Engineering tomorrow*. 2000. ISBN 0-7803-6262-4.

115. YIP, M., WEBBER, C., SHADBOLT, N. Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & society*. 2013. Vol. 23. Issue 4. ISSN 1043-9463.

116. ZAPLETAL, J. a kol. *Kriminologie pro posluchače magisterského studijního programu*. Praha: PA ČR, 2002, s. 184. ISBN 80-7251-103-3.
117. ZÁVRŠNÍK, A. Computer crime and digital investigation. *Revija za kriminalistiko in kriminologijo*. 2008. Vol. 59. Issue2. ISSN 0034-690X.

Elektronické zdroje

1. CELENTANO, L., Z., FARMER, J., J. *Computer crime, A joint report,* 2000 [online] Dostupné z WWW: <http://csrc.nist.gov/publications/secpubs/computer.pdf>.
2. *EU Kids Online 2009-11, final report* [online] Dostupné z WWW: <http://www.lse.ac.uk/home.aspx>.
3. HOLA, V. *Historie a vznik počítačů*. 2002. [online] Dostupné z WWW: <http://utf.mff.cuni.cz/vyuka/OFY016/F2001/Hola/referat.html>.
4. SIEBERT M. *Počítačová kriminalita: byznys za miliardy.* 2009. [online] Dostupné z WWW: <http://euro.e15.cz/profit/pocitacova-kriminalita-byznys-za-miliardy-895968>.
5. WAST. *Vznik a vývoj počítačů.* 2007. [online] Dostupné z WWW: <http://www.gamepark.cz/vznik_a_vyvoj_pocitacu_11279.htm>.
6. MORÁVEK D. *Zisky z počítačové krominality předčily zisky z drog.* 2010. [online] Dostupné z WWW: <http://www.podnikatel.cz/clanky/zisky-z-pocitacove-kriminality-predcily-drogy/>.
7. KONRÁD a kol. *Metodika vyšetřování jednotlivých druhů trestných činů*. 1999 [online] Dostupné z WWW: <http://www.vakobobri.cz/e107_files/public/metodika_vysetrovani_jednotlivych_trestnych_cinu.doc>.
8. MURČÁ J. *Počítačová kriminalita* [online] 2009. Dostupné z WWW: <http://referaty.portik.cz/rubrika/informatika/pocitacova-kriminalita-0/>.
9. OAK, M. *Types of computer crimes*. 2008 [online] Dostupné z WWW: <http://www.buzzle.com/articles/types-of-computer-crimes.html>.

10. PALEČEK, J. *Kybernetický zločin okrádá lidi po celém světě o 110 miliard dolarů ročně* [online] Dostupné z WWW: <http://pcworld.cz/novinky/kyberneticky-zlocin-okrada-lidi-po-celem-svete-o-110-miliard-dolaru-rocne-44833>.
11. POT, J. *Top five computer crimes & how to protect yourself from them*. 2010. [online] Dostupné z WWW: <http://www.makeuseof.com/tag/top-five-computer-crimes-protect/>.
12. PwC - *Počítačová kriminalita pod lupou, Celosvětový průzkum hospodářské kriminality*, Česká republika. 2011 [online] Dostupné z WWW: <www.pwc.cz/crimesurvey>.
13. STANDLER, R. B. *Computer crime*. 2002 [online] Dostupné z WWW: <http://www.rbs2.com/ccrime.htm>.
14. STANDLER, R. B. *Tips for avoiding computer crime*. 2012 [online] Dostupné z WWW:<http://www.rbs2.com/cvict.htm>.
15. WAST. *Vznik a vývoj počítačů*. 2007. [online] Dostupné z WWW: <http://www.gamepark.cz/vznik_a_vyvoj_pocitacu_11279.htm>.
16. Wikipedie [online] Dostupné z WWW: <http://cs.wikipedia.org>
17. WOJTOVIČ, J. *Kybernetická kriminalita – výnosný a rychle rostoucí byznys*. 2013 [online] Dostupné z WWW: <http://www.internetprovsechny.cz/kyberneticka-kriminalita-vynosny-a-rychle-rostouci-byznys/www.mvcr.cz>.
18. Zákon č. 40/2009 Sb., trestní zákoník, v platném znění 2009. [online] In: *Sbírka zákonů České republiky*, 354-461. Dostupné z WWW:<http://zakony.centrum.cz/trestni-zakonik>.
19. Senát parlamentu ČR, Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě, 2013 [online] Dostupné z WWW: <http://www.senat.cz/xqw/webdav/pssenat/original/66810/ 56264>.

VYSVĚTLIVKY

Zdroj Wikipedie [online] Dostupné z WWW: <http://cs.wikipedia.org>.

Phishing - je podvodná technika používaná na internetu k získávání citlivých údajů v elektronické komunikaci.

Pharming - je podvodná technika používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu po napsání URL banky do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky. Ani zkušení uživatelé nemusejí poznat rozdíl (na rozdíl od příbuzné techniky phishingu).

Spyware – je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.

Adware – je označení pro produkty znepříjemňující práci nějakou reklamní aplikací. Ty mohou mít různou úroveň agresivity - od běžných *bannerů* až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemnou věcí je např. změna domovské stránky ve Windows Internet Exploreru, aniž by o to uživatel měl zájem.

Hacker - počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb. V masmédiích se tento termín používá pro počítačové zločince a narušitele počítačových sítí, kteří se ale správně označují termínem *cracker*. Dnes jsou oba pojmy často zaměňovány a pro pojem blízký původnímu významu se používají také termíny *geek, guru, nerd*. V užším významu se slovo cracker často používá ve významu průnikář.

Extroverze – vyznačuje se pozitivním vztahem k vnějšímu světu. Extroverze je charakterizována zájmem o vnější objekty, vnímavostí k vnějším událostem a jejich pohotovým přijímáním. Extrovert má neutuchající zájem o okolní svět, o účast na společenských setkáních a navazování přátelství.

Banner – je druh reklamy používaný na WWW stránkách. Jedná se o zpravidla obdélníkový obrázek či animaci, případně interaktivní grafiku zobrazenou nejčastěji poblíž okraje obrazovky. Bannery tvoří stále jednu z nejčastějších forem reklamy na Internetu.

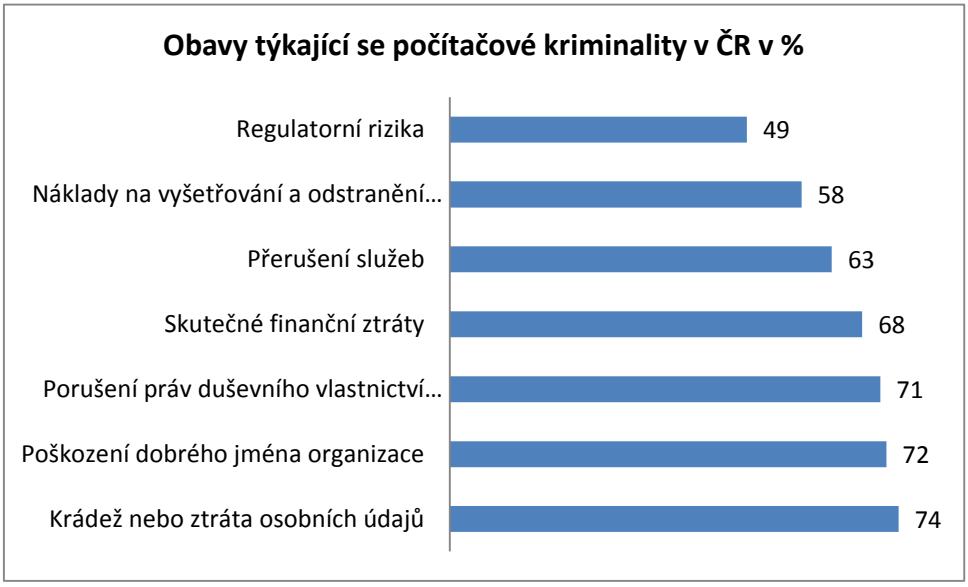
Viktimizace - je pojem, který se užívá v kriminologii, kriminalistické psychologii a mediálních studiích. Označuje proces, během něhož se oběť trestného činu, poté, co o ní a činu referují média, stane obětí znovu - tentokrát trpí psychicky.

Spoofing - označuje v informatice vytvoření IP datagramu s falešnou zdrojovou IP adresou, který je následně odeslán počítačovou sítí k cílovému počítači, před kterým má být zatajena totožnost odesílatele.

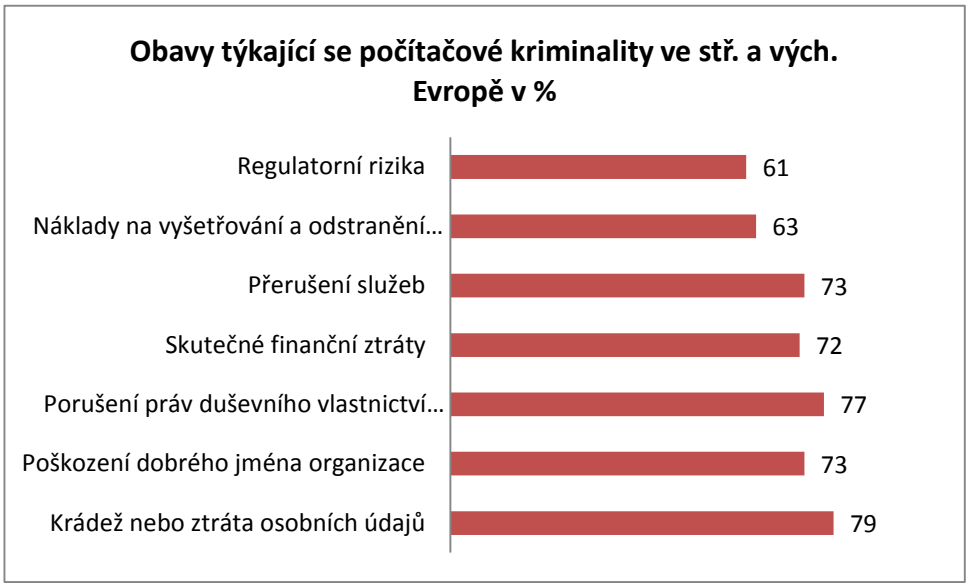
MITM (Man in the middle) - podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Důležitým faktem je, že v prostředí současných běžných počítačových sítí není nutné, aby Mallory (útočník) ležel fyzicky na cestě mezi Alicí a Bobem, protože lze síťový provoz snadno přesměrovat.

PŘÍLOHY

Příloha I: Počítačová kriminalita v České republice

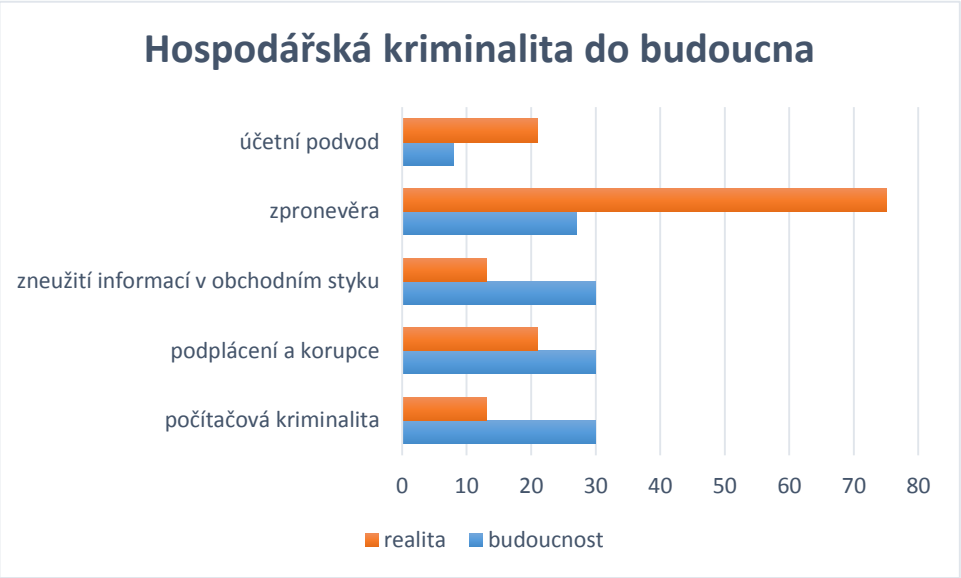


Příloha II: Počítačová kriminalita v zemích střední a východní Evropy



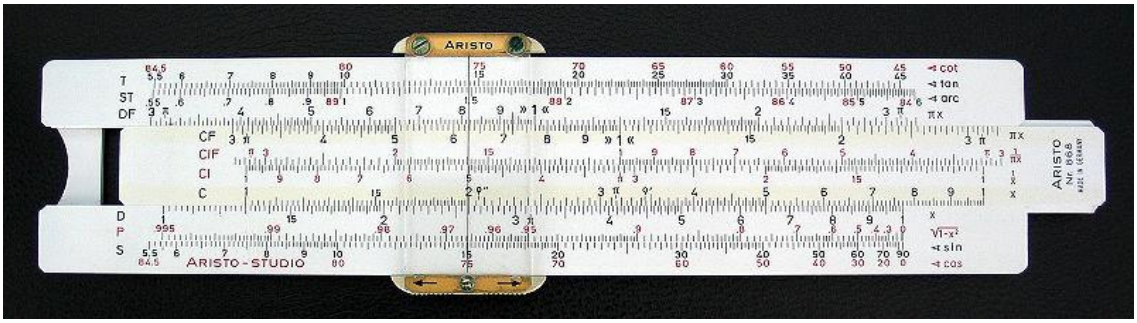
Příloha III: Počítačová kriminalita v celosvětovém měřítku

Příloha IV: Trend hospodářské kriminality v ČR do budoucna



Příloha V: Logaritmické pravítko

Wikipedie [online] Dostupné z WWW: <http://cs.wikipedia.org>.



Příloha VI: Abakus