Počítačová kriminalita s využitím internetové sítě

Computer crime using Internet network

Bc. Zuzana Prajzová

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zuzana PRAJZOVÁ**
Osobní číslo:	**A10946**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačová kriminalita s využitím internetové sítě**

Zásady pro vypracování:

1. **Prostudujte problematiku počítačové kriminality a jejích aktuálních trendů v ČR.**
2. **Pro získání vstupních dat pro vaši práci kontaktujte a popř. navštivte organizace, které se zabývají počítačovou kriminalitou.**
3. **Na základě získaných informací vytvořte rešerši aktuálních trendů počítačové kriminality v ČR.**
4. **Zpracujte statistiky počítačové kriminality v ČR za uplynulých několik let.**
5. **Zpracujte analýzu přičin nízké trestanosti počítačové kriminality v ČR ve všech jejích podobách.**
6. **Na základě rozhovorů se zástupci organizací z 1. bodu zadání sepište návrhy a možnosti pro zlepšení situace v oblasti počítačové kriminality v ČR.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MATĚJKA, M.: Počítačová kriminalita, Computer Press, Praha 2002, ISBN 80-7226-419-2.**
2. **DUNNIGAN, J.F.: Bojiště zítřka, Jak čelit globálnímu nebezpečí kyberterorizmu, BARONET, Praha 2004, ISBN 80-7214-642-4.**
3. **PORADA, V., Rak R. a kol.: Kriminalita související s informačními technologiemi a identifikace osob na základě projevu lokomoce člověka , Praha 2007, ISBN 978-80-254-0797-4.**
4. **ONDREJKA, V.: Podvody na internetu, Nová Forma s.r.o., EAN: 9700201005101.**
5. **SMEJKAL, V. Právo informačních a telekomunikačních systémů. Praha: C.H. BECK, 2004, ISBN: 80-7179-765-0.**
6. **LÁTAL, I. Ochrana informací, dat a počítačových systémů. Praha: Eurounion, 1996, ISBN 80-85858-32-0.**
7. **DUNNIGAN, J. Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu. Praha:Baronet, 2004, ISBN 80-7214-642-4.**
8. **CURTIN, M. Brute force: cracking the data encryption standard. New York: Copernicus Books, 2005, ISBN 0387201092.**
9. **DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat. Praha : Computer Press, 2004., ISBN 80-251-0106-1.**

Vedoucí diplomové práce:	**Ing. Tomáš Dulík** Ústav informatiky a umělé inteligence
Datum zadání diplomové práce:	**28. února 2011**
Termín odevzdání diplomové práce:	**17. října 2011**

Ve Zlíně dne 28. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce je zaměřená na problematiku počítačové kriminality a jejich aktuálních trendů. Popisuje nejčastější druhy, kterými se zabývá Policie ČR. V praktické části naleznete vývoj této trestné činnosti za uplynulých několik let. Je zde popsána analýza příčin nízké trestnosti. V neposlední řadě se v této diplomové práci zabývám návrhem možností na zlepšení této situace. Cílem této práce je seznámení s touto problematikou a boji proti ní.

Klíčová slova: Internet, kriminalita, kybernalita, extremismus, dětská pornografie, autorské právo, nebezpečné komunikační jevy

ABSTRACT

The thesis is focused on the issues of cyber crime and thein trends. It describes the most common species, which the Police must deal with. The practical part shows development of thes crimes in the past few years. It describes and analyses the causes of the criminality. It also deals with options to improve this situation.

Keywords: Internet, crime, Cybernality, extremism, childpornography, copyright, unsafe communication phenomena.

Tímto děkuji panu Ing. Tomášovi Dulíkovi za velmi užitečnou metodickou pomoc, spolupráci a ochotu při zpracování mé diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Jeden z hlavních rysů současnosti je každodenní užívání informačních a komunikačních technologií, které nás obklopují všude kolem, vstupují do všech oblastí lidské činnosti. Informační technologie se užívají ve zdravotnictví, školství, výzkumu, průmyslu, v běžném uživatelském životě. Přes Internet telefonujeme, chatujeme, objednáváme výrobky a zboží, seznamujeme se, vyhledáváme informace a mnoho dalších aktivit. Se snahou maximálního využití ale také vzrůstá snaha lidí tuto technologii co nejvíce využít k páchání trestné činnosti.

I přes to, že je informační a počítačová kriminalita relativně mladým oborem, její bleskový vývoj se stal během posledních let jedním z nejvýznamněji a nejvíce rozvíjejících se trestných činů u nás.

Ve své diplomové práci se zabývám Internetem jako takovým, jeho historií u nás i v světě. V druhé části popisuji jednotlivé formy trestných činů u nás. Jde o trestné činy, kterými se nejvíce zabývá policie ČR, mezi tyto trestné činy patří zejména dětská pornografie, extremistické projevy, porušování autorských práv, nebezpečné komunikační jevy, zneužívání obchodních a platebních styků.

V praktické části najdete vybrané druhy trestných činů a jejich statistiky za uplynulých několik let. Vzhledem k dostupnosti materiálů a jejich další využitelnosti jsem se rozhodla o zúžení tohoto výběru na extremistické projevy, porušování autorských práv a dětskou pornografii.

V závěru práce, konkrétně ve 4. kapitole, naleznete analýzu příčin nízké trestnosti. Jedním z nejzávažnějších rozdílů oproti „klasickému“ páchání trestné činnosti je fakt, že informační kriminalita může být páchána na jiném místě, než se konkrétní trestný čin stal, je páchán beze zbraní, bez krve, fyzicky poškozené oběti, ale i dalších běžných hmatatelných důkazů. Dále je v mé práci obsažen návrh na možnosti zlepšení situace, které jsou navrženy po kontaktování a prostudování problematiky s příslušnými orgány a institucemi, které se zabývají bojem proti této kriminalitě.

Cílem mé diplomové práce je seznámit čtenáře s nejrozšířenějšími druhy internetové kriminality u nás, následnými statistikami vývoje této trestné činnosti a v závěru popsat analýzu příčin nízké trestnosti a navrhnout možnosti na zlepšení situace.

I. TEORETICKÁ ČÁST

1 INTERNET

1.1 Co je to Internet

Odpovědí na otázku „co je to Internet?“ bychom určitě našli mnoho, ať už na samotném internetu nebo v různých publikacích, existuje mnoho definic. Takže co to vlastně Internet je?

- Je mezinárodní počítačovou sítí.
- Je jméno jedné konkrétní soustavy vzájemně propojených sítí.
- Internet je pouze jeden.
- Jako celek nemá žádného vlastníka.
- Své vlastníky mají jen dílčí sítě Internetu.

1.2 Internet z právního hlediska

Tzv. „počítačové právo“ (computer law) či „informatické právo“ je průřezovou právní disciplínou, která se zabývá nejrůznějšími právními obory a odvětvími, spojenými jedním společným prvkem - počítačem, jeho obsahem (daty a programy) a jeho příslušenstvím. Toto odvětví se vytváří napříč klasickými právními disciplínami, protože zasahuje do veřejnoprávní i soukromoprávní sféry, do procesních norem, do teritoriálních i mezinárodních úprav, do občanského, obchodního, správního, trestního i dalších oblastí práva. V zahraničí se používá termín „cyber law“ (kybernetické právo), a to zejména ve spojení s právem na internetu. [39]

Internet jako takový není subjektem práva – nemá právní subjektivitu, není ani ryze hmotným předmětem, ani čistě nehmotným statkem a dokonce není ani objektivní právní skutečností, nezávislou na lidském chování. Jde o informační a komunikační systém, který jako celek nemá svého majitele. Subjekty právních vztahů jsou v tomto případě uživatelé internetu, poskytovatelé služeb, vlastníci serverů a sítí apod. Právní vztahy při přenosu dat v internetu vznikají mezi jednotlivými provozovateli sítí, ale především mezi koncovými uživateli a providerem. Objekty práva jsou hmotné i nehmotné objekty, chování, resp. výsledky určitého chování apod. Z naznačených charakteristik internetu vyplývá jakási bezmocnost uchopit ho v rámci stávajícího právního řádu. Proto se na internet pohlíží jako na přenosové médium - umožňující využívání poskytovaných služeb.

Právní režim se řídí dvěma principy:

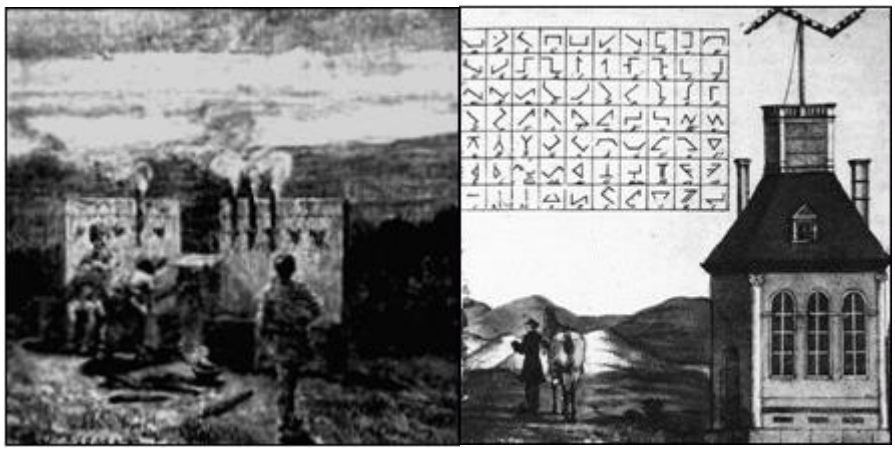
prioritní princip teritoriality, který uplatňuje právo země, kde je služba poskytována (sídlo poskytovatele služeb, příp. umístění serveru),

sekundární princip práva upravující druh činnosti, která je takto realizována, bez ohledu na médium (obchodní, občanský zákoník, autorský zákon apod.). Charakter internetového prostředí (globální, bez časových a prostorových hranic, anonymní aj.) však tuto situaci velmi komplikuje.

Vcelku zásadní problém, který nastává při odhalování elektronické informační kriminality, představuje sběr důkazních prostředků, které by mohly sloužit k usvědčení pachatele. Digitální důkazy jsou totiž nehmotné a přechodné povahy. Situace je komplikována snahou pachatelů zahlazovat po sobě veškeré stopy.[7]

1.3 Historie internetu

Snaha o dálkový a co nejrychlejší přenos informací doprovází celé dějiny lidstva. Stačí připomenout signalizaci ohněm, kouřem, světlem či zvukem, systém šíření zpráv pomocí běžců v Incké říši v Peru, Chappeův optický telegraf, Morseův telegraf či telefon Grahama Bella. [34]



Obr. 1. Předchůdci Internetu: Signalizace ohněm, Optický telegraf [34]

Historie se zmiňuje o dvou hlavních příčinách vzniku Internetu. První byla snaha uživatelů sdílet navzájem své počítače. Druhá se stala legendou. Po vypuštění první vesmírné družice Země – Sputnik, tehdejším sovětským svazem v roce 1956, zavládlo v armádě Spojených států zděšení. Sovětům se podařil husarský kousek a zdálo se, že ve vědecko-technickém výzkumu a vývoji jdou dopředu mnohem rychleji než Američané. Ve snaze dohnat tento náskok vznikla v roce 1957 speciální vládní agentura nazvaná APRA (Úřad pro pokročilé výzkumné projekty – Advanced Research Projects Agency), zaměřená na podporu nejmodernějšího vývoje a výzkumu. Jedním z problémů, které měly být vyřešeny v rámci jejích projektů, byl problém komunikace mezi jednotlivými velitelskými stanovišti armády a civilní správy v případě sovětského jaderného útoku. V takovém případě by zcela selhal tehdejší způsob komunikace. Telefonní vedení by byla zničena a nebylo by možné vzájemně koordinovat činnost. Proto vznikl projekt počítačové sítě, prostřednictvím které by se dalo komunikovat, i kdyby některé její části byly zničeny, a která by neměla jeden hlavní bod, neboť takový bod by se stal zákonitě hlavním terčem případného útoku (decentralizovaná síť). [1]

Průkopník této myšlenky byl Bob Taylor, který s myšlenkou sítě přišel již v roce 1966. Na tomto základě Američané začali budovat síť s názvem ARPANET. V roce 1969 byly připojeny 4 počítače, v roce 1972 jich bylo 23, v roce 1984 přes 1000. V dnešní době se již bavíme o miliardách počítačů, přesný počet není možno spočítat. [44]

1.3.1 Internet v ČR

Internet nebyl úplně první světovou sítí, která se k nám dostala po sametové revoluci. Prvními byly sítě FIDO a EUNET, vystačily s komutovaným spojením přes veřejnou telefonní síť. Další v pořadí byla síť EARN/Bitnet, která již vyžadovala pevné propojení pevnou linkou. Teprve po ní přišel Internet.[30]

EARN

V říjnu roku 1990 se k nám dostává i evropská odnož sítě Bitnet, tj. síť EARN (European Academic and Research Network). Protože síť EARN poskytovala pouze služby dávkového charakteru (zejména elektronickou poštu a přenos souborů), vystačila i s relativně pomalými pevnými okruhy. Prvním uzlem této sítě u nás (národním uzlem sítě

EARN) se stal střediskový počítač IBM 4381 na Oblastním výpočetním centru (OVC) ČVUT Praha (nyní VC ČVUT). Uzel CSEARN byl připojen na rakouský národní uzel sítě EARN v Linzi linkou o přenosové rychlosti 9600 bps.

Myšlenkou bylo vybudování celostátní páteřní sítě, která by všem tuzemských akademickým střediskům umožnila připojení na Internet, který by pak dále rozváděly navazující metropolitní sítě.

Federální orgány ČSR se stavěly k tomuto záměru negativně, a tak byly podány návrhy na vybudování dvou národních páteřních sítí jednotlivým ministerstvům školství. Potřebné propojení z Brna do Bratislavy bylo součástí českého projektu za přispění slovenské strany.

V prosinci 1991 byl podán příslušný návrh českému ministerstvu školství, které v červnu 1992 po jeho schválení uvolnilo 20 milionu korun a budování akademické páteřní sítě mohlo začít.

CESNET

Síť CESNET je považována za oficiální připojení na Internet. Český projekt dostal jmeno FESNET (Federal Educational and Scientific NETwork), starší označení FERNET (Federal Educational and Research NETwork) bylo zamítnuto. V roce 1992 se z původniho projektu FESNETu stal CESNET (Czech Educational and Scientific Network), zatímco na Slovensku se začal realizovat projekt sítě SANET (Slovak Academic Network).

Samotný CESNET realizoval původní myšlenku: zajišťoval přívod Internetu do jednotlivých akademických středisek, ale ne "rozvod" Internetu v rámci příslušných měst. Toto bylo řešeno navazujícími projekty metropolitních sítí, které po technické stránce samozřejmě velmi úzce navazovaly na CESNET, ale z hlediska financování byly samostatnými projekty.

V listopadu 1991 se u nás do evropského internetu připojují první univerzity - začátek historie internetu v České republice. Nejdříve šlo pouze o komutované napojení z Prahy (konkrétně z VC ČVUT) na uzel Internetu v rakouském Linzi. Později bylo připojení po pevné lince „uměle“ rozpůleno tak, aby jedna její polovina přenášela provoz v rámci sítě EARN, a druhá provoz Internetu. 13. února 1992 pak na ČVUT Praha dochází ke

slavnostnímu aktu formalního připojení Československa k Internetu, mj. i za účasti představitelů agentury NSF.[12]

1.4 Výhody a nevýhody internetu

1.4.1 Výhody

- Rychlý přístup k informacím.
- Možnost získat všechny informace o tom co lidstvo kdy objevilo a na čem pracovalo.
- Elektronický obchod.
- Elektronické bankovnictví.
- Možnost elektronické komunikace.

1.4.2 Nevýhody

- Viry.
- Zneužívání osobních údajů.
- Internetový terorismus.
- Počítačová špionáž.
- 95 % internetu je v angličtině. [11]

2 POČÍTAČOVÁ KRIMINALITA

Termínem počítačová kriminalita (též kybernetická kriminalita či kybernalita) se označují trestné činy zaměřené proti počítačům nebo trestné činy páchané pomocí počítače. Jde o nelegální, nemorální a neoprávněné konání, které zahrnuje zneužití údajů získaných prostřednictvím výpočetní techniky nebo jejich změnu. Počítače v podstatě neumožňují páchat nový typ trestné činnosti, jen poskytují novou technologii a nové způsoby pro páchání už známých trestných činů jako je sabotáž, krádež, zneužití, neoprávněné užití cizí věci, vydírání nebo špionáž. [32]

Trestné činy zaměřené proti počítačům (počítač je předmětem trestného činu) :

- úmyslné útoky proti vlastnímu nosiči informace, případně i datům v něm uložených s úmyslem je zničit. [31]

Trestné činy páchané pomocí počítače (počítač je nástrojem pro páchání trestného činu):

- trestné činy porušující soukromí,
- trestné činy se vztahem k obsahu počítače,
- trestné činy ekonomické,
- jednání porušující autorská práva,
- další např. Phishing, Pharming,…

Počítačová kriminalita dnes a kdysi je značně odlišná. Rozvojem výpočetní techniky, provozováním databází, užíváním počítačových sítí, včetně Internetu, vznikla obsáhlá škála možností páchání trestních činů. Počítač se stal běžným prostředkem v mnoha oborech lidské činnosti.

Znaky počítačové kriminality versus „klasické“ kriminality

- neobsahuje násilí, nepoužívá zbraně, nevzniká újma na zdraví,
- měří se na tisíciny vteřiny, pachatel nemusí být na místě páchání trestného činu,
- značné ztráty, ať už finanční nebo v podobě zneužití získaných dat,
- určitá diskrétnost trestného činu,
- vyznačuje se zpravidla hlubší znalostmi předmětnými i technickými z oblasti informačních technologií a počítačů = kriminalita „ bílých límečku“.

2.1 Počátky kriminality na Internetu

Existence velkého počtu izolovaných počítačů byla jedním z impulsů vedoucím k rozvoji počítačových sítí a k využití výpočetní techniky snad ve všech oblastech lidské činnosti.

Počítačová kriminalita v *šedesátých a sedmdesátých letech*. V těchto letech, v průběhu posledních čtyřiceti let došlo k významnému růstu i kvalitativnímu vývoji počítačové kriminality, ve světě i u nás. Sběr údajů o zneužití počítačů zajišťoval v USA již od roku 1958 *Stanford Research Institute (SRI)*.

V té době byly údaje rozděleny do čtyř kategorií na:

- vandalismus, namířený proti počítačovému hardware,
- krádež majetku nebo informací,
- podvod uskutečněný pomocí počítače nebo krádež peněz,
- nepřípustné použití počítače nebo krádež a prodej počítačového času.

Zaznamenaná data nebyla významná až do roku 1968, kdy bylo podchyceno 13 případů. V roce 1977 dosáhl počet zaznamenaných případů již 85. Statistiku vedl *SRI* do roku 1978.

Počítačová kriminalita v *osmdesátých letech*. Kromě podvodů a fyzických škod dochází ke krádežím databází, šíření virů, infiltraci logických a časových bomb, k rozšiřování a využívání pirátského softwaru. Krádež softwaru nelegálním kopírováním se postupně stává nejobecnějším a nejdražším typem počítačového zločinu.

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

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

Devadesátá léta přinášejí s celosvětovým rozvojem Internetu i jeho zneužití k šíření pornografie, rasismu, propagaci výbušnin a drog, k prezentaci extremistů a kriminálních živlů. Mezi útočníky, jejichž cílem jsou informace uchovávané na počítačích, patří vedle

profesionálních hackerů též zpravodajské služby, detektivní kanceláře, média, aktéři organizovaného zločinu i političtí extrémisté. [33]

2.2 Projevy počítačové kriminality (trestné činy na internetu)

2.2.1 Nebezpečné komunikační jevy

Spam

Bezesporu každý uživatel internetu má zkušenosti s nevyžádanou poštou, která někdy doslova zaplavuje jeho e-mailovou schránku. Pro nevyžádanou poštu se používají označení spam. Provozovat spamming znamená zaplavovat internet mnoha exempláři jedné a téže zprávy ve snaze vnutit ji lidem, kteří by jinak takovouto zprávu přijmout vůbec nechtěli. Většina spamů jsou obchodně zaměřené nabídky, často jde o nabídky pochybných produktů, postupů na rychlé zbohatnutí či o nabídky pololegálních služeb. Od roku 2004 je v účinnosti zákon č. 480/2004 Sb., o některých službách informačních společností nebo také tzv. antispamový zákon, který danou problematiku upravuje. [43]

Název spam

Název spam pochází z angličtiny a o jeho zásluhu se postaral seriál Monty Pythonův létající cirkus. Spam označuje v angličtině značku amerických konzerv studeného masa, něco jako lančmítu (překlad haše v televizních titulcích je nepřesný), která se vyrábí od 30. let dodnes (v současnosti ale výrobce trvá na psaní velkým písmem SPAM) a za 2. světové války a po ní byla hojně rozšířená a stále méně oblíbená ve Velké Británii. Proto se objevuje v závěrečném skeči 25. dílu seriálu Monty Pythonův létající cirkus.

Scénka se odehrává v restauraci, kde všechny položky jídelního lístku obsahují spam. Šunka a spam, vejce a spam, spam a spam... Spory zákazníků s číšnicí o objednávky přerušuje skupina Vikingů zpívajících Spam, spam, spam. Tato scénka se zřejmě divákům tak vryla do paměti, až se slovo SPAM stalo názvem pro něco nechtěného, nevyžádaného.[41]

Statistiky vypovídají o tom, že celosvětově je více než polovina odeslaných e-mailů spamem. Velké množství jednotlivců i organizací dnes už má se spamem řadu nepříjemných zkušeností. Kromě toho, že spam způsobuje uživatelům nemálo různých

potíží, nese s sebou také navyšování jejich nákladů (např. na systémovou kapacitu počítačů) nemluvě o tom, kolik času zabere jeho následné odstraňování. Spam někdy může být i příčinou poškození vašeho počítače, ale co je horší, v současnosti se stále častěji zneužívá k trestné činnosti. Spam bývá rovněž nositelem počítačových virů či jinak škodícího softwaru. [14]

Kouzlo spamu spočívá v minimálních nákladech. Ideální pro spamming jsou tyto informační kanály:

- e-mail,
- diskusní fóra a blogy,
- další komunikační služby (ICQ, Jabber, atd.).

Z uvedených kanálů je pro spamming nejrozšířenější e-mail, jelikož je také oblíbený u koncových uživatelů díky nízkým nákladům. Dále získat emailové adresy z nejrůznějších volně dostupných zdrojů je relativně jednoduché.

Z pohledu obsahu rozlišujeme tyto spamy:

- obchodní,
- kriminální (nebo jinak společensky nebezpečný),
- politický,
- náboženský. [36]

Ochrana proti spamu

- Zbytečně nesdělujte svoji e-mailovou adresu, tzn. sdělujte ji pouze těm, od nichž chcete, aby vám zprávy přicházely (přátelům, známým, obchodním a pracovním partnerům apod.).
- Mějte více e-mailových adres (na tzv. freemailovových serverech, jež tuto službu poskytují zdarma, např. Atlas, Seznam, Centrum apod.) s antivirovou a antispamovou ochranou.

- Pokud to není nutné, zbytečně svou e-mailovou adresu neumísťujte na webové stránky na internetu. Spameři mají k dispozici speciální vyhledávací programy, jež na internetu vyhledávají právě různé e-mailové adresy, na něž později posílají nevyžádanou poštu. E-mailovou adresu můžete také napsat v trochu pozměněném tvaru jako jméno.příjmení“zavináč“firma.cz a vyhledávací program nemá šanci.
- Pokud už vám dojde nějaká spamová zpráva, neodpovídejte na ni. Tím na sebe jenom upozorníte (že vaše e-mailová schránka je aktivní a používaná) a spam bude chodit o to častěji a více.
- Spamové zprávy neotvírejte. Platí opět podobné jako v předchozím bodě – říkáte tak, že vaše e-mailová adresa je aktivní.
- Pečlivě zvažte, jaké zprávy do svého PC přijímáte, jaké otevřete a čtete.
- Nabídek spamů v žádném případě nevyužívejte.
- Pokud už s něčím, co vám přišlo e-mailem, souhlasíte, činte tak po velice zralé úvaze. [19]

Antispamový zákon

Od roku 2004 je v účinnosti zákon č. 480/2004 Sb., o některých službách informační společnosti neboli také tzv. antispamový zákon.

Zákon reguluje nevyžádanou elektronickou inzerci a povoluje zasílání obchodního sdělení pouze podle takzvaného systému opt-in, tedy pouze s výslovným souhlasem adresáta. Nevyžádaná obchodní sdělení zákon zakazuje. Zákon tedy nezakazuje rozesílání spamu obecně, ale pouze rozesílání tzv. nevyžádaných obchodních sdělení. Nevyžádané obchodní sdělení je kategorie užší než obecná kategorie „spam“, protože spam samozřejmě může zahrnovat i e-maily, které s podnikáním nemají nic společného. Zákon definuje obchodní sdělení, jako všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem. Za obchodní sdělení považuje zákon též reklamu. Zákon dále vymezuje pojem obchodní sdělení i negativně, když stanoví, co se za obchodní sdělení nepovažuje. Za obchodní sdělení zákon nepovažuje údaje umožňující přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresu elektronické pošty. Jinými slovy, pokud podnikatel např. změnil telefonní číslo nebo e-mail a o tomto informuje své klienty nebo zákazníky prostřednictvím e-mailu, nebude se

jednat o obchodní sdělení a k rozesílání takového e-mailu nebude potřebovat souhlas adresátů. Dále zákon stanoví, že zasílání obchodního sdělení (tedy se souhlasem adresáta) ve formě e-mailu je zakázáno, pokud:

- takovéto sdělení není zřetelně a jasně označeno jako obchodní sdělení,
- skrývá nebo utajuje totožnost odesilatele, jehož jménem se komunikace uskutečňuje,
- nebo je zasláno bez platné adresy, na kterou je možno zaslat informaci o tom, že si adresát nepřeje, aby mu byla obchodní sdělení dále zasílána.

Hoax

Anglické slovo HOAX v překladu znamená: falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, výmysl, žert, kanadský žertík. [4]

Hoax je zjednodušeně řečeno nevyžádaná e-mailová zpráva, obsahující falešné varování - nejčastěji před počítačovým virem, ale nejenom před ním, obsah bývá různorodý. [5]

Často se lze setkat s hoaxy:

- které nabízejí zdarma určitou službu nebo zboží za podmínky, že e-mail pošlete určitému množství lidí,
- které jsou rozesílány jako řetězové dopisy štěstí nebo návody na rychlé zbohatnutí (pyramidové hry),
- falešné prosby o pomoc např. prosba o darování krve pro nemocného člověka,
- varování před smyšlenými viry a různými útoky na počítač,
- petice a výzvy.

Znaky hoaxu

- Varuje před blížícím se nebezpečím nebo přichází s nějakou exkluzivní zprávou, o které jste se z běžných zdrojů nemohli dozvědět.
- Ve většině případů se autor poplašné zprávy odkazuje na to, že varování přišlo od důvěryhodných zdrojů.

- Nejčastějším znakem HOAXu bývá výzva k dalšímu šíření této zprávy. Jako příklad můžeme uvést HOAX v ICQ: „Od 1. července má ICQ stát 50 Kč za měsíc, postav se proti tomu a pošli tento text alespoň 15 lidem z tvých kontaktů. Když to doděláš, stiskni tlačítko F1 a tvoje květinka bude modrá, to znamená, že nemusíš nic platit.“[8]

Jeden z nejčastěji rozesílaných hoaxů v ČR

Normálně takové nesmysly neposílám, ale tohle si pořádně přečtěte, je to finančně moc zajímavé. V normálním případě neposílám odkazy tohoto rázu, ale tento list přišel od jedné mojí velmi dobré přítelkyně, která je advokátka a vypadá to na zajímavou možnost. Když mi to ona poví, že to funguje, tak to funguje. Každopádně, člověk s tím nic neztratí. Povídala mi následující: Jsem právnička a znám právo. Je to fakt. Nenechávejte se přemluvit. AOL a Intel se drží při slibu kvůli jejich obavám ze soudů a z miliónových pohledávek, jako to udělala Pepsi Cola s General Electicom nedávno.
Milý příteli, nepovažujte toto za hloupý žert. Bill Gates teď rozdává svůj výrobek. Jakmile na toto nebudete ihned reagovat, můžete tento Mail smazat. Windows je ještě stále nejvíc používaný program. Microsoft a AOL Experimentují přes tento e-mailem poslaný text / email beta test/ Jakmile pošlete tento mail přátelům, tak Microsoft vás bude stopovat 2 týdny. Za každou osobu, která tento mail pošle, Microsoft platí 245 EUR za každou osobu. Komu jste poslali a kdo tento mail poslal dále, Microsoft platí 243 EUR. Za třetí osobu, která obdrží tento mail, dostane 241 EUR. Po 2 týdnech Microsoft Vám pošle list, ve kterém bude prosit o potvrzení Vaší poštovní adresy a pošle Vám šek.

S pozdravem
Charles S. Bailey General Manager Field Operations 1-800-842-2332
Ext. 1085 or 904/245-1085 or RNX 292-1085
mailto: Charles_Bailey@csx.com(mailto:Charles_Bailey@csx.com)

Text od Petry advokátky:
Já jsem toto považovala za podvod, ale 2 týdny potom, co jsem poslala tento mail dále, Microsoft se mě ptal na adresu a dostala jsem šek na 24800 EUR. Musíte odpovědět, než bude konec testu. Když se někomu nabídne taková možnost, musí se využít. Pro Billa Gatese tyto výdaje jsou jen jako výdaje na reklamu. Prosím, pošlete tento mail tolika

lidem, kolika to jen jde. Minimálně 1000 EUR dostat musíte. Ani my bychom nepomáhali v posílání mailu, kdyby to nebylo zajímavé. Jak jsem psala, znám právo a je pravda, že Intel a AOL se domlouvají o fúzi, aby se stali největším poskytovatelem služeb na světě, proto udělali tento test, aby si byli jistí, že zůstávají při nejpoužívanějším softwaru.

Kyberšikana

Cílem kyberšikany je někomu ublížit nebo ho zesměšnit za použití elektronických prostředků. Je to úmysl, nepřátelské chování, které se obvykle opakuje.

Jedná se o:

- hanlivé a urážlivé zprávy zasílané prostřednictvím SMS, MMS nebo internetu,
- zesměšňující nebo ponižující obrázky či videa posílané e-mailem nebo vyvěšené na webové stránce,
- webové stránky nebo blogy s cílem někoho zesměšnit,
- zesměšňování, vydírání, zastrašování, ubližování, ohrožování a obtěžování prostřednictvím komunitních sítí,
- zneužívání identity oběti rozesíláním obtěžujících a urážlivých zpráv pod jejím jménem, [25]
- pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit zachycenou osobu,
- obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním, [21]

Prostředky kyberšikany:

- textové zprávy,
- fotografie nebo videoklipy pořízené kamerou mobilních telefonů,
- mobilní telefonáty,
- e-maily,
- chatovací místnosti,
- instant messaging,
- sociální sítě. [37]

Typy kyberšikany

- Přímé útoky - hanlivé a urážlivé zprávy zasílané prostřednictvím SMS, MMS nebo internetu, kradení hesel a zneužití účtu, blogování, rozesílání zákeřných kódů (viry, spyware, hackování), internetové hlasování, zveřejňování choulostivých nebo lživých informací zejména záznam šikany, pornografické fotografie.
- Útoky v zastoupení - špinavou práci za agresora vykoná někdo druhý, často nevědomě se stává komplicem. Agresor krade heslo, nabourává se do účtu oběti, nebo si zakládá učet pod identitou oběti a pak se chová tak, aby oběť poškodil. [22]

Kyberšikana a zákon

Kyberšikana není v našem právním řádu vedená jako trestní čin, ale některé její projevy mohou být kvalifikovány jako jiné trestné činy či přestupky. V níže uvedené tabulce jsou tyto činy vypsány a k nim uvedené příslušné paragrafy a sazby odnětí svobody.

Tab. 1. Klasifikace kyberšikany na vybraných paragrafech trestního zákona [21]

Paragraf	Klasifikace kyberšikany na vybraných paragrafech	Sazba
§144	Účast na sebevraždě	až 12 let
§175	Vydírání	až 16 let
§180	Neoprávněné nakládání s osobními údaji	až 8 let
§181	Poškození cizích práv	až 5 let
§182	Porušení tajemství dopravovaných zpráv	až 10 let
§183	Porušení tajemství listin a jiných dokumentů uchovaných v soukromí	až 8 let
§184	Pomluva	až 2 roky
§191	Šíření pornografie	až 5 let
§192	Výroba a jiné nakládání s dětskou pornografií	až 8 let
§209	Podvod	až 10 let
§230	Neoprávněny přístup k počítačovému systému a nosiči informací	až 8 let
§231	Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	až 5 let
§232	Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	až 2 roky
§352	Násilí proti skupině obyvatelů a proti jednotlivci	až 3 roky
§353	Nebezpečné vyhrožování	až 3 roky
§354	Nebezpečné pronásledování	až 3 roky
§356	Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod	až 3 roky
§357	Šíření poplašné zprávy	až 8 let

Příklad

Žáci 7. A si založili stránku na sociální síti Spolužáci.cz. Téměř všichni žáci ze třídy si na stránce vytvořili svůj profil. Jedné z žákyň třídy, která nebyla mezi ostatními příliš oblíbená, ale neumožnili ke stránce přístup. Bylo to pro ni velmi ponižující. Navíc zjistila, že ji ostatní spolužáci na této stránce pomlouvají. [20]

Sexting

Termínem sexting označujeme elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem. Tyto materiály často vznikají mezi partnery, problém nastává po rozchodu, kdy jeden z partnerů tyto fotografie či videa zveřejní například na internetu nebo rozešle přes mobilní telefon.

První případ sextingu se vyskytl v roce 2005. V ČR se případy sextingu řeší individuálně, některé jsou vyhodnoceny jako přestupek, jiné jako trestný čin.

Trestné formy:

- § 205 TZ šíření a zpřístupňování – až 3 roky odnětí svobody, organizovaně 6 let, mezinárodně organizovaně 8 let,
- § 205a TZ přechovávání – až 2 roky odnětí svobody,
- § 205b TZ výroba – až 5 let, organizovaně 6 let, mezinárodně organizovaně 8 let.

Paradox v právním řádu v ČR říká, že osoby starší 15 let mohou mít sex, ale nesmí se u toho dokumentovat v podobě fotografií, videí nebo vedení deníku, v tomto případě by se jednalo o výrobu a držení dětské pornografie.

Kyberstalking

Kyberstalking je zneužívání internetu, mobilních telefonů či jiných informačních a komunikačních technologií ke stalkingu, tedy k pronásledování.

Stalking znamená v překladu pronásledování, opakované stupňované obtěžování, které může mít různou podobu a intenzitu.

Nejčastější projevy:

- opakované dlouhodobé pokusy kontaktování oběti (dopisy, e-maily, telefonáty, SMS zprávy, vzkazy na ICQ, zasíláním různých zásilek s dárky apod.),
- demonstrování moci a síly stalkera (výhrůžky),
- ničení majetku oběti (patří sem i zasílání počítačových virů),
- stalker označuje sám sebe za oběť,
- snaha poškodit reputaci oběti (stalker rozšiřuje o oběti nepravdivé informace v jejím okolí). [23]

Stalkeři:

- bývalý partner,
- uctívač (patří sem stalkeři celebrit) snaží se o navázání kontaktu s jimi obdivovanou osobou,
- neobratný milovník,
- ublížený pronásledovatel (pronásleduje z důvodů pomsty),
- sexuální útočník,
- poblouzněný milovník (je přesvědčený, že ho oběť miluje).

Příklad

Andrea a Silvie byly nejlepší kamarádky. Když si Silvie našla jinou nejlepší kamarádku a s Andreou už se nechtěla bavit, Andrea se rozhodla, že se jí pomstí. Koupila si novou SIM kartu a každý večer od 22:00 do 23:00 hodin Silvii prozváněla na mobilní telefon. Každých 5 minut... Noční telefony budily nejen Silvii, ale také její rodiče, kteří na ni za to byli hodně naštvaní. Mysleli si, že si Silvie s někým tajně v noci volá a že jim o tom lže. Silvie z toho měla velké problémy. Když to rodičům nakonec vysvětlila, snažili se prozvánění zarazit. Protože se jim ale nepodařilo zjistit skutečnou totožnost útočníka, Silvie nakonec musela požádat operátora, aby jí příchozí hovory z tohoto čísla zablokoval. [20]

Kybergrooming

Kybergrooming označuje jednání osoby, která se snaží pomocí chatu, SMS zpráv, ICQ atd. zmanipulovat svoji oběť a donutit jí k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití, fyzické mučení, nucení k terorismu atd.

Etapy kybergroomingu

- Vzbuzení důvěry (získání pozice dobrého kamaráda) a snaha izolovat oběť (pomocí e-mailu, telefonního čísla, fotografie, kterou využije k vydírání).
- Podplácení dárky či službami, budování kamarádského vztahu, získání diskriminujících materiálů.
- Vyvolání emoční závislosti oběti na útočníkovi.
- Osobní setkání.
- Sexuální obtěžování, zneužití dítěte, patologická manipulace obětí (např. terorismus).

Charakteristika kybergroomera

- Je neobyčejně trpělivý.
- Komunikuje se svojí obětí několik měsíců, než se odhodlá sjednat si schůzku.
- Tváří se přátelsky.
- Zajímá se o rozvíjení vztahu s vámi.
- Bude se snažit udržet váš vztah v tajnosti.
- Bude hovořit o tom, že tento láskyplný vztah bude pokračovat v reálném světě, až se potkáte.
- Do konverzace vkládá témata sexuální povahy.
- Žádá o fotografie.
- Vyžaduje sex za použití web kamery a podobně.

Pomluva

Trestným činem pomluvy je jednání, kdy pachatel sdělí o jiném nepravdivý údaj, který je značnou měrou způsobilý ohrozit vážnost této osoby u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo mu způsobit jinou vážnou újmu. [46]

2.2.2 Extremistické projevy

Internet je obecně vzato prostorem, jehož základní výhodou je otevřenost, dostupnost informací a jejich sdílení, jakož i možnost projevovat či uplatňovat vlastní názory a myšlenky. V tomto kontextu lze konstatovat, že je internet jakýmsi ideálním prostorem pro realizaci svobody projevu, prostorem, v němž by se co nejméně měla uplatňovat cenzura či jakékoliv jiné omezování. Přesto, s ohledem na samotné vymezení svobody projevu jako jednoho ze základních mezinárodně garantovaných práv, má své meze – základní mezí je míra, jakou je svobodně uplatňovaným projevem zasahováno do lidských práv a právního postavení jiných osob nebo, v širším pojetí, jakým je narušován základní rámec hodnot, na nichž je založena demokratická společnost. [13]

K pojmu extremismus je celá řada definicí. Ministerstvo vnitra využívá ve své koncepční činnosti tuto pracovní definici:

Pojmem extremismus jsou označovány vyhraněné ideologické postoje, které vybočují z ústavních, zákonných norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku.

Mezi tyto principy patří:

- úcta k právům a svobodám člověka a občana (čl. 1 Ústavy),
- svrchovaný, jednotný a demokratický právní stát (čl 1 Ústavy),
- nezměnitelnost podstatných náležitostí demokratického právního státu (čl. 9 odst. 2 Ústavy),
- svrchovanost lidu (čl. 2 Ústavy),
- volná soutěž politických stran respektujících základní demokratické principy a odmítajících násilí jako prostředek k prosazování svých zájmů (čl. 5 Ústavy),
- ochrana menšin při rozhodování většiny (čl. 6 Ústavy),
- svoboda a rovnost lidí v důstojnosti a právech, nezadatelnost, nezcizitelnost, nepromlčitelnost a nezrušitelnost základních práv a svobod bez rozdílu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického nebo jiného smýšlení, národního a sociálního původu, příslušnosti k národnosti nebo etnické menšině, majetku, rodu nebo jiného postavení (čl. 1, čl. 3 Listiny základních práv a svobod). [3]

V praxi se může jednat především o následující trestné činy:

- obecné ohrožení,
- násilí proti skupině obyvatel a proti jednotlivci,
- hanobení národa, rasy a přesvědčení,
- podněcování k národnostní a rasové nenávisti,
- výtržnictví,
- vražda,
- ublížení na zdraví,
- omezování osobní svobody,
- vydírání,
- omezování svobody vyznání,
- porušování domovní svobody,
- porušování svobody sdružování a shromažďování,
- poškozování cizí věci,
- genocidium,
- podpora a propagace hnutí směřujících k potlačení práv a svobod člověka,
- persekuce obyvatelstva. [3]

Rozdělení extremismu

Extremismus je dělen na politický (levicový a pravicový), náboženský, ekologický a národností

2.2.3 Zneužívání obchodních a platebních styků

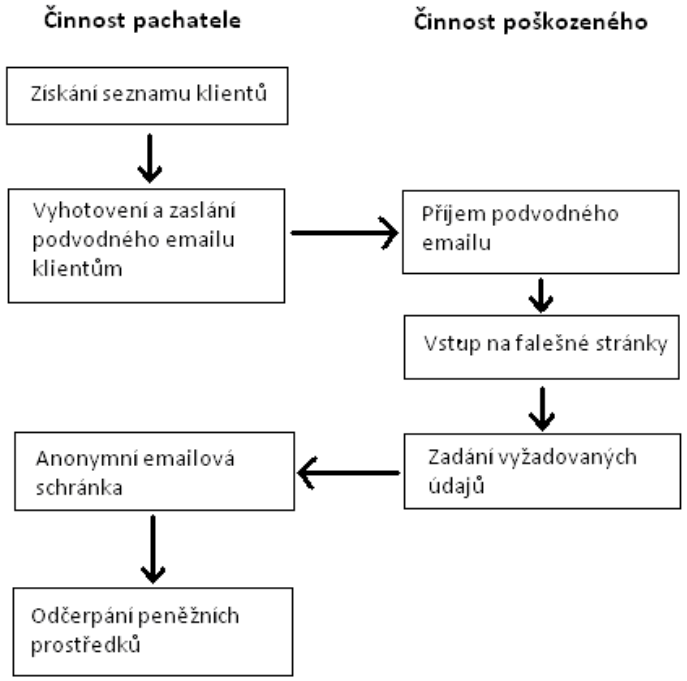
V ČR připadá čtvrtina veškeré hospodářské kriminality na neoprávněné držení platební karty. Odcizení identity na internetu je jednou z nejrychleji rostoucí kriminalitou.

Podvody lze páchat i bez přítomnosti platební karty, pokud víme patřičné údaje. Tyto údaje nám posléze slouží nejčastěji k nákupu na internetu. Jedná se o číslo platební karty, datum její expirace a CVV2/CVC2 kódu.

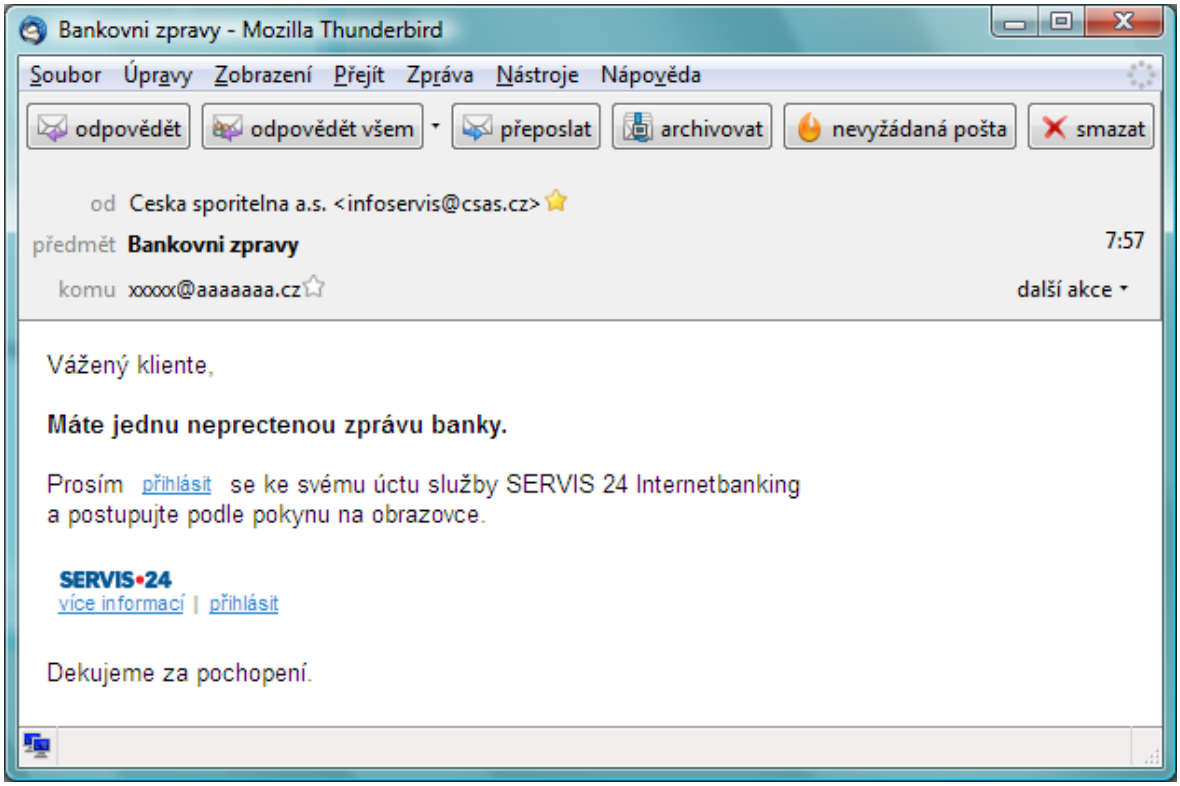
Phishing

V České Republice se vyskytuje od roku 2004. Vznikl přepisem anglického slova fishing (rybaření). Typickým příznakem této kriminality není využívání technických slabin, ale výhradně slabin lidských, plynoucích z neznalosti a nedbalosti člověka. [35] Známý také jako carving nebo brand spoofing. Phishing je podvod a padělání a lze ho definovat jako činnost, kdy je uživateli zaslán padělaný e-mail, který se klamavým způsobem staví do té pozice, že byl odeslán skutečnou finanční institucí ve snaze oklamat příjemce e-mailu tak, aby sdělil své soukromé informace typu čísla platební karty nebo bankovního účtu.[24]

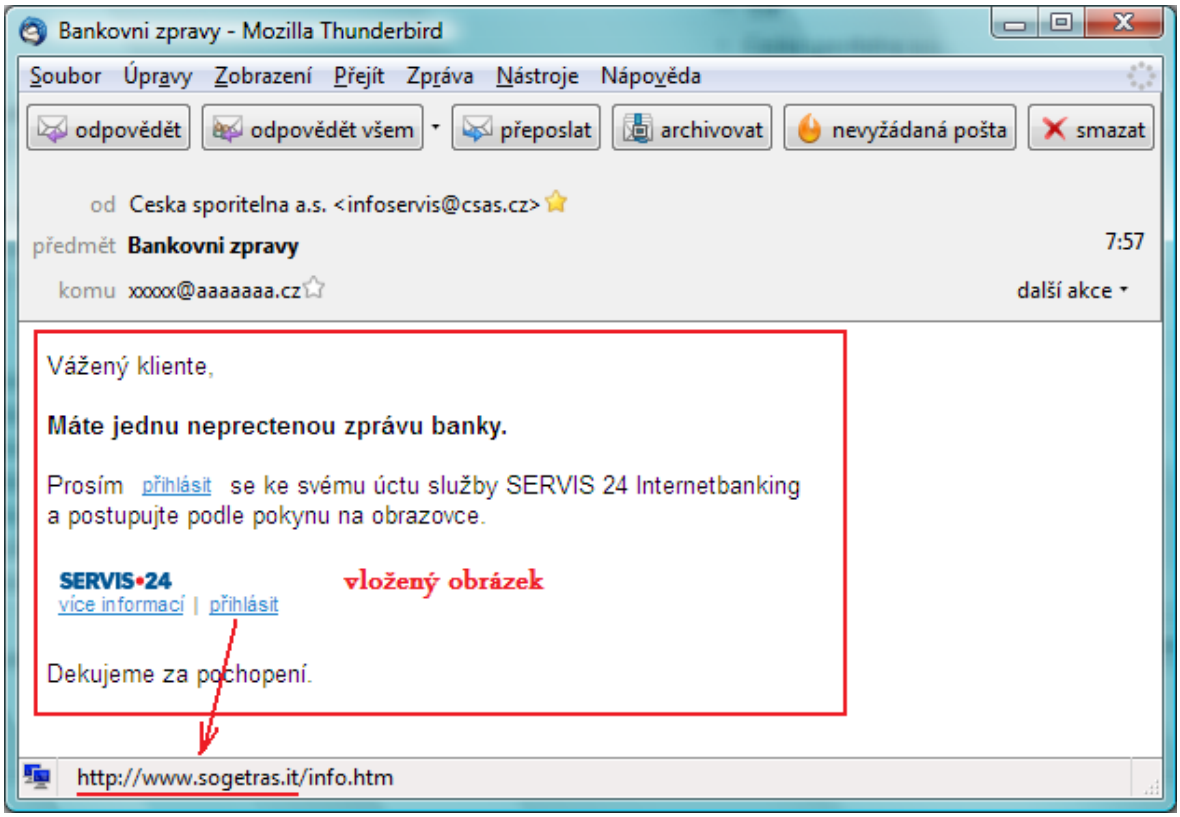
Základním znakem Phishingu je, že se graficky i podobou e-mailu tváří jako e-mail organizace. V textu zprávy se objevuje link, který má přesměrovat na stránky např. banky, ale ve skutečnosti odkazuje na jiné místo. Tyto stránky budí důvěryhodnost také díky své podobnosti s oficiálními stránkami banky, ale banky nikdy podobné e-maily nerozesílají, nemají důvod požadovat heslo, přihlašovací údaje či údaje o kartě.



Obr. 2. Průběh phishingového útoku [18]



Obr. 3. Ukázka phishingového útoku [24]



Obr. 4. Ukázka phishingového útoku [24]

Obr. 5. Ukázka phishingového útoku [24]

Pharming

Pharming je mladší a nebezpečnější verzí phishingu, kdy nemusí dojít k odhalení ani zkušeným uživatelem. I zde dochází k podvržení falešné stránky, která vypadá, jakoby pocházela z bankovního úřadu, ale navíc se na ni můžete dostat i při správném zadání regulérní internetové adresy banky v prohlížeči. Vy jednoduše vyťukáte adresu vaší banky s tím, že prostřednictvím internetového bankovnictví budete chtít provádět nějaké operace, a nic netušíc se však dostanete na podvržené stránky. Ty navíc vypadají naprosto stejně. [11]

2.2.4 Porušování autorských práv

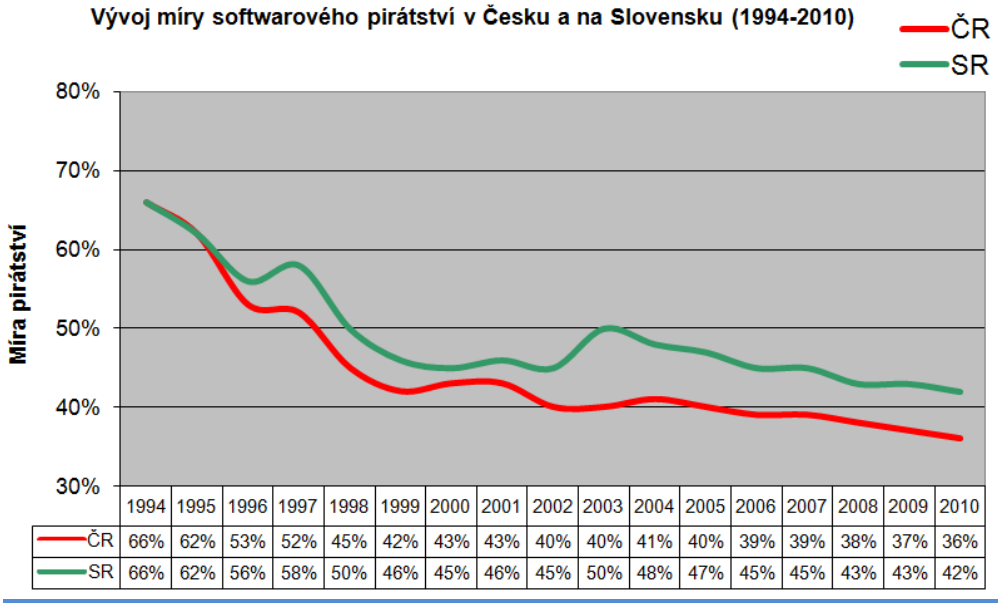
Pirátství a padělatelství bylo známé už mnoho let před objevením počítačů, kdy v dobách středověku dostávali králové padělky maleb od druhořadých malířů na místo originálů. Když na konci sedmdesátých let 20. století vstoupily na trh osobní počítače, neplatil ještě zákon o autorských právech z roku 1980, tehdy nebyl ještě software duševním vlastnictvím. Nejedná se ale pouze o nelegální software.

Stále více se objevují případy porušování autorských práv, nejvíce se jedná o šíření hudby a filmů na internetu. Užití díla či jiného předmětu ochrany podle práv souvisejících s právem autorským bez souhlasu vykonavatelů práv k nim je porušením práva autorského resp. práv souvisejících s právem autorským a zakládá občanskoprávní i trestněprávní resp. přestupkovou či správní odpovědnost. Kdo svévolně, tedy bez souhlasu nositelů autorských práv a práv souvisejících s právem autorským, užívá předmět ochrany podle těchto práv, dopouští se neoprávněného zásahu do autorského práva a práv souvisejících s právem autorským a měl by si být vědom nepříznivých důsledků, které pro něho z jeho jednání vyplývají.

Co mohou žádat jako nápravu:

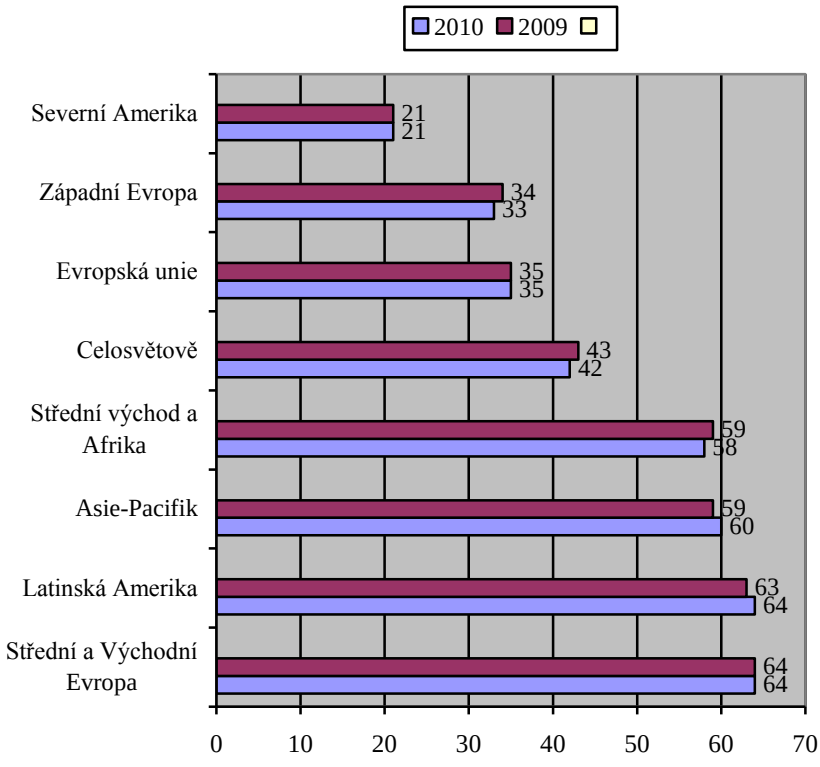
- aby se protiprávního jednání zdržel a závadný stav napravil,
- dále pak mohou žádat vydání bezdůvodného obohacení, a to ve výši dvojnásobku odměny, která byla na získání příslušné licence k užití obvyklá v době neoprávněného nakládání s předmětem ochrany,
- poskytnutí přiměřeného zadostiučinění a to i finančního. [16]

Na obrázcích níže je uvedena míra softwarového pirátství v Česku a na Slovensku v letech 1994 – 2010 a procentní vyjádření podílu softwarového pirátství v regionech.



	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
ČR	66%	62%	53%	52%	45%	42%	43%	43%	40%	40%	41%	40%	39%	39%	38%	37%	36%
SR	66%	62%	56%	58%	50%	46%	45%	46%	45%	50%	48%	47%	45%	45%	43%	43%	42%

Obr. 6. Vývoj míry softwarového pirátství [40]



Obr. 7. Procentní vyjádření podílu softwarového pirátství v regionech [29]

2.2.5 Dětská pornografie

Dětská pornografie je druhem pornografie, v níž jsou zobrazeny dítě či děti jako sexuální aktéři nebo objekty.

Definice pornografie ani dětské pornografie není obecně ustálená ani jednotná a obvykle se přizpůsobuje represivním potřebám státu.

Obvykle se za dětskou pornografii považuje:

- zobrazení soulože, masturbace nebo podobných aktivit, jichž se účastní dítě nebo děti,
- zobrazení dětských genitálií nebo dětské nahoty pořízené nebo používané za účelem sexuálního vzrušení nebo uspokojení. [6]

Základní rozdělení dětské pornografie

1. Obrazová pornografie

Ta představuje zobrazení dítěte při výslovně sexuální činnosti, skutečné nebo simulované nebo oplzlé vystavování pohlavních orgánů pro sexuální uspokojení uživatele; zahrnuje výrobu, rozšiřování anebo používání takového materiálu.

2. Zvuková pornografie

Ta představuje používání jakýchkoli zvukových prostředků užívajících dětský hlas, skutečný či simulovaný za účelem sexuálního uspokojení uživatele; též zahrnuje výrobu, rozšiřování anebo používání takového materiálu.

Legislativní rámec

§ 205 Šíření pornografie

(1) Kdo pornografické dílo písemné, fotografické, filmové, počítačové, elektronické nebo jiné takové dílo

a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo

b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří

fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo,

a) které zobrazuje nebo jinak využívá dítě,

b) v němž se zobrazuje násilí či neúcta k člověku, nebo

c) které zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem,

anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny,

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 205a Přechovávání dětské pornografie

Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, bude potrestán odnětím svobody až na dva roky.

§ 205b Zneužití dítěte k výrobě pornografie

(1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém

díle, bude potrestán odnětím svobody na jeden rok až pět let.

(2) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny, nebo

b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu. [46]

2.3 Netiketa

2.3.1 Co je netiketa

Slovo netiketa vzniklo spojením slov net (síť, zkráceně internet) a etiketa, což je nepsaný souhrn normy lidského chování. Původní text Netiquette vznikl někdy v osmdesátých letech v prostředí univerzity v Berkeley. Netiketa shrnuje zásady slušného chování v prostředí internetu a přidává zásady pro toto prostředí specifické. [27]

2.3.2 Pravidla

1. Chovejte se k druhým, tak, jak chcete, aby se oni chovali k vám - úplně nejzákladnější pravidlo mezilidských vztahů. Posíláte-li někomu zprávu, přečtěte si ji - a řekněte si: "Jak by mi bylo na jeho místě?". Toto pravidlo nechrání dokonale (pokud se vy a dotyčný více lišíte, nebo je vaše schopnost empatie malá), ale učí se již v mateřských školách.
2. Nespěchejte, myslete.
3. Nespěchejte, vychladněte - dostali jste ofenzivní mail (případně příspěvek v diskuzi) a jste rozzuřeni? Neměli by jste psát odpověď. Počkejte hodinku dvě, a pak se ještě jednou zamyslete - opravdu to dotyčný myslel tak zle? Nevyplývá to jenom z nepochopení? Nechce pouze provokovat?

4. Někdy je lepší soukromí - pokud s někým potřebujete vyřešit například jeho problematický příspěvek, aniž by to nějak souviselo s diskuzí, použijte osobní zprávy, případně mail,...
5. Nespěchejte, čtěte - pročtěte si pravidla fóra před tím, než začnete přispívat, neřkuli založíte nové vlákno! Taktéž prostudujte FAQ - často kladené otázky. Myslete na ty, kteří diskusi sledují a každý den se jim tam objeví ta samá často kladená otázka.
6. Nemějte tajnou identitu - zdá se vám snadné vydávat se za to (osobnost), čím nejste? Nedělejte to. Internet není anonymní. Jste zjistitelní. Nelžete o své identitě. Samozřejmě, proboha, chraňte si soukromí. Jenom nelžete a používejte ve styku s lidmi pouze jeden charakter (váš originální, který vám dala matka příroda).
7. Nekraďte identitu - opravdu, nevydávejte se za někoho jiného. I kdyby dotyčný měl jakkoliv uhodnutelné heslo, raději mu pošlete soukromou zprávu. Vydávat se za někoho jiného je velice vážný přestupek proti netiketě, na většině serverů trestaný zablokováním vaší IP adresy.
8. Nespamujte - SPAM je v jistém významu i zpráva nesouvisející s diskusí (off-topic). Horší je ovšem spam kterým něco propagujete (nejoblíbenější formou na internetu je odkaz, neboli hyperlink) - stále za předpokladu, že to nesouvisí s diskuzí. Posoudit co je a co není spam je občas docela těžké - ale pamatujte, že na netu jsou i, v tomto směru, dosti paranoidní uživatelé - dejte si pozor na nedorozumění.
9. Nerozesílejte řetězcové zprávy - Tyto zprávy v polovině případů člověku vyhrožují (co mu provedou, když je nerozešle), v druhé polovině případů obsahují poplašnou (nepravdivou) zprávu. Garantují vám, že jejich přeposláním prospíváte informovanosti, zdravotnímu stavu, nebo sexuální potenci vašich přátel. Není tomu tak. HOAXování vás může stát vaše kamarády, nebo prestiž.
10. Nedůvěřujte (nebo alespoň prověřujte) - na internetu je strašně moc lidí. Občas se vyskytnou i podvodníci, snažící se na vás vylákat peníze/číslo kreditní karty/jiné osobní údaje. Nedůvěřujte! Těmto praktikám se říká phising. Jak to funguje? Přijde vám mail, který se tváří jako z důvěryhodného zdroje, například z vaší banky. V mailu je odkaz na webový formulář na stránku, taktéž tvářící se důvěryhodně, kde máte vyplnit vaše uživatelské jméno a heslo, případně číslo karty, nebo jiné údaje o které jde. Vy si myslíte, jak jste své bance krásně pomohli opravením svých údajů, nebo co je záminkou a zatím se vaše peníze přelévají na konto phishera. Zlaté

pravidlo: NIKDO se vás na citlivé údaje neptá mailem. Respektive vás takto neodkazuje. Pokud se vám zdá, že by *přece jen* mohlo jít o pravdivý dopis, informujte se přímo u té organizace. Rozhodně neklikejte na linky v nedůvěryhodných mailech.

11. Nedůvěřujte (část 2) - Některým lidem nejde o vaše citlivé údaje. Třeba si chtějí udělat jenom srandu. Nebo jsou to nebezpeční psychopati. Každopádně, cizím lidem se nesvěřuje a bezhlavě se jim nedůvěřuje. Extrémně nebezpečné je to, samozřejmě, u dětí, kterým je tato zásad vštěpována jako prakticky první seznámení se světem a internetem. Oprávněně. [27]

2.4 Orgány a instituce zabývající se počítačovou kriminalitou

Počítačová kriminalita není v ČR ani v celosvětovém měřítku tabu a je prezentována jako jedna z největších hrozeb současnosti i budoucnosti. Organizace, zabývající se touto problematikou se snaží tuto činnost ze všech částí dokumentovat, provádět statistiky, průzkumy, dotazníky a pomocí výsledků tuto kriminalitu minimalizovat na základě doporučení institucím, ve kterých se počítačová kriminalita vyskytuje, ale i samotným uživatelům.

BSA (Business Software Alliance)

Je sdružení firem působící ve více než 80 zemích světa, prosazující zájmy softwarového průmyslu. Mezi členy BSA patří například Adobe Systems, Autodesk, Cisco Systems, Dell, Hewlett-Packard, IBM, Microsoft. Veřejně známa je BSA zejména svými "protipirátskými" aktivitami, kampaněmi proti nelegálnímu používání počítačových programů.[2]

Aktivity související s Mezinárodní asociací internetových horkých linek

Přední světové finanční subjekty (bankovní a úvěrové instituce) a představitelé internetového průmyslu (provideři, poskytovatelé internetových služeb) se spojili s Mezinárodním střediskem pro pohřešované a zneužívané děti a jeho sesterskou organizací, Národním střediskem pro pohřešované a zneužívané děti, aby společně bojovali proti dětské pornografii. Cílem iniciativy je vymýtit dětskou pornografii. Koalice navázala spolupráci s Mezinárodní asociací internetových horkých linek (International Association of Internet Hotlines. Jejím výsledkem je kampaň, apelující na nejširší veřejnost v

konkrétních zemích. Na ”horké linky” INHOPE je možné hlásit informace o výskytu internetových stránek s dětskou pornografií. V České republice od 1. dubna 2007 existuje horká linka ve správě nevládní organizace Naše dítě, která se stala součástí sítě INHOPE od 25. října 2007. [26]

Projekt E-bezpečí

Projekt E-Bezpečí je celorepublikový projekt zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény. Projekt je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi. Projekt jako celek byl zahájen v roce 2008

Zaměřuje se na nebezpečné internetové fenomény, které ohrožují jako děti, tak i dospělé uživatele internetu.

Projekt E-Bezpečí se specializuje zejména na kyberšikanu a sexting (různé formy vydírání, vyhrožování, poškozování obětí s pomocí informačních a komunikačních technologií), kybergrooming (komunikace s neznámými uživateli internetu vedoucí k osobní schůzce), kyberstalking a stalking (nebezpečné pronásledování s použitím ICT), rizika sociálních sítí (zejména sítě Facebook), hoax a spam, zneužití osobních údajů v prostředí elektronických médií.

Saferinternet.cz

Saferinternet.cz je osvětový projekt, usilující o zvýšení povědomí o bezpečnějším užívání internetu. Podporuje vzdělávání a výzkum v této oblasti, a to zejména dětí, kterým ubližuje nevhodné a závadné chování na internetu. Poskytuje pomoc, působí proti šíření ilegálního, zejména pedofilního a extremistického obsahu na internetu. Jde o projekt Národního centra bezpečnějšího internetu, který je spolufinancovaný Evropskou komisí.

Národní centrum bezpečnějšího internetu je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE a mezinárodní sítě horkých linek INHOPE.

Cílem projektu je osvěta a snaha propagovat pozitivní obsah a zodpovědné chování na internetu. Projekt také poukazuje na nevhodný obsah pro různé skupiny uživatelů, na projevy ohrožujícího chování v online prostředí a poskytuje rady, jak se takovým případům vyhnout.[38]

Policie ČR

odbor informační kriminality úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky v čele s plk. Mgr. Karlem Kuchaříkem

Mimo již uvedené nelze nezmínit aktivity společností jako je Microsoft, Siemens, Intel, kteří dávají nemalé finanční prostředky na tvorbu vlastních aktivit proti zneužívání jejich programů, ale také se účastní různých akcí, na kterých podporují boj s touto kriminalitou.

.

II. PRAKTICKÁ ČÁST

3 VÝVOJ POČÍTAČOVÉ KRIMINALITY V ČR

Informačními zdroji pro následné zpracování statistik v této kapitole byly orgány činné v trestním řízení (Policie ČR, soudy), Český statistický úřad a Ministerstvo vnitra.
Je třeba zdůraznit, že se zde uvádějí „surová“ data, které nelze považovat za odraz skutečného rozsahu počítačové kriminality v ČR. Uvádějí pouze kolik takových trestných činů bylo zjištěno.

Počet případů informační kriminality na území Zlínského kraje

Informace pro zpracování tab. 2. a 3. poskytlo Obvodní oddělení Policie ČR v Uherském Hradišti.

Tab. 2. Počet případů informační kriminality na území Zlínského kraje

	Zlínský kraj		**Okres Uherské Hradiště**	
	Trestný čin	**Přestupek**	**Trestný čin**	**Přestupek**
2010	137	119	40	35
Polovina roku 2011	58	62	15	35

Uvedená tabulka vypovídá o páchání informační kriminality na území Zlínského kraje a na jednom z jeho okresů Uherského Hradiště. Trestným činem je spáchaný čin, který přesáhl škodu 5000 Kč,-

Tab. 3. Počet policistů pracujících na oddělení informační kriminality ve Zlínském kraji

Okres	**Počet policistů**
Kroměříž	1
Zlín	1
Uherské Hradiště	1
Vsetín	1

3.1 Porušování autorského práva

Země s nejvyšší mírou softwarového pirátství

Gruzie 93%, Zimbabwe 91%, Bangladéš, Moldavsko, Jemen 90%, Arménie 89%, Venezuela, Bělorusko, Libye, Ázerbájdžán 88%, Indonésie 87%, Ukrajina 86%

Země s nejnižší mírou softwarového pirátství

USA, Japonsko, Lucembursko 20%, Nový Zéland 22%, Austrálie, Rakousko 24%, Švédsko, Belgie, Finsko 25%, Švýcarsko, Dánsko 26%, Německo, Velká Británie 27%, Norsko 29%. Česká republika je na 12. místě spolu s Arabskými Emiráty s mírou softwarového pirátství ve výši 36%. [40]

Tabulky 4. až 9. byly zpracovány na základě materiálů získaných z oddělení Preventivního informačního odboru ČR.

3.1.1 Rok 2010

Tab. 4. Počet trestních činů v oblasti porušování autorského práva v roce 2010

Kraj	Zjištěno	Objasněno		Škody v tis. kč	
		počet	%	celkem	zajištěno
Praha	66	9	13,64	8137	0
Středočeský kraj	16	5	31,25	1770	0
jihočeský	23	13	56,52	1586	0
Plzeňský	35	28	80	2743	0
Ústecký	37	21	56,76	6489	0
Královehradecký	8	1	12,50	1120	0
Jihomoravský	47	27	57,45	1587	0
Moravskoslezský	29	11	37,93	2144	0
Olomoucký	309	298	96,44	5320	0
Zlínský	25	15	60	0	0
Vysočina	7	2	28,57	30	0
Pardubický	29	22	75,86	575	0
Liberecký	13	8	61,54	374	0
Karlovarský	6	4	66,67	575	0
ČR celkem	**650**	**464**	**71,38**	**37708**	**0**

3.1.2 Rok 2009

Tab. 5. Počet trestných činů v oblasti porušování autorského práva v roce 2009

Kraj	Zjištěno	Objasněno		Škody v tis. Kč	
		počet	%	celkem	zajištěno
Praha	43	11	25,58	38431	0
Středočeský	24	12	50	1498	0
Jihočeský	10	8	80	3520	0
Plzeňský	33	30	90,91	14425	0
Ústecký	60	35	58,33	3449	0
Královehradecký	16	7	43,75	532	0
Jihomoravský	47	26	55,32	1771	0
Moravskoslezský	43	14	32,56	19589	0
ČR celkem	**276**	**143**	**51,81**	**83215**	**0**

3.1.3 Rok 2008

Tab. 6. Počet trestných činů v oblasti porušování autorského práva v roce 2008

Kraj	Zjištěno	Objasněno		Škody v tis. Kč	
		počet	%	celkem	zajištěno
Praha	89	45	50,56	9780	0
Středočeský	46	16	34,78	640	0
Jihočeský	29	22	75,86	1516	0
Plzeňský	75	29	38,67	9996	0
Ústecký	89	35	39,33	5081	0
Královehradecký	41	22	53,66	740	0
Jihomoravský	44	25	56,82	2838	0
Moravskoslezský	46	22	47,83	2062	0
ČR celkem	**459**	**216**	**47,06**	**32653**	**0**

3.1.4 Rok 2007

Tab. 7. Počet trestných činů v oblasti porušování autorského práva v roce 2007

Kraj	Zjištěno	Objasněno		Škody v tis. Kč	
		počet	%	celkem	zajištěno
Praha	80	54	67,50	37924	0
Středočeský	41	17	41,46	816	0
Jihočeský	20	0	0	420	0
Plzeňský	42	35	83,33	5816	0
Ústecký	33	30	90,91	9146	0
Královehradecký	29	21	72,41	1123	0
Jihomoravský	120	39	32,50	6765	0
Moravskoslezský	97	22	22,68	2160	0
ČR celkem	**462**	**230**	**49,78**	**64214**	**0**

3.1.5 Rok 2006

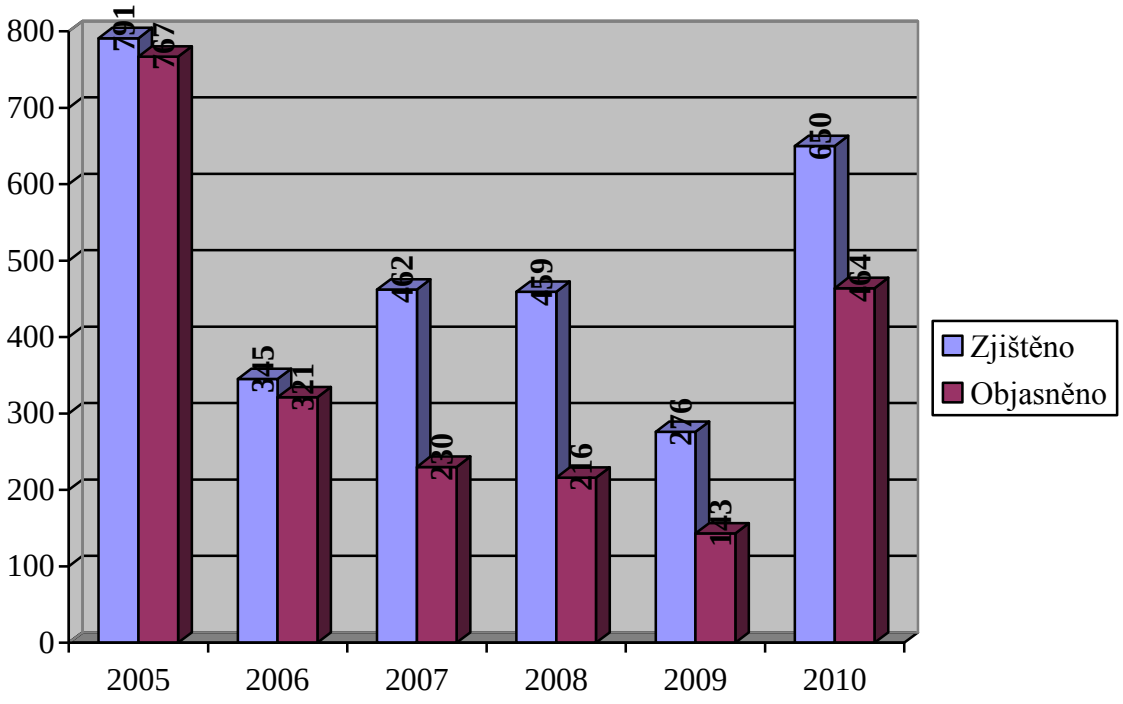
Tab. 8. Počet trestných činů v oblasti autorského práva v roce 2006

Kraj	Zjištěno	Objasněno		Škody v tis. Kč	
		počet	%	celkem	zajištěno
Praha	151	139	92,05	2288	0
Středočeský	28	27	96,43	1012	0
Jihočeský	17	17	100	212	0
Plzeňský	29	28	96,55	7485	0
Ústecký	46	42	91,30	6713	0
Královehradecký	13	12	92,31	198	0
Jihomoravský	50	49	98	178	0
Moravskoslezský	20	7	35	113	0
ČR celkem	**345**	**321**	**90,68**	**18198**	**0**

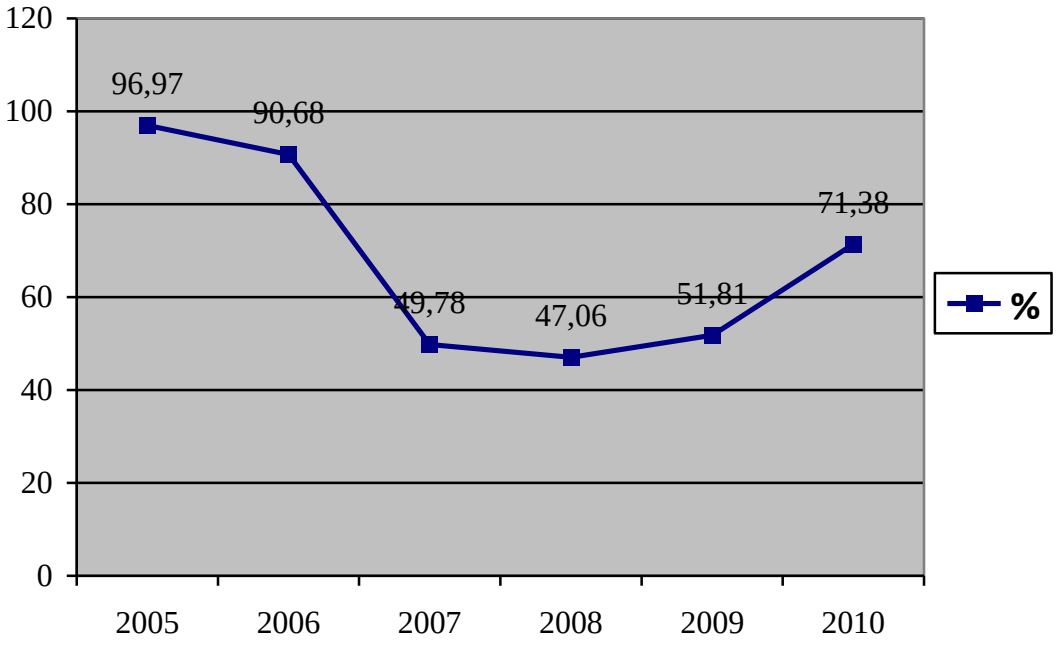
3.1.6 Rok 2005

Tab. 9. Počet trestných činů v oblasti autorského práva v roce 2005

Kraj	Zjištěno	Objasněno		Škody v tis. Kč	
		počet	%	celkem	zajištěno
Praha	483	475	98,34	9674	0
Středočeský	72	71	98,61	1901	0
Jihočeský	19	19	100	661	0
Plzeňský	45	42	93,33	6922	736
Ústecký	56	54	96,43	1744	0
Královehradecký	25	24	96	3866	0
Jihomoravský	72	70	97,22	647	0
Moravskoslezský	19	12	63,16	729	0
ČR celkem	**791**	**767**	**96,97**	**26144**	**736**



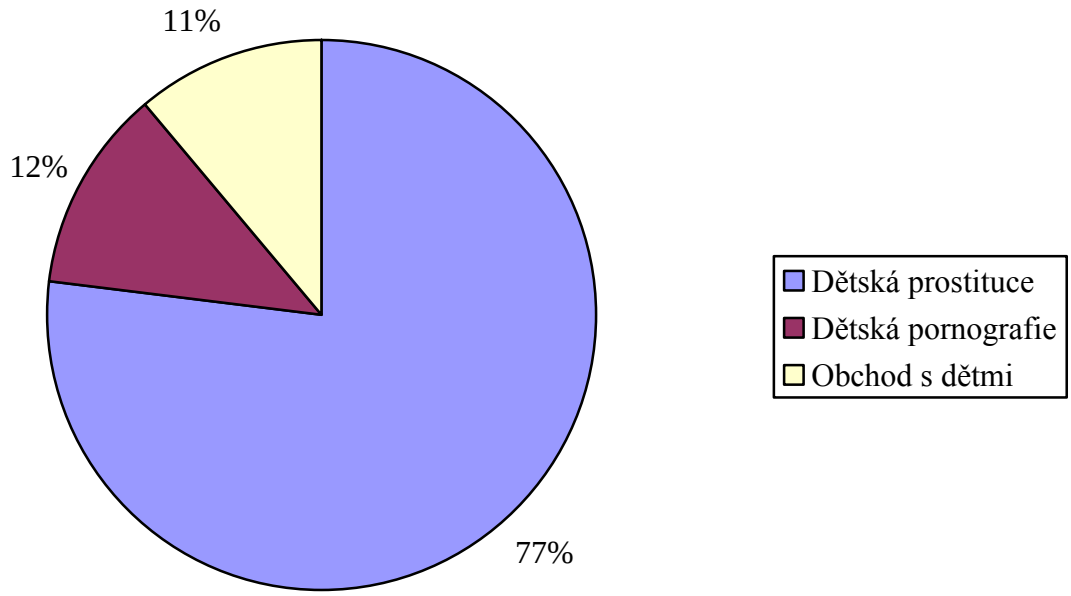
Obr. 8. Srovnání zjištěných a objasněných trestních činů v jednotlivých letech



Obr. 9. Vývoj objasněných případů v jednotlivých letech

3.2 Kriminální jednání související s dětskou pornografií [28]

Policie ČR získá největší množství poznatků od samotných uživatelů Internetu, kteří např. náhodně zjistí dětskou pornografii a tuto skutečnost oznámí. Je nutné také ocenit snahu samotných provozovatelů veřejných internetových portálů v České republice i v zahraničí při vyhledávání dětské pornografie, jejím odstraňování a jejich spolupráci s orgány činnými v trestním řízení. Další případy šíření dětské pornografie zjišťuje Policie ČR vlastním monitoringem Internetu nebo tyto poznatky obdrží od zahraničních policejních sborů (většinou prostřednictvím Interpolu).



Obr. 10. Podoby komerčního sexuálního zneužívání dětí v ČR [28]

3.2.1 Rok 2005

Tab. 10. Počet trestných činů a odsouzených v roce 2005 [28]

	Počet trestních činů	**Počet odsouzených osob**
Šíření pornografie zobrazující dítě	6	6
Přechovávání dětské pornografie	0	0
Zneužití dítěte k výrobě pornografie	0	0
Celkem	**6**	**6**

3.2.2 Rok 2006

Tab. 11. Počet trestných činů a odsouzených v roce 2011 [28]

	Počet trestních činů	Počet odsouzených osob
Šíření pornografie zobrazující dítě	8	8
Přechovávání dětské pornografie	0	0
Zneužití dítěte k výrobě pornografie	0	0
Celkem	**8**	**8**

3.2.3 Rok 2007

Tab. 12. Počet trestných činů a odsouzených v roce 2007 [28]

	Počet trestních činů	Počet odsouzených osob
Šíření pornografie zobrazující dítě	5	5
Přechovávání dětské pornografie	0	0
Zneužití dítěte k výrobě pornografie	0	0
Celkem	**5**	**5**

3.2.4 Rok 2008

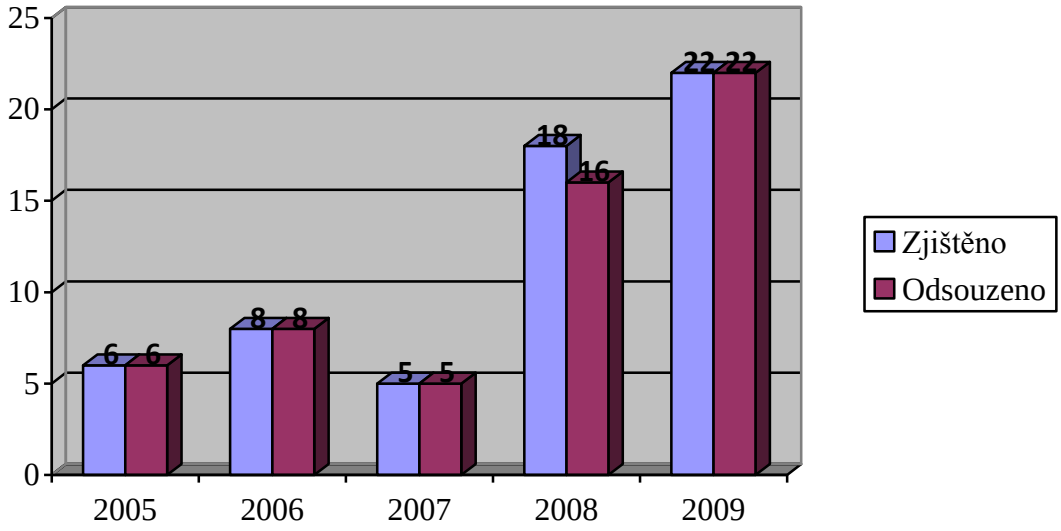
Tab. 13. Počet trestných činů a odsouzených v roce 2008 [28]

	Počet trestních činů	Počet odsouzených osob
Šíření pornografie zobrazující dítě	12	12
Přechovávání dětské pornografie	4	2
Zneužití dítěte k výrobě pornografie	2	2
Celkem	**18**	**16**

3.2.5 Rok 2009

Tab. 14. Počet trestných činů a odsouzených v roce 2009 [28]

	Počet trestních činů	Počet odsouzených osob
Šíření pornografie zobrazující dítě	9	9
Přechovávání dětské pornografie	11	11
Zneužití dítěte k výrobě pornografie	2	2
Celkem	**22**	**22**



Obr. 11. Počet zjištěných a odsouzených trestných činů v jednotlivých letech [28]

3.3 Extremismus

Problematiky extremismu patří mezi významné priority vlády ČR a Ministerstva vnitra. V roce 2009 existovaly na pravicově extrémistické scéně v České republice neregistrovaná uskupení, občanská sdružení a politické strany. Byly to Národní odpor (NO), Autonomní nacionalisté (AN), Občanská sdružení vlastenecká fronta (VF) a Dělnická mládež (DM) a politické strany Národní sjednocení (NSJ), Národní strana (NS) a Dělnická strana (DS). Z těchto subjektů byly nejaktivnější a nejvíce se zviditelňovaly Národní odpor, Autonomní nacionalisté a Dělnická strana. [45]

3.3.1 Celkový počet trestních činů s extremistickým podtextem zaevidovaných na území ČR v letech 2005 až 2009

Tab. 15. Počet extremistických trestných činů v letech 2005-2009 [45]

Rok	Zaevidováno TČ	Podíl na celkové kriminalitě	Objasněno TČ	Stíháno osob
2005	253	0,07	191	269
2006	248	0,07	196	242
2007	196	0,05	119	181
2008	217	0,06	126	195
2009	265	0,07	186	293

3.3.2 Vývoj zaevidovaných trestných činů s extremistickým podtextem a počet stíhaných osob

Rok 2006

Z celkového objemu zaregistrované kriminality v České republice v roce 2006 činila trestná činnost s extremistickým podtextem 0,07%. Počet zaevidovaných trestných činů s extremistickým podtextem se **snížil proti roku 2005 cca o 2% tedy z počtu 253 na 248 tj. o 5 trestných činů.** Ale oproti roku 2005 se počet stíhaných osob **zvýšil o cca 10%.**

Rok 2007

Z celkového objemu zaregistrované kriminality v České republice v roce 2007 činila trestná činnost s extrémistickým podtextem 0,05%. Počet **zaevidovaných trestných činů** s extremistickým podtextem **se snížil proti roku 2006 cca o 21%.** Rovněž **poklesl cca o 25% počet stíhaných osob** oproti roku 2006.

Rok 2008

Z celkového objemu zaregistrované kriminality v České republice v roce 2008 činila trestná činnost s extremistickým podtextem 0,06%. Počet **zaevidovaných trestných činů** s extremistickým podtextem se **zvýšil proti roku 2007 cca o 11%.** Rovněž **vzrostl o cca 8% počet stíhaných osob** oproti roku 2007.

Rok 2009

Z celkového objemu zaregistrované kriminality v České republice v roce 2009 činila trestná činnost s extrémistickým podtextem 0,07%. Počet **zaevidovaných trestných činů** s extrémistickým podtextem se **zvýšil oproti roku 2008 cca o 22%.** Rovněž **vzrostl o cca 50,3% počet stíhaných osob** oproti roku 2008.

3.3.3 Nejčastěji byly pachatelé odsouzení za níže uvedené trestné činy

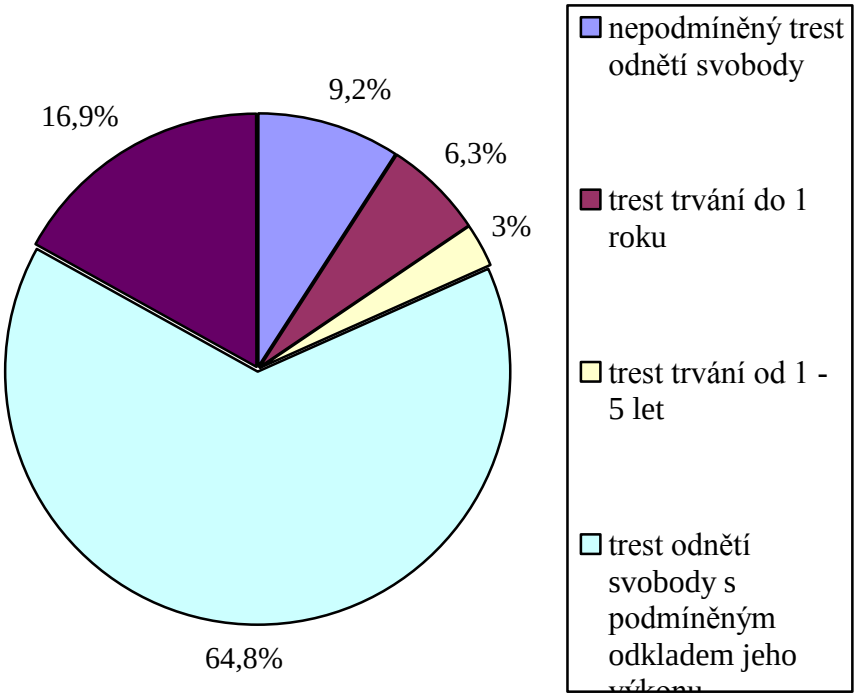
Tab. 16. Odsouzení pachatelé v letech 2005 – 2009 [45]

Trestný čin	Ustanovení tr. zákona	Počet osob				
		2005	2006	2007	2008	2009
Podpora a propagace hnutí směřující k potlačení práva svobod člověka	§ 260,261	67	34	24	47	40
Hanobení národa, etnické skupiny, rasy a přesvědčení	§198	39	14	13	15	20
Násilí proti skupině obyvatelů a proti jednotlivci	§196	26	21	14	14	30
Výtržnictví	§202	8	7	4	8	60
Ublížení na zdraví	§221	5	3	6	6	7
Útok na veřejného činitele	§155	5	2	0	0	2
Vydírání	§235	2	1	1	0	1
„nebezpečné ohrožování“	§197a	2	2	1	0	4
Podněcování nenávisti vůči skupině osob nebo k omezování jejich práv a svobod	§198a	2	1	0	0	1
Ublížení na zdraví – těžká újma	§222	1	5	1	1	4
Krádež	§247	1	1	1	0	2
Celkem		**158**	**91**	**65**	**91**	**171**

3.3.4 Skladba trestných činů

V roce 2005

Tresty

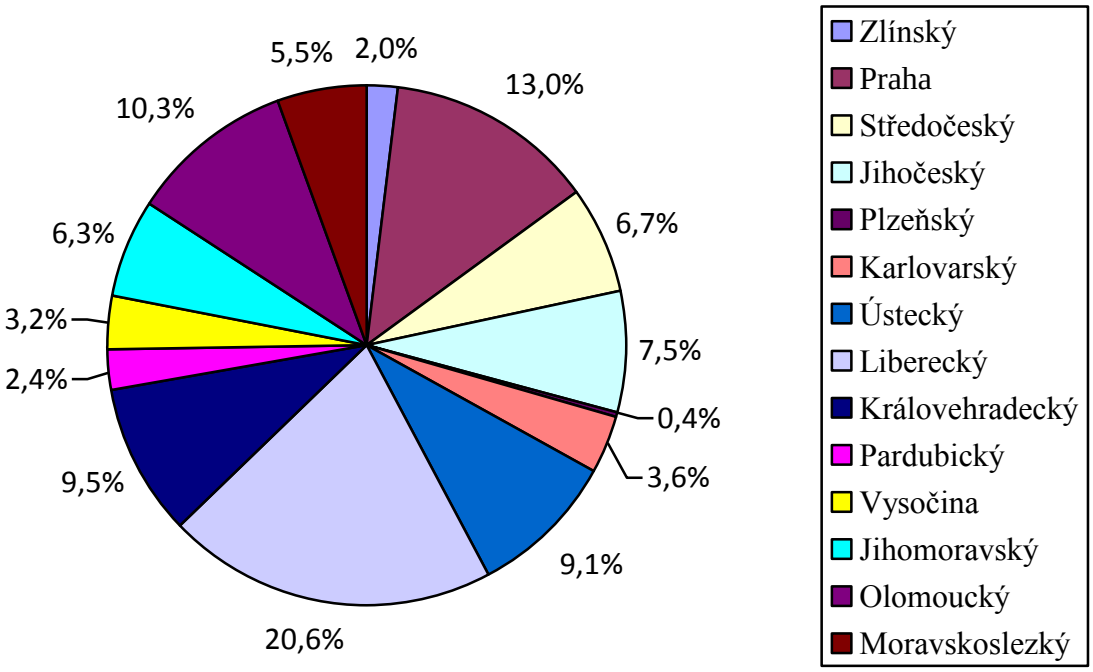


Obr. 12. Udělené tresty v roce 2005 [45]

Skladba odsouzených

Z celkové počtu odsouzených bylo 19 osob recidivisty, označených soudem, naopak 86 osob bylo doposud netrestaných. Mladistvých osob bylo odsouzeno 22 z celkového počtu osob odsouzených za trestné činy s rasovým podtextem. Odsouzených žen bylo 11. [9]

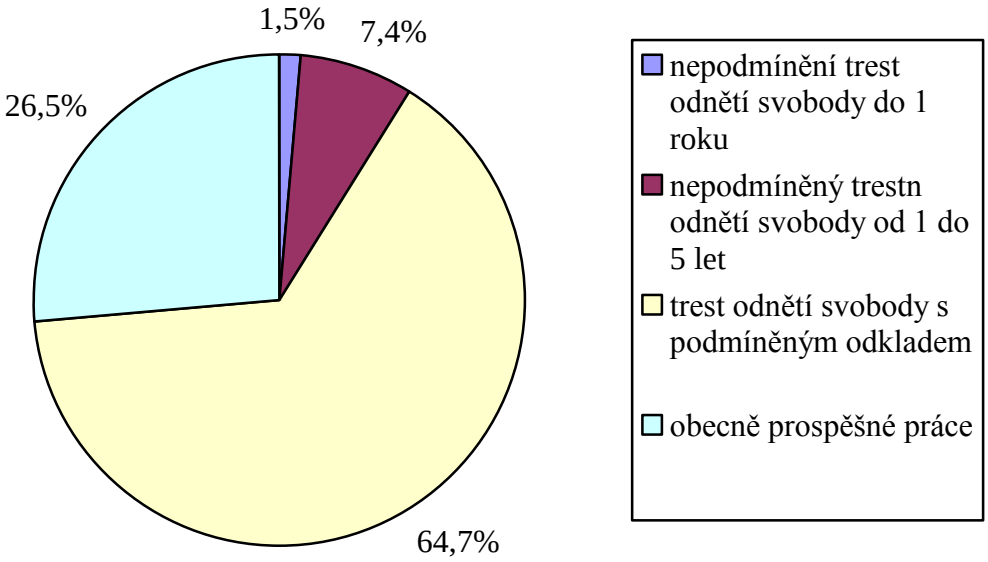
Podíl jednotlivých krajů



Obr. 13. Podíl jednotlivých krajů na extremismu v roce 2005 [45]

Rok 2006

Tresty

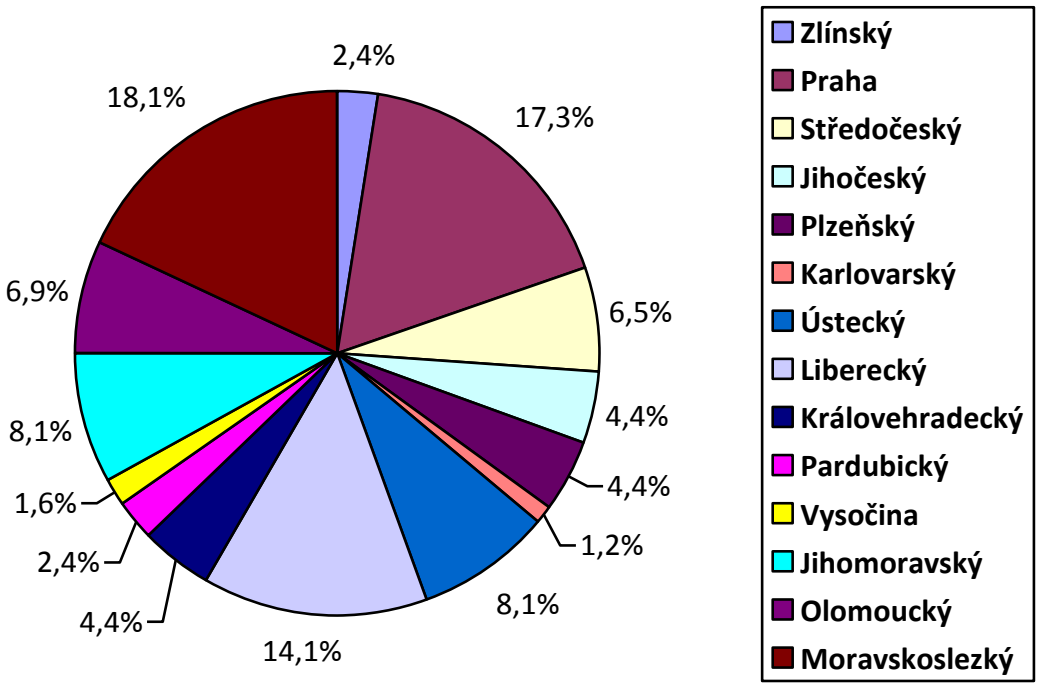


Obr. 14. Udělené tresty v roce 2006 [45]

Skladba odsouzených

Z celkové počtu odsouzených bylo 13 osob recidivisty, označených soudem, naopak 35 osob bylo doposud netrestaných. Mladistvých osob bylo odsouzeno 18 z celkového počtu osob odsouzených za trestné činy s rasovým podtextem. Odsouzených žen byly 2.

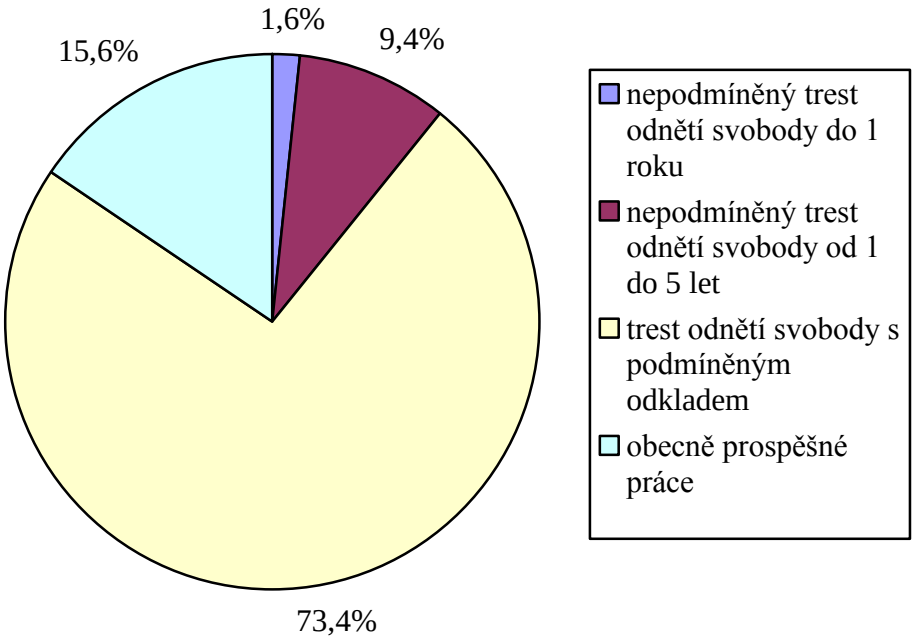
Podíl jednotlivých krajů



Obr. 15. Podíl jednotlivých krajů na extremismu v roce 2006 [45]

Rok 2007

Tresty

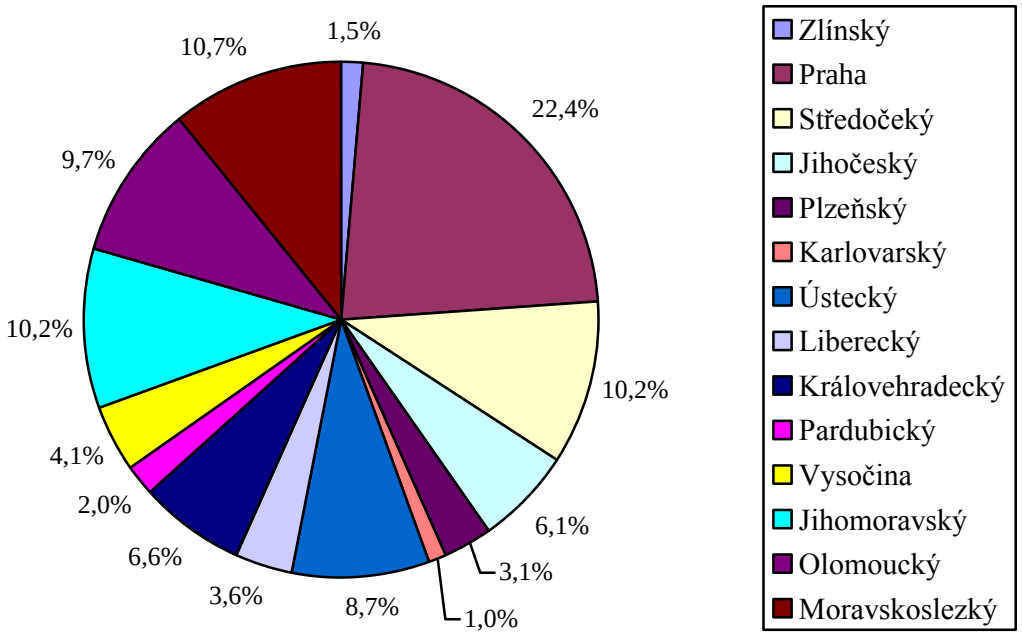


Obr. 16. Udělené tresty v roce 2007 [45]

Skladba odsouzených

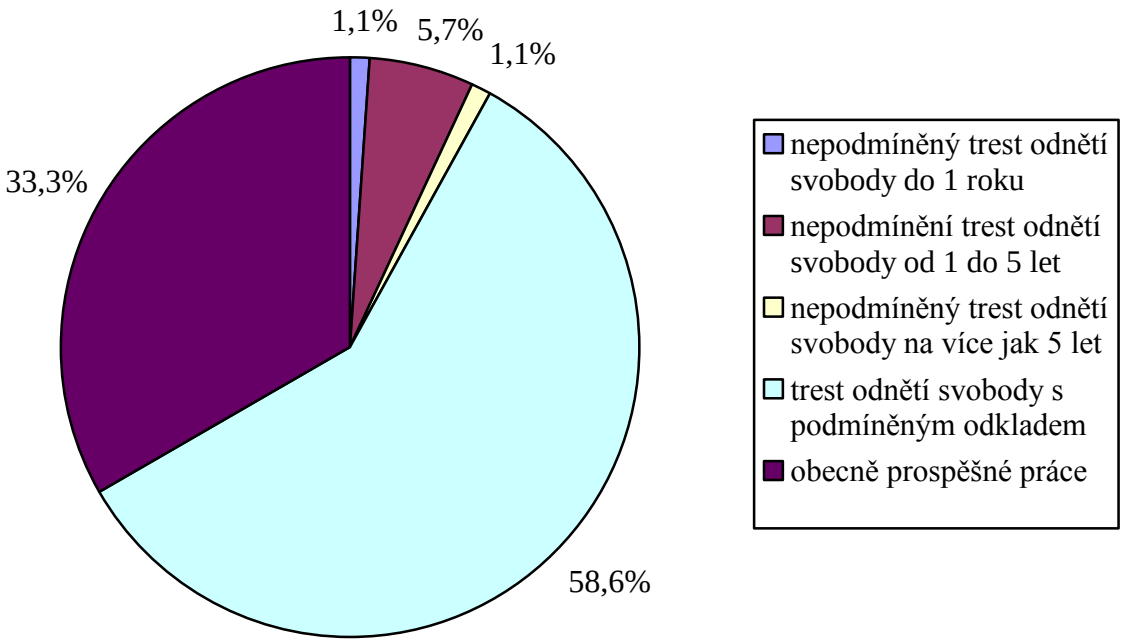
Z celkové počtu odsouzených bylo 10 osob recidivistů, označených soudem, naopak 35 osob bylo doposud netrestaných. Mladistvých osob bylo odsouzeno pouze 4 z celkového počtu osob odsouzených za trestné činy s rasovým podtextem. Odsouzené ženy byly 4.

Podíl jednotlivých krajů



Obr. 17. Podíl jednotlivých krajů na extremismu v roce 2007 [45]

Rok 2008

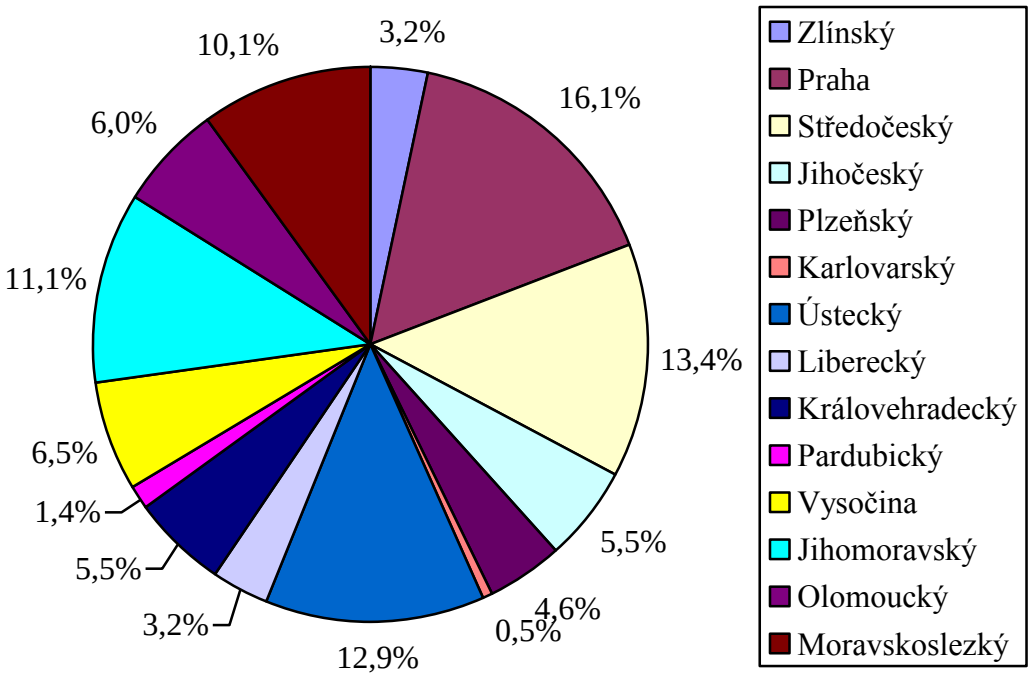


Obr. 18. Udělené tresty v roce 2008 [45]

Skladba odsouzených

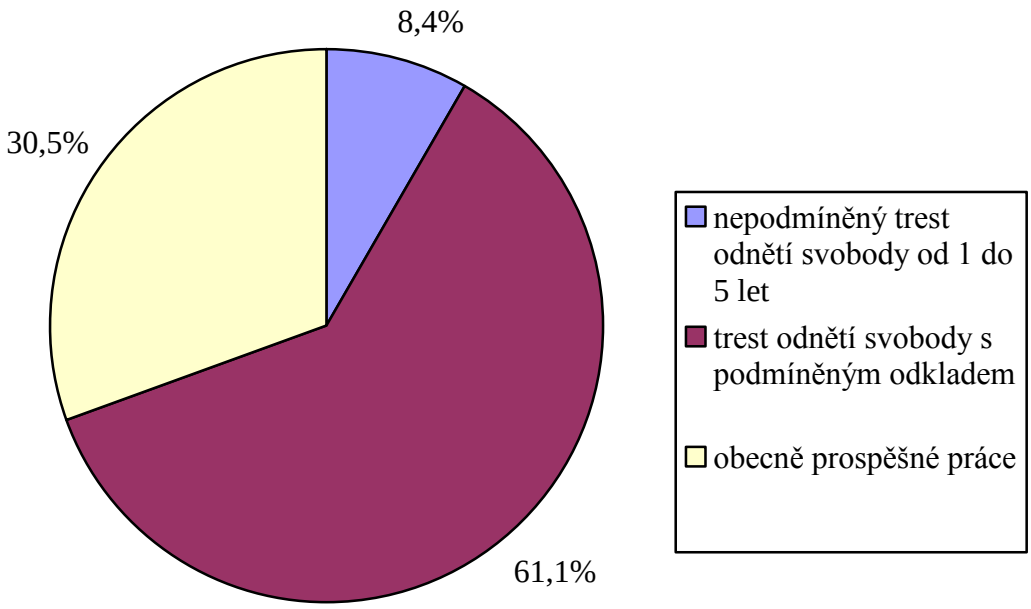
Z celkové počtu odsouzených bylo 9 osob recidivistů, označených soudem, naopak 46 osob bylo doposud netrestaných. Mladistvých osob bylo odsouzeno pouze 6 z celkového počtu osob odsouzených za trestné činy s rasovým podtextem. Odsouzené ženy byly 3.

Podíl jednotlivých krajů



Obr. 19. Podíl jednotlivých krajů na extremismu v roce 2008 [45]

Rok 2009

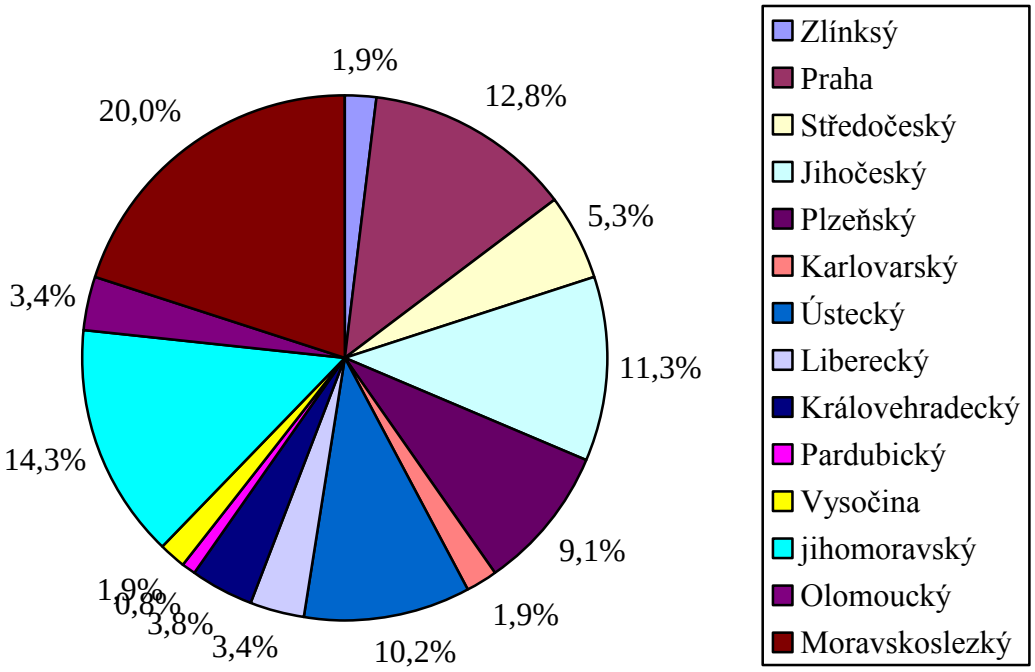


Obr. 20. Udělené tresty v roce 2009 [45]

Skladba odsouzených

Z celkového počtu odsouzených nebylo 48 osob doposud soudně trestáno. Odsouzeno bylo pouze 7 mladistvých osob z celkového počtu osob odsouzených za trestné činy s rasovým podtextem. Odsouzeny byly pouze 4 ženy.

Podíl jednotlivých krajů



Obr. 21. Podíl jednotlivých krajů na extremismu v roce 2009 [45]

Extremismus sebou vždy nese možné ohrožení demokracie. Je proto nutné toto jednání a názory co nejvíce potlačovat, ať už ze strany politiků, vzdělávání ve školních zařízeních nebo ze strany legislativní.

3.3.5 Extremismus a internet

Internet je fenomén, který ovlivňuje i extremistickou scénu. Jeho význam lety vzrostl a vzrůstal také na důležitosti u extremismu. Hlavně díky anonymitě, dostupnosti, rychlosti spojení, ale také proto, že je jednoduchým a levným nástrojem k projevům svých názorů. Čeští extrémisté využívají toto médium k celé řadě činností, jako je např. prezentace svých myšlenek, komunikaci, prodeji zboží s extrémistickou tématikou, svolávání demonstrací, ale hlavně propagandou. Jako propagace svých názorů hrál, hraje a jistě bude nadále hrát roli Facebook, kdy se objevují např. skupiny s názvem „Nikdy se nesměj cikánovi na kole, třeba to kolo je právě tvoje“, která má ke dni 6.10.2011 15636 členů, „Cikáni bez sociálních dávek = cesta z ekonomické krize, která měla ke dni 6.10.2011 10268 členů. Nejen Facebook je na internetu používán k propagaci extremismu. Díky Internetu se objevují návody jak se při zadržení policií, tyto návody posléze ztěžují vyšetřování a potrestání pachatelů.

4 ANALÝZA PŘÍČIN NÍZKÉ TRESTANOSTI

Analýza příčin nízké trestnosti

Kybernetická kriminalita, neboli kybernalita je velmi široká mezioborová disciplína a vztahuje se na velmi široký okruh trestních a nemorálních činů. Prvotní nebezpečí těchto hrozeb je, že nejsou na první pohled viditelné. Podle statistik USA je odhaleno jen asi 5% této trestné činnosti a z nich se pouze 20% dostane do soudní síně. Vzhledem ke globálním rozměrům kybernality, kdy není omezena hranicemi států je řešení škody a dohledávání pachatelů dosti náročné. Nehledě na to, že to co je v jedné zemi považováno za trestný čin může být v druhé zcela legální.

V této kapitole se pokusím sepsat příčiny nízké trestnosti :

1. **Svoboda internetu** – narůstající snahy o kontrolu, regulaci, cenzuru Internetu, jediného doposud volně šiřitelného svobodného média je omezována demokracie a svoboda našeho projevu. Je jedno, jakým způsobem se to děje. Lidé si zakládají profily, aby zde svobodně projevovali své názory, přispívají do diskuzí a mnoho dalších činností, které mohou být v určitém stádiu brány jako forma trestného činu.

2. **Chápání společnosti** - Vnímání počítačové kriminality společností je zatíženo nehmotným charakterem produktů a bezprostřední neviditelností následků trestné činu. Zatímco krádež počítače, tedy fyzického hardwaru, je vnímána jako běžný trestný čin, u věcí, které nemají hmotnou podstatu, se veřejné mínění přesouvá na druhou stranu barikády. Pachatel, který převede několik miliónů z účtu svého zaměstnavatele na účet vlastní, je posuzován jinak, než kdyby přišel do banky s pistolí a peníze si vzal násilím. Společnost ho spíše považuje za šikovného a mazaného podvodníčka. [17]

Tab. 17. Porovnání následků klasického a kybernetického trestného činu [17]

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn nebo zabit	Bez rizika fyzického zranění
Zisk	Průměrně 3 až 5 tisíc USD	Od 50 až do 50 tisíc USD
Pravděpodobnost dopadení	Dopadeno 50 až 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 skutečně odsouzeno jenom 50%
Trest	Průměrně 5 až 6 let, pokud pachatel někoho nezranil	Průměrně 2 až 4 roky

Tabulka uvádí porovnání běžné ozbrojené bankovní loupeže s kybernetickým zločinem obdobného charakteru a vychází z dlouhodobých statistik amerického úřadu pro vyšetřování FBI.

3. **Globální hledisko** - internet nemá hranice a neomezuje ho vzdálenost ani hranice států.

4. **Nedostatek pracovníků** - společně s přibývajícím počtem připojení obyvatel k internetu, přibývá na síti i kriminality. Další problém nastává při řešení této nelegální činnosti, kdy se nedostává policistů na řešení této situace. Tato skutečnost souvisí mimo jiné i s požadavky, které jsou na tyto místa kladeny. Zájemci musí mimo jiné u Policie odsloužit nejméně devět let a mít vysokoškolské vzdělání.

5. **Kvalifikace pracovníků**- kriminalita týkající se kyber prostoru je činnost páchaná s použitím specifickým technologických nástrojů a specializovaných znalostí. K potírání a odsouzení této činnosti je tedy opět nutné mít množství speciálních nástrojů, znalostí a postupů. S tím souvisí nedostatek kvalifikovaných pracovníků, kteří by byli schopni tuto problematiku zvládnout. Nehledě na to, že „klasické" vyšetřovací metody v tomto případě selhávají zejména z důvodů snadného a neomezeného pohybu v kyber prostoru, kde se stopy snadno a rychle ztrácí.

6. **Problém justice** – i přesto, že je bezpochyby kybernalita trestná, není snadné jí prokázat a posléze pachatele odsoudit. V případě soudců je to obdobné jako s nedostatkem kvalifikovaných pracovníků u policie, kdy soudce je specialista na právo a ne na informační technologie, pro tyto účely se zařazují do vyšetřování soudní znalci. Tyto procesy bývají značně zdlouhavé a častokrát vedou až ke ztrátě důkazů.

7. **Rychlost** - zatím co stopy klasického trestného činu lze zajistit ještě několik hodin nebo dnů po činu, v případě kybernality je zajištění stop otázkou minut. Trestný čin se odehrává ve složitém technologickém prostředí, jehož stav se každou sekundou mění.

8. **Internet jako demokratické médium** – internet je často spojován se svobodou projevu. I přesto by měli být stanoveny hranice, kdy je obsah ještě svobodným projevem a nepoškozuje práva ostatních, a kdy už obsah tuto hranici překročil.

9. **Kriminalita tzv. „bílých límečků"**- pachatel počítačové kriminality bývá zpravidla vyzbrojen znalostmi informačních technologií.

10. **Vybavení a možnosti policie** - pachatelé trestných činů mívají viditelný náskok před policií, je zcela nemožné tento náskok dohnat, útočníci jsou vždy před policií, už jen z důvodů organizování, kdy větší skupiny mají větší možnosti vybavení.

11. **Zákony**- kdy přijetí každého navrhovaného zákona trvá nepřiměřenou dlouhou dobu

12. **Neustálé vzdělávání pracovníků**- policie ale i orgány činné v trestním řízení by se neustále měli zdokonalovat v tomto odvětví kriminality a tím svoje poznatky zvyšovat a zkvalitňovat boj s touto kriminalitou.

13. **Digitální propasti** - V souvislosti s rozšiřováním ICT do celého světa je nutné zmínit jejich nevyvážené pokrytí a vznik tzv. digitální propasti (digital divide). Rozvojové země s minimální technologickou úrovní se pak mohou stát výhodnou základnou nebo přestupní stanicí kybernetických útoků. V takovýchto zemích se předpokládá nízká, popř. nulová úroveň legislativy, což je pochopitelně pro útočníky neodolatelným lákadlem. [7]

14. **Legislativa** - jedním ze základních problémů kybernality je obtížnost konkrétní definice počítačového trestného činu a jeho dokazování. Podle statistik USA je odhaleno jen asi 5% takových činů a z nich se pouze 20% dostane do soudního procesu. Právní normy nejsou schopny zcela jasně vyjmenovat a konkretizovat jednotlivé zločiny, a proto jsou soudní řízení velmi nejasná a zdlouhavá, nehledě na nedostatečnou kvalitu navrhovaných zákonů.

15. **Různé pohledy zemí** – co je v jedné zemi bráno, jako trestný čin v druhé může být zcela legální. Např. warez je v západních zemích považován za nelegální a v zemích třetího světa je legální.

16. **Odpovědnost poskytovatele služeb** - poskytovatelé služeb nejsou povinni dohlížet na obsah jimi přenášených nebo ukládaných informaci, ani aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace. Jinak řečeno, nelze chtít po poskytovatelích, aby v tak velkém množství uživatelů hledali nelegální obsah informací. Pokud ale na takový obsah narazí, je jeho povinností, takový obsah odstranit nebo se zasloužit o to, aby byl takový obsah znepřístupněn, v tomto případě se stává za tento obsah zodpovědný.

17. **Nezájem o vyšetřování-** není výjimkou že poškozená strana nemá zájem o odhalení pachatele trestné činnosti, děje se tak např. z důvodů ztráty klientů, kdy se banky nerady svěřují s útokem hackera obav, že přijdou o své klienty.

Extremismus na Internetu

Internet je fenomén, který ovlivňuje i extremistickou scénu. Jeho význam lety vzrost a vzrůstal také na důležitosti u extremismu. Hlavně díky anonymitě, dostupnosti, rychlosti spojení. Využívají čeští extremisté toto médium k celé řadě činností, jako je např. prezentace svých myšlenek, komunikaci, prodeji zboží s extremistickou tématikou, svolávání demonstrací, ale hlavně k propagandě. Jako propagace svých myšlenek hraje roli i sociální síť Facebook, kdy se objevují skupiny s názvem „Cikán bez sociálních dávek = cesta z ekonomické krize“ (10268 členů), „Cikáni do práce“ (15902 členů), „Za chvíli budou chtít cikáni zrušit i šachy, protože začínají BÍLÍ..:D“ (12579 členů). Nejen Facebook, je na Internetu používán k propagaci extremismu. Díky Internetu se objevují i internetová rádia. Objevují se zde také návody, jak se zachovat při zadržení policií, tyto návody posléze ztěžují vyšetřování a potrestání pachatelů. Mezi rady patří např.:

- Máš právo nevypovídat (v zákoně je napsáno, že v případě, pokud by jsi sobě nebo osobě své blízké způsobil trestní stíháni za trestný čin či přestupek - tuto osobu však nemusíš blíže specifikovat). To je často nejlepší řešení. Pokud se tak rozhodneš, buď skutečně důsledný.
- Pokud vypovídáš, neříkej rezolutní ne - policie pak může napadnout rozpory ve tvé výpovědi. Použij radši formulace “nepamatuji se”
- Na demonstraci neber s sebou diáře, telefoníčky a další poznámky, které by policii mohli dovést ke Tvým přátelům. Zablokuj paměť mobilního telefonu.
- Přijďte pokud možno ve větší skupince, ve které se dobře znáte. Můžete se předem domluvit, že se uvedete navzájem jako svědky nebo na tom, že nebudete vypovídat.
- Na demonstraci jsi se pochopitelně ničeho nezákonného nedopustil ani jsi si nevšiml nikoho, kdo by něco takového páchal. Byl jsi v davu a neviděl jsi dál než na lidi stojící vedle tebe.
- Na demonstraci jsi nikoho neznal (pokud jsi se ovšem s kamarády nedomluvil na vzájemném svědectví).

- Řekni, že se žádné demonstrace nezúčastníš. Pokud to je po akci, klidně řekni, že jsi tam byl (dle situace, naopak to klidně zapři), ale že jsi už odešel. Pokud je u tebe nalezena v takovéto situaci nějaká zbraň, policistovi řekni, že ji máš pro vlastní obranu a jelikož nejsi na demonstraci, tak nemá právo ti ji odebrat. Pokud je to před akcí, na žádnou demonstraci samozřejmě nejdeš a ani nevíš, že se něco takového koná. [15]
- Jeden z hlavních důvodů ztěžujících nebo znemožňujících identifikaci osob dopouštějících se extremismu je to, že mají zakrytý obličej a tím je nemožná jejich identifikace.
- Od 1. Ledna 2009 má povolení policie vstupovat do všech prostor, u kterých lze mít důvodné podezření, že se v něm zdržují fyzické osoby, a to i po skončení provozní doby, mohou vstupovat i do skladů, kuchyní a jiných prostor.

5 NÁVRHY A MOŽNOSTI ZLEPŠENÍ SITUACE

Pravidla všeobecné prevence

Prevencí se rozumí různá zabezpečení, která zkomplikují případnému útočníkovi dostat se k datům ve vašem počítači. Mezi tuto prevenci nepatří pouze technologická prevence v podobě antivirových a preventivně zaměřených programů, ale také především povědomí uživatelů pohybujících se na internetu, tato činnost se netýká pouze soukromých uživatelů, ale také společností.

Dalším důležitým bodem prevence je neustálé připomínání nemorálnosti a společenské nepřijatelnosti protiprávních činů souvisejících s tímto druhem kriminality.

Zákony

- Zákony by měli popisovat všechny formy příslušné kriminality a stanovit jejich postihy.
- Sledování vývoje dosavadní kriminality na Internetu a mapování nových trendů.
- Zlepšení koordinace mezi zúčastněnými státy.
- Vytvoření skupiny odborníků na odhalování této kriminality a jejího následného řešení.
- Provádět neustálé školení a semináře o vývoji kriminality pro orgány činné v trestním řízení v oblasti informačních technologií.
- Podporovat výzkumnou činnost v této oblasti trestných činů.
- V rámci boje spolupracovat s mezinárodními a nadnárodními organizacemi a zúčastňovat se pořádaných akcí.
- Do boje se musí zapojit i poskytovatelé internetových služeb a to v možnosti blokace webů s danou problematikou, kde se nachází obsah v rozporu se zákonem.

Internetová komunikace

- Jedním z hlavních pravidel je nikdy nezveřejňovat osobní údaje (jméno, příjmení, telefon,..).

- Neuvádět bydliště.
- Nezveřejňovat fotku.
- Na sociálních sítích typu Facebook, Yahoo apod. si přidávat jen skutečné přátele.
- Nikdy nikde nezaškrtávat „pamatovat si mě na tomto počítači“.
- Neotvírat e-maily od adresátů, které neznáme a k nim přiložené soubory. Většinou se jedná o spam nebo vir.
- Nereagovat na snahu o navázání komunikace cizím člověkem.

Rady pro online transakce

- Zvolit si silné heslo.
- Neprozrazovat nikomu svá hesla.
- Neklikat na odkazy v příchozích e-mailech, vždy odkaz napsat do řádku pro adresu.
- Nevyplňovat a nezasílat formuláře vyplněné přes Internet.
- Hlásit jakoukoliv námi neprovedenou změnu na bankovním účtu.

Extremismus

- Jedinou možností jak bojovat s extremismem je komunikace. Zabráněním projevů by bylo bráno jako omezování svobody projevu a nebylo by toto jednání demokratické. Přes všechno musí být stanoveny hranice mezi svobodným projevem a omezováním práv ostatních.
- Do boje s extremismem se musí zapojit krom Ministerstva vnitra a policie ČR také další subjekty jako je škola (v rámci výuky, pořádání seminářů), ale také média.
- Zavedení pojmu extremismu už do výuky na ZŠ.
- Nekompromisní postihy pro osoby s extremistickými projevy.

Kyberšikana

- Zvyšování podvědomí u občanů o této problematice.
- Spolupráce školy, polici, rodičů.
- Pravidelné proškolování personálu škol, jak postupovat v případě zjištění kyberšikany, ale také jak ji předcházet.
- Začlenit kyberšikanu do výuky IT.
- Pořádat besedy pro žáky, rodiče, školy.
- Je třeba zaměřit se na prevenci.
- Určit jasná pravidla potrestání.

Softwarová policie

Příčinou nedostatečné činnosti policie ČR v této oblasti jsou nedostatečné prostředky, které jsou investovány do tohoto sektoru. Tento nedostatek způsobuje nedostatek pracovníků specializujících se na tuto problematiku. Ke zvýšení počtu policistů dosáhneme nabídkou motivující mzdy. Ministerstvo vnitra by mělo nabídnout takové platové ohodnocení, které je rovno nejméně tomu ve firmách, které zaměstnávají odborníky přes informační technologie.

FTP servery

Tyto servery vznikli pro zálohování dat, náhražka pro posílání dat s větším obsahem, které nelze odeslat. Jedná se servery, kde je možné anonymně uložit jakákoliv data, která může kdokoliv stáhnout. Díky anonymitě a snadnému šíření se ale staly jedním z hlavních nástrojů k šíření nelegálního obsahu. K napravení této situace by došlo s povinností registrace, kdy by povinnost zadat osobní data vedla ke strachu pachatelů k této činnosti a policii ČR by se značně usnadnila práce.

ZÁVĚR

S obrovským nárůstem informačních technologií a pronikání výpočetní techniky do mnoha lidských odvětví vznikly také nové druhy kriminality. Díky převážné anonymitě, kterou internet nabízí, se tato kriminalita rozšířila o to rychleji.

V úvodní části jsem se věnovala samotnému Internetu, jeho vývoji, historii, právnímu pojetí. Dále jste se v teoretické části mohli dočíst o trestné činnosti přes internetovou síť, která nejvíce zaměstnává Policii ČR, jedná se především o dětskou pornografii, porušování autorských práv, extremismus, nebezpečné komunikační jevy a zneužívání platebních a obchodních styků.

Cílem mé diplomové práce bylo upozornit na nebezpečí počítačové kriminality, která se šíří přes Internet. Tato kriminalita může postihnout široké pole osobního i společenského života např. jako útoky v podobě kyberšikany, sextingu, kybergroomingu..

V praktické části jsou zpracovány statistiky vybraných druhů kriminalit za uplynulých několik let. Mezi tuto kriminální činnost patří porušování autorských práv, dětská pornografie, extremismus. Cílem této části bylo poskytnout přehled o nejdůležitějších a nejvíce frekventovaných jednáních z pohledu soudních statistik.

Dále je zde uvedena analýza příčin nízké trestnosti, která především vypovídá o tom, že není možné potírat tyto delikty bez potřebného vybavení, poznatků a dalšího navyšování kvalifikace vyšetřujících složek. Úspěšnost dopadení pachatele této trestné činnosti závisí nejen na vyšetřujících složkách, ale také na chápání společnosti, změně zákonů, spolupráci mezi zeměmi, odpovědností poskytovatelů a mnoho dalšího.

Závěrečná část práce je věnovaná prevenci, jakož nejdůležitějšímu prvku v boji proti s touto kriminalitou. Důležitým faktorem prevence je naučit se chránit svá data, neměli bychom otevírat nevyžádanou poštu, zveřejňovat a nikomu neposkytovat své osobní údaje, čísla účtů, hesla. Proto je také třeba zvyšovat povědomí a kvalifikaci uživatelů a zvyšovat tak povědomí o této problematice.

Mým hlavním cílem bylo poukázat na aktuální, nejzávažnější a nejvíce známé projevy kriminality v oblasti Internetu.

Doufám, že jsem svojí diplomovou prací přispěla k osvětlení této problematiky a umožnila čtenáři seznámit se blíže s touto trestnou činností.

ZÁVĚR V ANGLIČTINĚ

With the huge in crease in the penetration of information technology and computer technology to many human industries, also created new types of crime. With the vast anonymity that Internet offers, this crimesprej that much faster.

In the first part, I was devoted to the Internet it self, its development, history and legal concepts. In theoretical part, you could read about the crime through the Internet network, which employs most Police, it is mostly child pornography, copyright violations, extremism, hazard ous communication phenomena and abuse of credit and trade relations.

The aimofmy thesis was to drawattention to the Langersof cybercrime, which spreadacross the Internet. This crimecanaffect a widearray of personal and social life, such as attacks in the formof cyberbullying, sexting, kybergrooming ..

In the practical part of the statistics are processed in selected types of crime in the past few years. The criminal activities include copyright in fringement, child pornography, extremism. The aim of this sectionis to provide an over view of the most important and most frequent negatiations from the perspective of judicial statistics.

The reis also ananalys is of the cause so flow criminality, which reflects the fact that it is not possible to combat these offenses with out the neceséry equipment, know ledge and skills furtherin creases investigating components. The Access of the capture of the perpetrators of crimes depends not only on investigating the in gredients, but also on the understanding of society, law schange, cooperation between countries, responsibilities of providers and much more.

The final part is devotedint oprevention, as well as the most important element in the fight against crime with this crime. Very important factor in preventionis to learn how to protectour data, weshould not open junk mail, and not to disclose your personal information, account numbers, passwords. It is also important to raise awareness and skill so fusers and in leasing the awarenes soft his issue.

My main goal was to show the current, most serious and most well-known manifestations of crime in the Internet.

I hope thatmy thes is helped to illuminatet his issue and allow the read closer with this crime.

SEZNAM POUŽITÉ LITERATURY

[1] BARANOVIČ, R., MORAVČÍKOVÁ, Ľ., ŠNAJDER, Ľ. Internet. Computer press: Praha 1999. ISBN 80-7226-186-x

[2] *Business Software Alliance* [online]. [cit. 2011-30-09]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Business_Software_Alliance

[3] *Co je extremismus?* [online]. [cit. 2011-08-05]. Dostupný z WWW: http://www.policie.cz/clanek/prevence-informace-o-extremismu-co-je-extremismus.aspx

[4] *Co je to hoax* [online]. [cit. 2011-10-04]. Dostupný z WWW: http://www.hoax.cz/hoax/co-je-to-hoax

[5] *Co je to hoax a jak se mu bránit* [online]. [cit. 2011-10-04]. Dostupný z WWW: http://www.hobbystranky.cz/zajimavosti/co-je-hoax-jak-se-mu-branit Computer Press, 2007. str. 150. ISBN 978-80-251-1777-4.

[6] *Dětská pornografie* [online]. [cit. 2011-09-05]. Dostupný z WWW: http://iuridictum.pecina.cz/w/Dětská_pornografie

[7] *Elektronická informační kriminalita* [online]. [cit. 2011-09-18]. Dostupný z WWW: http://www.ikaros.cz/node/3554

[8] *HOAX aneb poplašné zprávy* [online]. [cit. 2011-10-04]. Dostupné z WWW: http://www.dvojklik.cz/2010-07/hoax-aneb-poplasne-zpravy

[9] *Informace o problematice extremismu na území České republiky v roce 2005* [online]. [cit. 2011-09-25]. Dostupný z WWW: http://www.mvcr.cz/soubor/zprava-o-problematice-extremismu-2005.aspx

[10] *Internet - Co je to Internet, výhody a nevýhody, popište: internetovou adresu, e-mailovou adresu, co je to: email, emailová zpráva, elektronická pošta* [online]. [cit. 2011-09-14]. Dostupný z WWW: http://www.ok2stm.cz/ke_stazeni/internet.pdf

[11] *Internet skrývá nové nebezpečí nejen pro vaše bankovní účty nazývající se pharming* [online]. [cit. 2011-09-09]. Dostupný z WWW: http://trojanhelp.wz.cz/pharming.htm

[12] Internet u *nás* [online]. [cit. 2011-09-12]. Dostupné z WWW: http://ihistory.webzdarma.cz/chap/cr.php

[13] *Internetové projevy nesnášenlivosti* [online]. [cit. 2011-08-05]. Dostupný z WWW: www.helcom.cz/download/extremismus/hate_speech_obecne.doc

[14] Jak se bránit proti nevyžádaným e-mailům [online]. [cit. 2011-08-24]. Dostupný z WWW: http://www.uoou.cz/uoou.aspx?menu=23&submenu=24

[15] *Jak se chovat při zadržení nebo předvolání* [online]. [cit. 2011-10-07]. Dostupný z WWW: http://www.csaf.cz/stara_verze/abc/jak_se_chovat.html

[16] *Jaké hrozí ČR tresty za porušování autorského práva* [online]. [cit. 2011-10-08]. dostupný z WWW: Zdroj:http://www.mpx.cz/ZAJIMAVOSTI/Jake-hrozi-v-CR-tresty-za-porusovani-autorskeho-prava.html

[17] JIROVSKÝ, V., *Kybernetická kriminalita*, Grada 2007, ISBN 80-247-1561-9

[18] KOLOUCH, J., VOLENECKÝ, P. *Trestněprávní aspekty phishingového útoku*. Trestní právo, 2008, roč. XII, č. 9, s. 6.

[19] KRÁL, M., Bezpečnost domácího počítače prakticky a názorně, Grada, ISBN:80-247-1408-6

[20] *Kyberšikana – kybernetická šikana* [online]. [cit. 2011-10-05]. Dostupné z WWW: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie

[21] *Kyberšikana* [online]. [cit. 2011-10-06]. Dostupné z WWW: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/4-pehledovy-list-kyberikana-1-a-2

[22] *Kyberšikana a její prevence* [online]. [cit. 2011-09-10]. Dostupný z WWW: http://www.bezpecnemesto.eu/prevence-kriminality/prevence-aktualne/kybersikana-a-jeji prevence.aspx

[23] *Kyberšikana i stalking je všude kolem nás, koho se týká?* [online]. [cit. 2011-08-04]. Dostupný z WWW: http://www.nasepenize.cz/kybersikana-i-stalking-je-vsude-kolem-nas-koho-se-tyka-5949

[24] LANCE, J., *Phishing bez záhad*, ISBN 978-80-247-1766-1

[25] *Leták kyberšikana – rodiče* [online]. [cit. 2011-10-05]. Dostupné z WWW: http://www.minimalizacesikany.cz/images/stories/plakaty_kybersikana/kybersikana_rodice.pdf

[26] *Mezinárodní spolupráce v boji proti informační kriminalitě* [online]. [cit. 2011-10-02]. Dostupný z WWW: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx

[27] *Netiketa – jak se chovat na internetu* [online]. [cit. 2011-09-25]. Dostupný z WWW: http://adasek.cz/netiketa.php

[28] *Pachatelé komerčního sexuálního zneužívání dětí* [online]. [cit. 2011-09-14]. Dostupný z WWW: http://www.vyzkum-mladez.cz/zpravy/1314622340.pdf

[29] *PC Software Piracy Rates by Region* [online]. [cit. 2011-10-04]. Dostupný z WWW: http://www.bsa.org/country/~/media/D02B5A4B60444B0AAF6CFDD598C72CBC.ashx

[30] PETERKA, J. *Historie naší liberalizace, díl II: Ještě než přišel Internet* [online]. [cit. 2011-09-11]. Dostupné z: http://www.earchiv.cz/b01/b1016001.php3

[31] *Počítačová (informační) kriminalita a úloha policisty při jejím řešení* [online]. [cit. 2011-10-04]. Dostupný z WWW: http://www.scritube.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php

[32] *Počítačová kriminalita* [online]. [cit. 2011-09-11]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Počítačová_kriminalita

[33] *Počítačová kriminalita: Nástin problematiky: Kompendium názorů specialistů* [online]. cit.[8-10-2011]. Dostupný z WWW: www.ok.cz/iksp/docs/256.pdf

[34] *Počítačové sítě a internet* [online].. Ostrava: VŠB-TU, 2006, [cit. 2011-09-09]. Dostupné z: http://geologie.vsb.cz/geoinformatika/

[35] *Pojištění a zneužití platební karty s programem Exclusive* [online]. [cit. 2011-09-12]. Dostupný z WWW: http://www.rb.cz/osobni-finance/kreditni-karty/visa-vernostni-program-exclusive/pojisteni-zneuziti-platebni-karty/

[36] POLČÁK, R.: *Právo na internetu : spam a odpovědnost ISP.* 1. vydání. Brno:

[37] ROGERS, V., *Kyberšikana*, Rok vydání: 2011, ISBN: 978-80-7367-984-2

[38] *Saferinternet.cz* [online]. [cit. 2011-09-15]. Dostupný z WWW: http://www.saferinternet.cz/o-nas

[39] SMEJKAL, V. *Informační a počítačová kriminalita v České republice* [online]. [cit. 2011-09-11]. Dostupné z WWW: http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html.

[40] *Softwarové pirátství v Česku kleslo třetím rokem o procentní bod, hodnota ukradeného softwaru činí 3,7 miliardy korun* [online]. [cit. 2011-10-01].

Dostupný z WWW: http://portal.bsa.org/globalpiracy2010/downloads/press/pr_czech_czech.pdf

[41] *Spam* [online]. [cit. 2011-09-27]. Dostupný z WWW: http://szs-bnl.wz.cz/view.php?cisloclanku=2008090001

[42] *Šikana – 4 hovory denně* [online]. [cit. 2011-09-09]. Dostupný z WWW: http://www.linkabezpeci.cz/webmagazine/articles.asp?ida=373&idk=416

[43] ŠTĚDROŇ, B., LUDVÍK, M. *Právo v informačních technologiích.* Computer media, s.r.o. 2008. *ISBN* 978-80-86686-36-3

[44] VOŘECH, J. MORKES, D. *1001 Tipů a triků pro Internet*. Computer press: Praha 1998, strana 263

[45] *Výroční zprávy o extremismu a strategie boje proti extremismu* [online]. [cit. 2011-09-22]. Dostupný z WWW: http://www.mvcr.cz/clanek/extremismus-vyrocni-zpravy-o-extremismu-a-strategie-boje-proti-extremismu.aspx

[46] Zákon č.140/1961 Sb., trestní zákon, ve znění pozdějších předpisů

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Tzv.	Tak zvaný.
Apod.	A podobně.
Resp.	Respektive.
Příp.	Případně.
Aj.	A jiné.
APRA	Úřad pro pokročilé výzkumné projekty.
APRANET	Advanced Research Projects Agency Network.
EUNET	Evropská UNIXová síť.
EARN	Evropské akademické a výzkumné sítě.
ČVUT	České vysoké učení technické.
Bps.	Bit za sekundu.
ČSR	Československá republika.
CESNET	České vzdělávací a vědecké sítě.
FESNET	Federální vzdělávací a vědecké sítě.
FERNET	Federální vzdělávací a výzkumná síť.
SANET	Slovenská akademická síť.
Sb.	Sbírka.
Č.	Číslo.
Např.	Například.
Tzn.	To znamená.
SMS	Služba krátkých textových zpráv.
MMS	Multimediální zprávy.
TZ	Trestní zákon.
SIM	Účastnická identifikační karta.
Čl.	Článek.

FAQ	Často kladené dotazy.
IP	Internetový protokol.
ČR	Česká republika.
BSA	Business Software Alliance.
Plk.	Plukovník.
Mgr.	Magistr.
CD	Kompaktní disk
Cca	Cirka.
Tj.	To je.
FBI	Federální úřad pro vyšetřování

SEZNAM OBRÁZKŮ

SEZNAM TABULEK