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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ KRIMINALITA A JEJÍ PŘÍČINY

Autor práce: Jiří Havlena

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

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

Katedra: Katedra právních oborů a bezpečnostních studií

2013

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s využitím uvedených pramenů a literatury.

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

…….

Děkuji vedoucímu bakalářské práce panu JUDr. Romanu Svatošovi, Ph.D. za pomoc, odborné vedení, cenné rady a připomínky během mé práce.

ABSTRAKT

HAVLENA, J. *Počítačová kriminalita a její příčiny : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2013. XX s. Vedoucí bakalářské práce : JUDr. Roman Svatoš, Ph.D.

Klíčová slova: Počítačová kriminalita, internet, sociální sítě, Facebook

Bakalářská práce se zabývá počítačovou kriminalitou a jejími příčinami. V první teoretické části se zaměřuje na počítačovou kriminalitu jako takovou. Věnuje se zde její historií a vývoji a jejím druhům. Ve druhé teoretické části se zaměřuje na internet a sociální sítě. Zde se věnuje historii a vývoji internetu, řeší např. otázky, co to vlastně internet je a jaký je jeho vliv na naši společnost. Dále pak se zabývá vývojem sociálních sítí a jejich rozdělením. Praktická část je zaměřena na analýzu bezpečnosti na internetu a sociálních sítích a navrhuje případná preventivní opatření.

ABSTRACT

HAVLENA, J. *Computer crime and its causes : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, o. p. s., 2013. XX p. Supervisor : JUDr. Roman Svatoš, Ph.D.

Key words: Computer crime, internet, social networks, Facebook

Bachelor thesis applies computer crime and its causes. The first teoretical part of the thesis is concentrated on computer crime. It dedicates its history and development and kinds of computer crime. The second teoretical part of the thesis is concetrated on the internet and social networks. It dedicates history and development of the internet, solves the question - what is the internet? And its influence on our society. Also it applies development of social networks and their dividing. The practical part analyses security on the internet and social networks and suggests possible precautions.

Obsah

Úvod

Předkládaná bakalářská práce je věnovaná problematice počítačové kriminality, kterou s sebou přináší současný rozvoj počítačové technologie.

Počítače jako takové samozřejmě neumožňují páchat trestnou činnost, jen poskytují nové možnosti a způsoby pro páchání trestných činů. Vývoj počítačové technologie stále pokračuje, setkáváme se s nimi v dnešní době na každém kroku. Vznik nových počítačových technologií by však měl člověku především ulehčovat práci, stává se ovšem i prostředkem pro kriminální činnost. Počítačové technologie pomáhají v páchání přestupků nebo trestných činů nejen v počítačové kriminalitě, ale i v ostatních odvětvích kriminality. Když se ohlédneme desítky let zpátky, počítače byly pro většinu lidi něčím neznámým, zatímco v dnešní době bychom už jen těžko hledali člověka, který by počítač neměl nebo s ním neuměl pracovat na základní úrovni.

S rozvojem počítačové technologie je spojen vznik internetu a počítačových sítí, které umožňují uživatelům vzájemně komunikovat. Internet je fenomén dnešní doby, kde lze najít téměř jakoukoli informaci během pár vteřin. Asi málokdo si už dokáže život bez internetu představit. Díky internetu jsme stále ve spojení s okolním světem, ať už se nacházíme doma nebo kdekoliv jinde na světě. Ale právě toto propojení uživatelů s sebou přináší velké riziko a nebezpečí počítačové kriminality.

S počítačovou kriminalitou se mnozí určitě setkali. Ať už jako oběti nebo jako pachatelé. Asi kdekdo má doma nelegálně vypálený CD nebo DVD nebo pomocí internetu stáhl některé programy, filmy, hudbu, hry atd. Mnozí uživatelé berou jako běžnou věc v životě, že když dostanou chuť se podívat na film, najdou si ho na určitých webových serverech a zadarmo si ho stáhnou během pár minut či hodin. Mnohem závažnější důsledky mají taková jednání jako je útok na počítač, vymazání nebo pozměnění dat, neoprávněný přístup k tajným informacím, vytvoření poplašných zpráv, podvodné převedení peněz z účtu a mnoho dalších, o kterých budu v bakalářské práci hovořit konkrétněji. Každý uživatel internetu by měl mít na svém počítači kvalitní antivirový program, který jej ochrání před možnými hrozbami, které číhají na některých webových stránkách; stačí jedno kliknutí a uživatel má rázem svůj osobní počítač napaden a může přijít o veškerá zálohovaná data.

Sociální sítě jsou v dnešní době velmi rozšířený a oblíbený prostředek pro uživatele internetu a je hned několik druhů, na kterých si lze vytvořit vlastní veřejný profil. Sociální síť je propojení skupiny lidí, které jim umožňuje mezi sebou komunikovat ve virtuálním světě, sdílet osobní údaje, fotografie a veškeré informace, které mohou být zneužity ve prospěch kriminální činnosti, což si mnozí z uživatelů vlastně ani neuvědomují. Sociální sítě mohou sloužit i jako velká pomoc policii při dopadení pachatele. Sociální sítě mohou někteří z uživatelů vnímat jako druhý život, do kterého unikají před skutečným světem. V tomto případě se uživatelé mohou vydávat, za koho vlastně chtějí, a vytvořit si profil dokonalé a úspěšné osobnosti. I díky těmto falešným profilům se stává internet velmi nebezpečným místem pro každého z nás, jelikož v určitých případech nevíme, s kým vlastně komunikujeme a koho necháváme sdílet své osobní informace. Na těchto veřejných profilech se skrývá i mnoho nebezpečných deviantů, kteří se snaží získat důvěru ve většině případů mladých lidí a nalákat je na nějaké zajímavé nabídky jako např. brigády apod. Takovýchto případů už bylo mnoho odhaleno; díky oblíbenosti sociálních sítí jich však stále přibývá.

1 Cíle a metodika bakalářské práce

Cílem bakalářské práce je rozebrat problematiku bezpečnosti na internetu a sociálních sítích. V práci budou jednak shrnuty informace získané z dostupné literatury, jednak v ní budou analyzovány výsledky výzkumu mezi uživateli internetu a sociálních sítí provedeného za účelem zjištění jejich informovanosti o riziku a nebezpečí, které jim hrozí, a navržena preventivní opatření pro zvýšení bezpečnosti.

Bakalářská práce bude rozdělena na dvě části. První část bude teoretická a druhá část bude praktická, v níž budou analyzovány výsledky výzkumu bezpečnosti na internetu a sociálních sítích. První část bakalářské práce se bude věnovat teorii o počítačové kriminalitě jako takové. Obsahem bude historie a vývoj počítačové kriminality v souvislosti s novými technologiemi až do současnosti, budou rozebrány druhy počítačové kriminality a jejich příčiny. V této části jde hlavně o základní informace o problematice, co vlastně počítačová kriminalita je a jaké má následky a dopady, ať už na samotného uživatele, nebo na celou společnost. Další kapitola se bude věnovat internetu, jeho historii a vývoji a jeho významu v dnešní společnosti. V poslední kapitole teoretické části bude charakterizován fenomén sociální sítě. Tato kapitola je pro bakalářskou práci velmi důležitá, protože bude hrát velkou roli při samotném výzkumu prováděném v souvislosti s bakalářskou prací. Obsahem opět bude historie a vývoj sociálních sítí, druhy sociálních sítí, bezpečnost a soukromí na sociálních sítích.

Druhá část bakalářské práce bude analyzovat výzkum problematiky bezpečnosti na internetu a sociálních sítích. Cílem práce je zjistit pomocí dotazníků předaných určitému okruhu uživatelů internetu a sociálních sítí rozsah používání internetu a sociálních sítí, stav ochrany při tomto používání a znalosti uživatelů, zejména jejich informovanost o riziku. Výzkum bude proveden tak, že určitému okruhu uživatelů internetu a sociálních sítí bude předán dotazník, v němž budou otázky zaměřené na zjištění, v jakém rozsahu internet a sociální sítě používají, co vědí o riziku používání internetu a sociálních sítí a jak se proti tomuto riziku chrání. V zájmu jednoduchosti budou účastnící výzkumu vybírat z nabídnutých možností odpovědi. Výsledky výzkumu budou analyzovány a budou z nich vyvozeny závěry o stavu informovanosti veřejnosti a v důsledku toho i míře rizika počítačové kriminality. V souvislosti s tím budou navržena preventivní opatření, která by problémy, s kterými se uživatelé setkávají, mohla pomoci z velké části snížit či úplně odstranit.

Práce bude zpracovaná jednak na základě dostupné literatury a informací získaných z internetu, jednak na základě praktických poznatků získaných z uvedeného výzkumu zaměřeného na danou problematiku.

2 Počítačová kriminalita

Pod pojmem počítačová kriminalita chápeme nelegální nebo nemorální činnost zahrnující užití dat získaných prostřednictvím výpočetní techniky nebo změnu těchto dat[1]. Tato kriminalita může být namířena přímo proti počítačům, jejich softwaru, hardwaru nebo datům v nich obsaženým, počítačovým sítím apod[2].

Charakter počítačové kriminality se neustále mění v důsledku vývoje počítačové techniky. Většina incidentů z oblasti počítačové kriminality však představuje činnosti, které jsou považovány za trestné již odedávna, například krádeže informací, špionáž, obchod s drogami, dětská pornografie. Počítačová kriminalita tyto trestné činy ale rozšiřuje o speciální dovednosti z oblasti softwarového inženýrství[3].

Vzhledem k rostoucí komplikovanosti a společenské nebezpečnosti počítačových zločinů jsou v mnoha zemích světa sestavovány a vyškolovány specializované týmy odborníků, kteří mají za úkol porozumět tomuto druhu kriminality a v rámci možností ho potírat. Díky ohromnému rozvoji informačních technologií není tento úkol vůbec jednoduchý. I přesto však jsou v činnosti těchto týmů zaznamenávány určité úspěchy, i když nelze vyloučit, že tento zločin zůstane nepotrestaný[4].

2.1 Historie počítačové kriminality

I když je počítačová kriminalita z pohledu dějin kriminality jev relativně nový, lze dobu jeho existence rozdělit na několik etap.

2.1.1 Pravěk (do roku 1981)

Za první „počítačový“ zločin je považován případ, který se stal ve Francii v roce 1801, tedy téměř 150 let před sestavením prvního skutečného počítače. Tkadlec Jacquard tehdy sestrojil jednoduché zařízení, které umožňovalo automatizovat a opakovaně provádět jednotlivé úkony používané při tkaní látky. Zaměstnanci Jacquardovy manufaktury byli z tohoto vynálezu tak šokováni, že ve strachu před ztrátou svého pracovního místa donutili sériemi sabotáží pana Jacquarda od dalšího vývoje jeho zařízení upustit.

[1] SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* VŠERS, 2010. s. 123.
[2] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 19.
[3] PROSISE, Ch., MADIA, K. *Počítačový útok. Detekce, obrana a okamžitá náprava*. Praha, 2002. s. 4.
[4] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 4.

V 70. letech 19. století je zaznamenáno z dnešního pohledu celkem nevinné jednání náctiletých chlapců obsluhujících telefonní ústředny, které spočívalo ve spojování k sobě nepatřících hovorů, jejich jakoby náhodném přerušování nebo chichotání se do telefonu. Poté se začaly množit stížnosti na toto jednání, a proto byli chlapci v roce 1878 nahrazeni dívkami, které byly odpovědnější a takovýchto jednání se nedopouštěly. Od počátku 20. století pak byly telefony běžně zneužívány k nelegálním aktivitám jako například k domlouvání mezi zločinci.

Vynález telefonu, který se stal prvním prostředkem elektronické komunikace, dal vzniknout také dalšímu závažnému fenoménu. Protože první způsoby komunikace dvou počítačů mezi sebou vedly přes telefonní linku, umožnil právě telefon vznik toho, co bylo později označeno termínem kyberprostor. Jedná se o síť, neidentifikovatelný prostor mezi počítači, kde se odehrává veškeré dění na síti, zábava, komunikace, obchod a také zločiny. Na počátku všeho byl tedy obyčejný telefon, zatímco druhá komponenta vzniku Kyberprostoru – osobní počítač, byla sestrojena až o více než padesát let později[5]. Kyberprostor je zvláštní virtuální svět, který vypadá jakoby žil svým vlastním životem[6].

Počítačový věk se zrodil dne 14. února 1946. Tehdy byl na univerzitě v Pennsylvánii vyroben první elektronický počítač s názvem ENIAC a brzy následovaly další. Takovéto počítače ovšem byly velkých rozměrů (zabíraly téměř celou místnost) a jejich cena dosahovala desítek tisíc dolarů. Musely být provozovány ve speciálních místnostech s kontrolovanou teplotou a mělo k nim přístup jen pár vyvolených programátorů. Rozhodně se ještě nedalo hovořit o možnostech jejich kriminálního zneužití.

Právě v těchto dobách se zrodilo slovo, které dnes slyšíme v souvislosti s počítačovou kriminalitou velmi často. Programátoři, kteří na těchto velkých počítačích pracovali, se museli často vypořádat s nepříliš dobře fungujícími programy, přičemž byli odkázáni na svépomoc. Zásahy do programů, které měly zajistit, aby počítače fungovaly lépe a efektivněji, se označovaly anglickým slovem „hacks“. Z toho vznikla tolik používaná slova hacking a hacker. Úloha tehdejších hackerů byla pozitivní,

[5] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 18–19.
[6] LAPÁČEK, J. *Internet pro úplné začátečníky.* Praha, 2000. s. 13.

protože zasahovali do programů, aby mohly být lépe využívány. Časem termín hacker změnil smysl a stal se termínem pro označení pachatele útoků proti počítači.

Z hlediska porušování autorských práv je významnou skutečností masové rozšíření kotoučového magnetofonu v průběhu 60. let, který poprvé umožnil kopírování hudebních nahrávek. Tato technologie sice nemohla na tehdejší úrovni sloužit rozvoji počítačové kriminality, ale znamená počátky činnosti, která se v důsledku rozvoje internetu stala jedním z nejvýraznějších druhů počítačové kriminality – masového porušování autorských práv[7].

2.1.2 Středověk (1981 – 1994)

Za počátek nové éry v oblasti informačních technologií, a tedy i v oblasti počítačové kriminality, lze označit uvedení počítače typu IBM PC na trh. Došlo k tomu 12. 8. 1981 a znamenalo to obrovskou změnu. PC vytvořilo předpoklady pro to, aby se počítač stal běžnou součástí každé domácnosti a byl využíván při řadě lidských činností. Stavebnicové uspořádání počítače umožňovalo jeho snadné rozšíření o nové součásti; cena tohoto typu počítače byla sice z počátku vyšší, ale postupem doby se stala přijatelnou.

V 80. letech došlo také konečně k výše zmiňovanému spojení počítače a telefonní linky. Stále více počítačů se prostřednictvím modemů začalo propojovat do sítí a došlo tak k rozšíření předchůdce dnešního internetu v podobě systému BBS. Šlo většinou o servery s textovým rozhraním, na které se připojovalo přímo volbou čísla. Zprostředkování přístupu pomocí Internet Service Providerů (ISP) se začalo využívat až později.

Konec období středověku poznamenala především změna typického pachatele počítačového zločinu. Zatímco v předchozí době je jím „počítačový nadšenec‘‘, pro nějž proniknout do systému představuje intelektuální výzvu, tak konec středověku znamená profesionalizaci. Cílem již není získat slávu, ale dosáhnout finančního zisku. Počítače již nejsou neobvyklými stroji pro studenty univerzity a nadšence, nýbrž masově rozšířenými obchodními nástroji, a jejich ekonomický význam roste. Tím se mění i počítačová kriminalita.

[7] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 20–22.

Mnoho zajímavého se odehrálo v období středověku také v další oblasti počítačové kriminality, a to v počítačovém pirátství. Objevil se nový nástroj, který výrazně zdokonalil aktivity počítačových pirátů – médium pro digitální záznam dat, tedy kompaktní disk neboli CD. Napříště již nebylo třeba používat k záznamu dat pásky, která byla náchylná k poškození a měla malou kapacitu. CD se svou na tehdejší dobu ohromnou kapacitou záznamu 650 megabajtům proniklo rychle nejen do domácností, ale také do pirátských dílen. Kolem poloviny 80. let se CD začalo využívat v oblasti hudebních nahrávek. Až později, od začátku 90. let došlo k jeho využití pro účely uchování dat. Tehdy byla do prodeje uvolněna mechanika CD-ROM (Compact Disk Read Only Memory), která sloužila ke čtení CD nosičů[8]. Tato počítačová mechanika se stala začátkem 90. let symbolem multimédií[9].

U této technologie byl jen jeden negativní faktor, a to, že zařízení pro digitální záznam na CD bylo zpočátku velmi drahé. To se změnilo až kolem poloviny 90. let. Tehdy byla dána do prodeje mechanika CD-R, která uměla nejdříve jednorychlostně, později i vícerychlostně zaznamenávat neboli vypalovat data na CD. Snížení cen a masové rozšíření těchto mechanik, které dovolilo skoro každému majiteli počítače se stát možným pirátem, nastalo až později a je jedním z významných mezníků novověků počítačové kriminality[10].

2.1.3 Novověk (1994 – dodnes)

Období novověku se vyznačuje především masovou rozšířeností počítačů, a to zejména těch na platformě PC s operačním systémem Microsoft Windows. Počítače se stávají každodenní součástí života a vyvíjí se i software pro ně[11]. „*Software je počítačový program obsahující sekvence instrukcí, které jsou vykonávány procesorem počítače, je: digitální, automatizovaný, modulární, proměnlivý a překódovaný*“[12].

V této době též dochází k rozšíření sítí typu internet a především jejich nejviditelnější podoby – grafického prostředí WWW (World Wide Web). Internet přestává být jen záležitostí akademických kruhů, začínají na něj vstupovat podnikatelské subjekty a stává se obchodním nástrojem, čili do něj proudí peníze. To

[8] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 22–29.
[9] PAVLÍČEK, A., *Nová média a web 2.0*. Praha, 2007. s. 41.
[10] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 29.
[11] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 32.
[12] PAVLÍČEK, A., *Nová média a web 2.0*. Praha, 2007. s. 35.

samozřejmě přitahuje počítačové podvodníky, jejichž typický obraz se ale mění. Zatímco v dobách akademické sítě to byli „počítačoví nadšenci“, nyní jde o profesionály, jejichž prvotním motivem je dosažení zisku. Naštěstí zatím nedošlo k ovládnutí počítačového podsvětí organizovanými zločineckými skupinami. Internet také nelze nikdy zcela ovládnout a organizovaný zločin potřebuje trh ovládat bezezbytku.

Je logické, že masové rozšíření počítačů vede k rozšíření počítačové kriminality. Již proto nejde o ojedinělé činy počítačové kriminality, ale o určité mezníky. Jedním z nich je případ Citibank s ruským matematikem Vladimirem Levinem, jakožto vedoucím skupiny hackerů, kde došlo k uloupení 10 miliónů dollarů. Tento případ ukázal, kam se bude počítačová kriminalita především ubírat.

Virové hrozby 1999 – 2001. Hrozba počítačových virů se stává s masovým rozšířením internetu do firem i domácností stále větším nebezpečím. Už v roce 1988, kdy Robert Morris vypustil do světa svého červa, došlo k postižení stovek počítačů na celém světě. O více než deset let později ovšem viry zasahují milióny počítačů, působí obrovské škody hospodářským subjektům a mnohdy zapříčiňují i výpadky celých sítí. Významným distribučním kanálem počítačových virů se stala elektronická pošta. V případě virů obsažených v programech jsou nejvíce ohroženi domácí uživatelé, neboť namísto originálních a legálních programů velmi často používají software z pochybných zdrojů.

Jestliže za zlatou éru hackingu lze považovat léta osmdesátá, zlatá éra počítačového pirátství rozhodně přichází ve druhé polovině devadesátých let. Do prodeje se dostává zařízení na vypalování dat na CD, mechanika CD-R (vypalovačka). Jeho cena se stává natolik příznivou, že je v krátké době dostupné každému majiteli běžného PC. A pro ty, kdo toto zařízení nevlastní, začínají vznikat „vypalovací centra‘‘, která za malý poplatek zákazníkovi vypálí donesená data na CD, aniž by se někdo příliš zajímal o jejich legalitu. Počítačovým pirátům navíc pomáhá i rozvoj internetu, jehož stálé rostoucí přenosová rychlost umožňuje rychlou výměnu dat i mezi kontinenty[13].

[13] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 32-41.

2.2 Formy počítačové kriminality

2.2.1 Tradiční jednání

Do počítačové kriminality řadíme i určité trestné činy, které existovaly už před vznikem informačních technologií, ale nyní se působením informačních technologií jejich podoba změnila[14].

a) Podvody a zpronevěry

Právě podvody a zpronevěry se začaly s rozšířením informačních technologií do běžného života objevovat ve značném rozsahu. Pochybné podvodné aktivity jsou v reálném světě již překonané, ale v kyberprostoru se rozjíždí s novou silou. Na internetu se objevují podvody jako podvodné e-shopy, vylákání peněz za neexistující služby apod.

Výjimkou nejsou ani podvodní finančníci, kteří slibují zázračné zisky z různých obchodů s měnami, komoditami nebo cennými papíry, a nalákají tak důvěřivé oběti. Tito podvodní finančníci mívají amatérské stránky na freewebech a honosí se vysokými ratingy od agentur, jejichž jména v neinformovaném světě navodí pocit důvěryhodnosti, přestože bývají ve skutečnosti vymyšlená. Je až nepochopitelné, kolik lidí se v dnešní době nechá na podobné nabídky nalákat a později se diví, že přijdou o své peníze.

Nezastupitelné místo má v této kategorii také počítačová zpronevěra. Dochází k ní tehdy, když například zaměstnanec instituce (banky apod.), který má možnost přístupu k finančním prostředkům takové instituce, zneužije počítač k tomu, aby využil prostředky ke svému osobnímu obohacení. Další skupinu v této oblasti představují bankovní podvody. Počítačové systémy bank a kanály elektronického bankovnictví jsou zpravidla zabezpečeny na takové úrovni, že průniky zvenčí jsou ojedinělé. Většina útoků proto přichází zevnitř, to znamená od zaměstnanců bank s přístupovými právy, administrátorů systému apod. Snížení rizika takových podvodů je věcí bezpečnostních opatření a nastavení procesů uvnitř bank[15].

[14] SELIMOVIČ, M. *Zcu.cz.* Kriminalita a web [online]. 1991-2013 [cit. 28. Prosince 2012]. Dostupné na WWW: <http://home.zcu.cz/~mselimov/ins/Druhy.html>

[15] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 60-62.

Jednání toho druhu lze podle trestního zákona č. 40/2009 Sb., trestní zákoník ve znění pozdějších právních předpisů (dále jen „TZ“) postihnout jako podvod dle § 209 TZ, zpronevěra dle § 206 TZ a provozování nepoctivých her a sázek dle § 213 TZ[16].

b) Padělání

I staré řemeslo padělatelů a penězokazů umožňují informační technologie zásadním způsobem usnadnit. Zatímco v dřívějších dobách bylo padělání peněz či veřejných listin úkolem pro nejzručnější kreslíře a rytce, v dnešní době jde o to, naučit se ovládat příslušný software a investovat do kvalitní technologie tisku. Nejnovější grafické programy dokážou v tomto směru skutečné zázraky. Totéž lze říci o moderních laserových a sublimačních tiskárnách, případně barevných kopírkách. Jediným problémem tak zůstává použití správného druhu papíru s odpovídajícím složením, ale ani to nemusí být pro padělatelské gangy nepřekonatelnou překážkou. Tato skutečnost klade maximální nároky na ochranné prvky peněz, cenin a veřejných listin, které se musí neustále zdokonalovat, aby dokázaly čelit ohrožením plynoucím ze stále lepší reprodukční technologie[17].

Jednání toho druhu lze podle trestního zákoníku postihnout jako padělání a pozměňování peněz dle § 233 TZ nebo padělání, pozměnění veřejné listiny dle § 348 TZ a výroba a držení padělatelského náčiní dle § 236 TZ[18].

c) Pomluvy a elektronická msta

Také šíření pomluv se v elektronickém věku dostalo na novou úroveň. Pachatelé tohoto trestného činu získali vznikem internetu nástroj s mnohem větší účinností, než měly v minulosti hromadné sdělovací prostředky.

Tuto trestnou činnost může spáchat velmi efektivně v podstatě každý, kdo má přístup do počítače a internetu. Oblíbeným způsobem spáchání takového trestného činu je například předání údajů o oběti do erotických seznamovacích služeb. Oběť je pak po nějakou dobu obtěžována nechtěnými erotickými telefonáty, v horším případě i nežádoucími návštěvami. I v České republice došlo k případu, kdy se takového jednání dopustila vůči soudkyni poražená strana soudního sporu, která nebyla s jejím rozhodnutím spokojena. Pachatelé těchto trestných činů bývají většinou odhaleni

[16] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 89–92.
[17] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 4 62-63
[18] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 100–144.

zejména proto, že policie vždy v první řadě prověřuje osoby, které mohou mít k takovému jednání motiv.

Další možností je, že pachatel vědomě rozšiřuje o oběti prostřednictvím internetu nepravdivé informace, které jsou způsobilé oběť poškodit, ať už v osobním nebo profesním životě[19]. Skutková podstata příslušná k tomuto činu je pomluva dle § 184 TZ[20].

d) Elektronické výpalné a vydírání

I v případě trestného činu vydírání došlo ke změnám podmínek, za nichž je tento čin v prostředí moderních informačních technologií páchán. Vyskytují se případy tzv. elektronického výpalného, které spočívají v tom, že majitelé systémů připojených k internetu jsou zastrašování hrozbami průniku do systému, hrozbami zničení či zneužití dat atp. Jelikož u žádného systému asi není jistota dokonalého zabezpečení, mnohé instituce raději zaplatí e-výpalné, aby se hrozby nezrealizovaly. Tento způsob vydírání je mimořádně nebezpečný, neboť se tím vlastně dostává do počítačového podsvětí organizovaný zločin. Naštěstí tyto případy nejsou zatím příliš časté, ale lze se obávat jejich postupného nárůstu[21]. Jednání toho druhu lze podle trestního zákoníku postihnout především jako vydírání dle § 175 TZ[22].

e) Hoaxes

Pod pojmem hoaxes se rozumí šíření nepravdivých varování, více či méně uvěřitelných informací a vyvolávání paniky prostřednictvím internetu. Zatímco dříve, kdy mohly být takové informace šířeny jen ústně nebo prostřednictvím bulvárních médií, nebyl jejich dosah tak rozsáhlý, nyní se díky internetu stává doslova celosvětovým a správně napsaná poplašná zpráva dokáže skutečně ovlivnit chování mnoha uživatelů internetu.

Z hlediska obsahu jde o různé druhy zpráv. Pravděpodobně nejčastější, ale ve skutečnosti poměrně málo nebezpečná jsou varování o počítačových virech. Jde o zprávu napsanou tak, aby vypadala jako od důvěryhodné počítačové firmy, antivirové laboratoře apod. Tím zpráva vyvolává zdání, že je pravdivá. Přitom informuje uživatele,

[19] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 64–65.
[20] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 81.
[21] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 65.
[22] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 77.

co hrozného jim může ten zcela nový, fatální a žádným existujícím antivirovým programem neodhalitelný virus s počítačem provést[23].

Hoaxes jsou určitým druhem spamu, ale druhem specifickým: jejich cílem není přimět nás například ke koupi určitého zboží nebo služby, nýbrž působí na naše emoce, jsou častěji antireklamou než reklamou, navíc se šíří lavinovitě dál, protože jsou napálenými uživateli internetu dále rozmnožovány. Hoaxes jsou svým způsobem nebezpečnější než klasické reklamní spamy. Reklamy jsou vždy částečně předstíráním, ale nikdy otevřenou lží, takže nemohou být trestnou činností. Prostředky, které reklamy používají, jsou sice rafinované, ale jejich úmysl je vždy zřejmý. Spamy je mnohem snazší smazat bez čtení; jde o rozhodnutí nepodlehnout reklamě. „*Hoaxes nesvádí, ale varují, nenabízejí požitky, ale prosí o pomoc, tváří se jako akt mezilidské solidarity, která živí jejich přenos, jejich smyšlený charakter není často na první pohled zřejmý*“[24].

Pokud může taková šířená zpráva způsobit, že na jejím základě vznikne znepokojení mezi větším počtem lidí, naplňuje skutkovou podstatu trestného činu šíření poplašné zprávy dle § 357 TZ[25].

2.2.2 Nová jednání

Se vznikem a rozšířením moderních informačních technologií se objevily také nové trestné činy. Mezi tato nová jednání patří též počítačové pirátství neboli trestné činy porušující autorská práva, i když existovaly už před nástupem informačních technologií, ovšem ne v tak rozsáhlé míře. Rozlišujeme několik druhů těchto jednání[26].

a) Hacking

Hacking v původním pojetí lze obtížně označit za trestný čin, neboť nelze vyčíslit škodu, která tímto jednáním byla způsobena. Někdy ani správce systému netuší, že mu hacker do systému pronikl. Motivací prvních hackerů nebylo způsobit někomu škodu, ale pouze zvítězit nad technikou a získat obdiv ostatních hackerů. Zjednodušeně

[23] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 68.

[24] ČINČERA, J. *Ikaros.cz.* Mha přede mnou, mha za mnou - hoaxes útočí na lidskou solidaritu [online]. 2002-2013 [cit. 16. Ledna 2013]. Dostupné na WWW: <http://www.ikaros.cz/node/931>.

[25] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 148.

[26] SELIMOVIČ, M. *Zcu.cz.* Kriminalita a web [online]. 1991-2013 [cit. 28. Prosince 2012]. Dostupné na WWW: <http://home.zcu.cz/~mselimov/ins/Druhy.html>.

lze hacking definovat jako proniknutí do počítačového nebo řídícího systému jinou než standardní cestou s tím, že se obejde nebo prolomí jeho bezpečnostní ochrana[27].

Hackeři vždy provádějí před pokusem o jakýkoliv manipulační útok průzkum. Tím získávají informace o jakémkoliv subjektu, který chtějí při své činnosti zneužít. Čím více informací mají, tím spíš jsou při své činnosti úspěšní[28].

Nabourání do sítě nebo konkrétního systému je prakticky možné vždy nějakou chybou v softwaru. Bylo by však nesprávné svalovat vinu na programátory, protože ti dělají jen to, co po nich jejich zaměstnavatel a trh žádají – v krátkých termínech vytvářejí programy, které mají mnoho funkcí. Teprve v posledních několika letech se začínají vedle požadavků na velký počet funkcí objevovat i požadavky na vyšší bezpečnost, takže dodavatelé i programátoři se dnes musí snažit jak splnit nové nároky na vývoj, tak při své činnosti docílit zisku[29].

Jednání tohoto druhu lze podle trestního zákoníku postihnout jako trestný čin vyzvědačství dle § 316 TZ nebo trestný čin ohrožení utajované informace dle § 317 TZ[30].

b) Spamming

Pod pojmem spamming se rozumí zasílání nevyžádané elektronické pošty, která má obvykle reklamní obsah. Tento typ nepříjemného přímého marketingu, který obtěžuje zejména v případech, kdy uživatel platí poplatek podle doby připojení nebo objemu přenesených dat, se objevil spolu se vznikem elektronické pošty. Spammeři získávají elektronické adresy uživatelů nejrůznějším způsobem, přičemž nejběžnějším jsou různé www konference, IRC, ICQ, registrační stránky pro služby ,,zdarma“ nebo obdobné komunikující objekty. I když existuje celá řada programů, které spam dokážou odfiltrovat, nejsou trvale účinné, protože spammeři tento mechanismus znají a dokážou ho přelstít tím, že změní adresu odesílatele. V poslední době jsou pro filtraci spamu používány tzv. Bayesovské filtry, které jsou založeny na vyhodnocení pravděpodobnosti spamu na základě analýzy struktury příslušné zprávy. Spam je velmi obtěžujícím jevem

[27] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 102.

[28] HATCH, B., LEE, J., KURTZ, G. *Linux hackerské útoky. Bezpečnost Linuxu – tajemství a řešení.* Praha, 2002. s. 171.

[29] HARRIS, S., HARPER, A., EAGLE., NESS, J., LESTER, M. *Manuál hackera*. Praha, 2008. s. 36.

[30] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 132-133.

spojeným s elektronickou komunikací. K jeho potlačení byla vymyšlena mnohá opatření a návrhy, ale přesto je jeho narůst téměř nezastavitelný[31].

Právní názory na možnosti postihnutí spamu nejsou jednotné. Existuje např. názor, že pokud bude možno z adresy jednoznačně identifikovat příjemce, jde o trestný čin neoprávněné nakládání s osobními údaji dle § 180 TZ[32].

c) Warez

Moderní počítačové pirátství, které je doprovodným jevem používání informačních technologií a rozšiřuje se s rozmachem internetu, je většinou skupinovou záležitostí. Jedna část pachatelů pracuje na prolamování ochranných prvků programových produktů, kdežto druhá část se specializuje na jejich šíření pomocí www serverů a získávání financí na jejich provoz tím, že umisťuje reklamu na pornografické servery nebo servery, které mají erotický obsah. Tato reklama obvykle nezkušeného uživatele zahltí přívalem samovolně se otevírajících oken, aniž by se dostal k tomu, co hledal.

Warezy jsou spíše jakýmsi pozůstatkem minulosti. Dnes jsou používány pro šíření tzv. cracků, to znamená programů umožňujících zrušení ochrany u programových produktů, jejichž plné verze lze stáhnout z internetových stránek dodavatele nebo je získat z reklamních CD, avšak jen na omezenou dobu[33]. Daleko rozšířenější jsou dnes ale programy pro sítě peer-to-peer, které představují jednoduchý způsob, jak sdílet soubory. Lze je též dobře využít pro stahování hudby, filmů nebo programů[34].

Postihnout nelegální obsah šíření v síti peer-to-peer je samozřejmě daleko složitější, než když je k šíření použit server warez. Z pohledu trestního práva je vyhodnocení takovéhoto jednání jednoznačné. Jde o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ[35].

[31] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 104.

[32] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 79.

[33] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 105–106.

[34] BEZPEČNÝ INTERNET. *Rady pro vaši bezpečnost na internetu* [online]. 2008-2013 [cit. 10. ledna 2013]. Dostupné na WWW: <http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/site-peer-to-peer.aspx>.

[35] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 114.

d) Cracking

S trestnou činností označovanou jako hacking a warez je neoddělitelně spjata další společensky nebezpečná činnost označovaná jako cracking. Jde o prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů za účelem jejich neoprávněného použití. Cracking používá celou řadu metod počínaje prostým debutováním spuštěného programu a konče tzv. reverse engineering. Cracking je často používaná metoda při průniku do systému, přičemž jeho cílem není zprovoznit program chráněný softwarovým nebo hardwarovým klíčem, ale zjistit informace důležité pro umožnění neoprávněného přístupu do cílového systému. Nejčastějším typem je tzv. ,,password cracking", tj. zjišťování hesla pro přístup do systému. Password cracking zahrnuje mnoho metod, počínaje snahou uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použitím hrubé síly při zkoušení všech možných kombinací znaků, které mohou přicházet v úvahu, až po sofistikované algoritmy, které se snaží o zpětnou rekonstrukci kombinace znaků.

Z hlediska trestního práva může být tato trestná činnost kvalifikována různým způsobem. Případ, kdy tomu, kdo je vlastníkem systému, vůči němuž byl útok crackingem prováděn, nevznikla prokazatelná škoda, nemusí být vůbec jako trestný čin hodnocen[36]. V ostatních případech může jít o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ nebo poškození záznamu v počítačovém sytému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ[37].

e) Sniffing

Podobně jako cracking, i sniffing má za cíl především usnadnit jinou nelegální činnost. Jednoduše lze sniffing definovat jako odchytávání komunikace po počítačové síti, především internetu, subjektem, který není adresátem této komunikace. V důsledku toho může neoprávněná osoba získat veškerý obsah určité nešifrované komunikace, přístupová jména a hesla, znění e-mailů, soubory posílané po síti apod. Obranou proti sniffingu je především důsledné šifrování komunikace po internetu. Informace získané sniffováním lze pak využít k průnikům do systému, případně i k vydírání určité osoby apod.[38] V dnešní době existují desítky nástrojů, které slouží k odposlouchávání a nesou

[36] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 106.
[37] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 100.
[38] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 74.

název Sniffer. Sniffer patří k nejoblíbenějším komerčním nástrojům určeným k odposlouchávání[39].

Z hlediska trestního práva lze sniffing kvalifikovat jako porušení tajemství dopravovaných zpráv dle § 182 TZ[40]. Dopadení pachatele takového činu je ale velice složité a rovněž tak je i složité i dokazování. Výjimkou jsou případy, kdy bude takové odposlouchávání soustavně provádět soukromý subjekt s cílem získání určitých informací, které následně využije k dalším krokům vůči odposlouchávanému subjektu. V tom případě bude použití takových informací samo o sobě umožňovat obvinění ve smyslu výše uvedeného paragrafu.

V této souvislosti je nutno též připomenout, že internetové adresy, záznamy o provozu sítě a ostatní záznamy umožňující jednoznačně identifikovat osobu, ke které se vztahuje nějaká činnost na síti, jsou chráněny ještě podle dvou zákonů – telekomunikačního zákona a zákona o ochraně osobních údajů. Neznalý správce sítě, který tyto údaje poskytne třetí osobě, se tak vystavuje postihu podle výše citovaného ustanovení trestního zákona.

Jiná situace je tehdy, když poskytnutí takových údajů požaduje orgán policie. Zde záleží na tom, zda organizace, které síť patří, je poskytovatelem služby elektronických komunikací ve smyslu zákona o elektronických komunikacích. Pokud ano, je správce sítě povinen policii požadované údaje poskytnout pouze tehdy, když má policie k dispozici povolení soudu k poskytnutí takovýchto údajů. Pokud organizace, které síť patří, není poskytovatelem služeb elektronických komunikací, je správce sítě povinen policii požadované údaje poskytnout, a to na základě zákona o policii.

f) Cybersquatting

Názvem Cybersquatting se označuje donedávna legální blokování internetových domén. Zaregistrování domén s názvem velkého podniku, instituce nebo produktu a spekulace s prodejem tohoto jména se již tolik nevyskytuje. Svůj význam měl cybersquatting v době, kdy velké společnosti na internet vstupovaly, nebo se rozhodovaly na něm uvést své produkty. Dnes se spíše než porušování práv vyplývajících z ochranné známky vyskytuje tzv. nekalá soutěž. K té může dojít např.

[39] SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* Praha, 2002. s. 163.
[40] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 80.

tehdy, kdy bude zaregistrována doména s názvem známého produktu a pod ní bude běžet internetový obchod s tímto produktem[41].

Problematika registrace domény je velmi široká, ale patří do oblasti soukromého práva[42]. Z trestně právního hlediska by za jistých okolností mohlo výše uvedené jednání naplnit skutkovou podstatu trestného činu porušení předpisů o pravidlech hospodářské soutěže dle § 248 TZ nebo porušení práv k ochranné známce a jiným označením dle § 268 TZ[43].

g) Phishing

Phishing je druh internetového podvodu, který je páchán tak, že jsou z uživatelů internetového bankovnictví vylákávány přístupové údaje k účtům a pak zneužity pro obohacení pachatelů. K získání těchto důvěrných informací pachatelé využívají podvodné e-maily, které vyvolávají dojem, že jsou odeslány přímo z banky, a které se snaží přesvědčit uživatele, aby kliknul na určitý odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde je po něm požadováno, aby sdělil své přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně sdělí, poskytne je podvodníkům, kteří je následně využijí ve svůj prospěch[44].

Phishing představuje podskupinu kategorie spamu. Phishing je známý už přes 15 let – poprvé se objevil v roce 1995 u America Online (poskytovatel internetových služeb). Byly vymyšleny programy, které automatizovaly proces phishingu v souvislosti s údaji o účtech a platebních kartách. Phishing se tehdy nepoužíval v oblasti elektronické pošty, nýbrž u Internet Relay Chat (chatovaní po internetu) nebo systému upozorňování na nové zprávy, používaného u America Online. Pachatelé napodobovali administrátora a sdělovali obětem, že se objevily komplikace s vyúčtováním a že je třeba, aby uživatel znovu zadal údaje o platební kartě a přihlašovací údaje. Tehdy byla tato metoda docela úspěšná, protože spojení domácího osobního počítače a připojení k internetu bylo prakticky novinkou. Neměla však takový dosah jako současný phishing[45].

[41] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha, 2007. s. 106–107.

[42] MATĚJKA, M. *Počítačová kriminalita*. Praha, 2002. s. 75.

[43] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 100-113.

[44] DŽUBÁK, J. *Hoax.cz.* Phishing [online]. 2008-2013 [cit. 30. Prosince 2012]. Dostupné na WWW: <http://www.hoax.cz/phishing>.

[45] JAMES, L. *Phishing bez záhad*. Praha, 2007. s. 28.

Jednání tohoto druhu lze podle trestního zákoníku postihnout jako krádež dle § 205 TZ[46].

2.3 Kyberšikana

Kyberšikana je specifický druh šikany, který využívá nástroje moderních komunikačních technologií jako internet, mobilní telefony a případně další, aby ublížil či zesměšnil jinou osobu. Kyberšikana může mít různou formu. Agresor může oběti zasílat výhružné a kruté e-maily a SMS zprávy, nebo ji obtěžovat výhružnými telefonáty, případně přes chat. Další formou kyberšikany je vytváření webových stránek, které různými způsoby (verbálně, graficky, zvukově apod.) oběť uráží a zesměšňují. Patří sem také případy, kdy jsou obrázky, fotografie a videonahrávky, na nichž je oběť zesměšňována, zasílány on-line lidem z okolí oběti, nebo případy, kdy jsou na internetu vyvěšeny pornografické fotografie s tváří oběti. Vyskytují se i případy, kdy agresoři pod jménem oběti zasílají ostatním na internetu vulgární a obtěžující zprávy, protože získají hesla a identifikační údaje oběti [47].

Kyberšikana se od šikany, kdy jsou oběť a agresor v přímém kontaktu, liší tím, že si agresor může zachovat od svých obětí určitý odstup. Ten mu umožňuje určitou anonymitu a pocit, že nebude odhalen. Zároveň je pro něj snazší zapomenout na své chování a neuvědomovat si jeho dosah, protože vlastně nevidí, co způsobil. Negativní důsledek to má ovšem pro oběť, která tím, že nezná pachatele, může ztratit důvěru k ostatním lidem.

Velikost internetového světa poskytuje kyberšikaně ohromné možnosti. Jediný obrázek, který někdo uložil na Facebook, se může zanedlouho rozšířit mezi miliony uživatelů počítačových sítí. A přitom uživatel, který takový obrázek pošle dál, nemusel mít takové šíření vůbec v úmyslu.

Další odlišností od šikany, k níž dochází v přímém kontaktu mezi agresorem a obětí, je to, že kyberšikana může probíhat kdykoli během celého dne a proniknout i do

[46] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha, 2011. s. 88.
[47] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 37.

míst, která byla dříve považována za bezpečná. Toto může oběť psychicky značně poškodit, protože získá dojem, že nemůže nikomu věřit a nikde není v bezpečí[48].

2.3.1 Kyberšikana a legislativa

Kyberšikana stejně jako šikana není podle české právní úpravy trestným činem. Takovéto chování ale může naplňovat skutkovou podstatu některých trestných činů, například vydírání, vyhrožování, nebezpečné pronásledování (stalking) nebo útisk.

Protože kyberšikana se vyskytuje i mezi žáky i studenty, je dnes již předmětem školské legislativy. Základní informace jsou obsaženy v Metodickém pokynu MŠMT č. j. 24 246/2008-6, který upravuje mimo jiné i zásady prevence a řešení kyberšikany[49].

2.3.2 Prostředky kyberšikany

a) Webové stránky

Webové stránky nabízejí mnoho možností využití. Díky jim můžeme číst zprávy z celého světa, nakupovat, seznamovat se, prohlížet si objekty našeho zájmu jako například vzdálená místa, hrát hry a mnoho dalšího. Ale existují i webové stránky, které jsou vytvořeny přímo za účelem kyberšikany. Příkladem je situace, kdy jsou na webové stránky umisťovány fotografie či videa oběti, které jsou úmyslně zesměšněny nebo měněny v provokativním sexuálním stylu. Na takovéto webové stránce může agresor zveřejnit i jméno, adresu a další informace o oběti, která se tak může stát cílem útoků, ať už např. prostřednictvím e-mailů, nebo přímého kontaktu od naprosto neznámých osob[50].

b) Textové zprávy

Ke kyberšikaně dochází textovými zprávami, které zpravidla mají výhružný nebo útočný obsah. Kyberšikana probíhající prostřednictvím textových zpráv může mít i takovou podobu, že agresor zasílá oběti opakovaně velké množství textových zpráv. Vzhledem k tomu, že jsou k dostání SIM karty „na jedno použití“, které může agresor stále vyměňovat, oběť nemá šanci zjistit, kdo ji takto obtěžuje[51].

[48] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 32.
[49] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 13-14.
[50] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 40-41.
[51] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 33.

c) E-mail

I e-mail lze využít pro zasílání útočných a výhružných zpráv. Protože e-mailové účty lze vytvořit velice snadno, mohou agresoři posílat takové zprávy buď pod pseudonymem, nebo pod cizí identitou a vůbec se nemusí bát, že budou odhaleni[52].

d) Sociální sítě

Sociální sítě umožňují, aby se prostřednictvím internetu sdružili lidé, kteří by se jinak fyzicky nemohli setkat, ale také ti, kteří se běžně scházejí i mimo on-line prostředí[53]. Tyto služby poskytují snadné a jednoduché spojení jednotlivých osob, takže mohou společně sdílet např. fotografie nebo zábavu. Ovšem pokud se na sociálních sítích neuplatní bezpečnostní pravidla, mohou být zneužity k rozšiřování pomluv a nepravdivých zpráv. Zejména pro děti spočívá nebezpečí v tom, že v zájmu „být IN" přijmou „žádost o přátelství" od člověka, kterého vůbec neznají. Tím mu poskytnou přístup k osobním informacím, což je velmi rizikové.

Na sociálních sítích navíc lze vytvořit si vcelku bez obtíží falešný profil a kontaktovat oběť kyberšikany pod cizí či smyšlenou identitou. To umožňuje agresorům sledovat svou oběť, přičemž sami zůstanou v anonymitě[54].

Jako příklad lze uvést následující:

„Jedna z nejznámějších českých zpěvaček a idol dospívající mládeže Ewa Farna má jen na Facebooku minimálně deset profilů, které se tváří jako oficiální. O čem to svědčí? Především o tom, že identita člověka je na internetu pojem zatraceně relativní. Pobyt v říši, kde se kdokoliv může vydávat za kohokoliv, pak může být nebezpečný zejména pro děti, u kterých má důvěřivost navrch před ostražitostí"[55].

e) Instant messaging

IM je v dnešní době velmi využívanou internetovou službou, která umožňuje svým uživatelům sledovat, kdo z jejich přátel je právě on-line, a podle potřeby jim

[52] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 34.

[53] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 41.

[54] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 34.

[55] VAŇURA, M. *Novinky.cz.* Děti na internetu chytají do pastí falešné celebrity [online]. 2012 [cit. 1. března 2013]. Dostupné na WWW: < http://www.novinky.cz/internet-a-pc/272272-deti-na-internetu-chytaji-do-pasti-falesne-celebrity.html>.

posílat zprávy nebo jiné soubory, chatovat a i jinak komunikovat. Hlavní výhodou oproti používání e-mailu je princip odesílání a přijímání zpráv v reálném čase[56].

V České republice se pro tuto formu komunikace používá nejčastěji ICQ nebo Skype. Během komunikace v reálném čase může dojít k tomu, že diskuze se změní v útok na vybranou oběť[57].

[56] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 42.

[57] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 34.

3 Internet a sociální sítě

3.1 Internet

Internet je celosvětová počítačová síť, jejímž cílem je zaslání dat uživateli na jeho žádost. Internet je všude kolem nás a lze se na něj připojit z kteréhokoliv místa na světě. Součástí internetu je především síť velkých počítačů, takzvaných serverů, které jsou propojeny datovými kabely s vysokou průchodností. Po nich proudí informace, které si lze představit jako nuly a jedničky. Pohybují se velmi rychle, a proto se internetu říká i informační dálnice. Kromě serverů, které jsou součástí internetu nepřetržitě a měly by být stále v provozu, tvoří internet ještě milióny osobních počítačů, připojujících se k němu vždy jen na určitý čas[58].

Často máme pocit, jako by byl internet součástí našeho života odjakživa. Pro mnohé z nás je velmi obtížné si jen představit, že by nemohli kontaktovat osoby pomocí e-mailů, vyhledávat informace týkající se různých oblastí pouze pomocí klíčového slova zadaného do internetového vyhledávače, nakupovat po celém světě prostřednictvím internetových obchodů, volat a vidět člověka nacházejícího se třeba v daleké zemi a provozovat mnoho dalších aktivit, které nám internet nabízí a umožňuje[59].

3.1.1 Historie internetu

Počátek internetu spadá do šedesátých let dvacátého století, kdy se americká armáda snažila zajistit bezproblémovou komunikaci armádních počítačů rozmístěných po celém území USA i za situace, že část těchto počítačů bude vyřazena z provozu. Pracovníci RAND Corporation vymysleli unikátní řešení, a to vybudování sítě bez centrálního uzlu. To umožňovalo, že v případě zničení některé linky byla informace vedena k příjemci jinou cestou. Tak vznikl v srpnu 1969 arpanet.

Postupně se k internetu začaly připojovat další subjekty, především university. V této době byl internet čistě nekomerční záležitostí. Na jeho vybudování přispívala americká armáda a různé vládní agentury. Podnikatelé o něj neměli zájem, protože nenacházeli způsob, jak jej využívat.

V roce 1989 vymyslel Tim Berners-Lee nový způsob komunikace - hypertextové dokumenty. Jde o texty, které obsahují odkazy na další dokumenty, které

[58] PEKÁREK, O., ČÍŽEK, V. *Práce s agenturními a elektronickými informacemi*. České Budějovice, 2007. s. 9.

[59] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 16.

mohou být umístěny na jiném třeba hodně vzdáleném počítači světa. Díky jednoduchému a intuitivnímu ovládání se tento způsob komunikace rozšířil i mimo laboratoře CERN, kde Tim Berners-Lee pracoval, a dnes jej známe pod jménem World Wide Web. Zanedlouho se začaly k dokumentům připojovat i obrázky. Právě existence www a masové rozšíření osobních počítačů stály za ohromným rozmachem internetu. V roce 1992 pronikl internet i do komerční sféry[60].

Rychlost, s jakou se internet začal šířit do celého světa, je nepředstavitelná. Již čtyři roky poté, co byl otevřen široké veřejnosti, získal 50 miliónů uživatelů. Rychlost vynikne zejména ve srovnání s šířením rozhlasu a televize. Rozhlas získal stejný počet uživatelů za 30 let a televize za 13 let. V roce 2005 měl internet 950 miliónů uživatelů a na konci roku 2008 již 1,58 miliard uživatelů, což představuje 23,6% celkové světové populace[61].

3.1.2 Internet v ČR

V Československu se internet objevuje po pádu komunismu v roce 1989. V květnu roku 1990 se k nám dostává síť EUNET. V říjnu téhož roku se k nám dostává také evropská síť EARN, která je odnoží evropské sítě Bitnet. K oficiálnímu připojení Československa k internetu došlo v listopadu roku 1991. Formální připojení ČSFR k internetu se uskutečnilo slavnostně 13. února 1992. Internet byl tehdy dostupný v Praze na ČVUT, ale o připojení měly zájem o ostatní vysoké školy ČSFR[62].

Před rokem 1995 měl v naší zemi ponětí o existenci internetu jen málokdo. Na přelomu let 1995 a 1996 se však tato situace mění, protože na trh vstupuje celá řada subjektů, které poskytují připojení k internetu. Do této doby zabraňoval rozvoji komerčních poskytovatelů monopol společnosti Eurotel (Český Telecom, dnešní O2), který se vztahoval mimo jiné i na veřejné služby přenosu dat. Tím, že tento monopol na sklonku roku 1995 skončil, otevřel se prostor pro komerční využití internetu a s tím spojený rozmach[63].

---

[60] PEKÁREK, O., ČÍŽEK, V. *Práce s agenturními a elektronickými informacemi*. České Budějovice, 2007. s. 8.

[61] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 17.

[62] PEKÁREK, O., ČÍŽEK, V. *Práce s agenturními a elektronickými informacemi*. České Budějovice, 2007. s. 8

[63] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 19.

3.1.3 Internet a vzdělání

Internet má mimo jiné velký význam pro vzdělávání. Studenti mohou komunikovat se svými učiteli a spolužáky prostřednictvím e-mailů nebo mohou pro komunikaci používat instant messaging. Internet umožňuje, aby se studenti účastnili různých on-line výukových kurzů a programů. On-line výuka prostřednictvím webové kamery může být velkým přínosem pro tělesně postižené studenty, protože jim umožňuje účast na vyučovací hodině bez nutnosti jejich fyzické přítomnosti.

Jednou z největších výhod internetu při vzdělávání je možnost jeho využití při zpracování domácích úkolů, psaní seminárních a dalších prací. On-line knihovny a vědecké databáze velmi usnadňují jakékoliv vyhledávání potřebných údajů. Internet šetří čas i práci nejen studentům, ale i všem ostatním, kteří chtějí získat nové informace[64].

3.1.4 Internet a komunikace

Internet způsobil, že se komunikace mezi lidmi stala rychlejší, jednodušší a méně nákladnou. Internet umožňuje kontakt s lidmi i na velmi vzdálených místech země a nabízí tak možnost poznání rozmanitých světových kultur. Tím, že umožňuje komunikaci mezi lidmi různých národností, vytváří jakousi on-line komunitu, ve které se každý uživatel internetu může cítit jako její právoplatný člen. Tím vlastně internet „boří hranice“, a to nejen hranice zeměpisné, ale i hranice mezi lidmi vyvolané věkem, pohlavím, sociální třídou, rasou a náboženstvím.

Skutečností však je, že na jedné straně internet svět spojuje, na druhé straně pomáhá k jeho rozdělení. V internetovém globálním světě totiž také existují ohromné rozdíly mezi rozvojovými a vyspělými národy. Lidé v rozvojových zemích asi většinou nemají žádný přístup k internetu a přitom to jsou právě oni, kteří by nejvíce potřebovali, aby získali různé informace např. o zdraví, hygieně, péči o dítě, hospodářství a jiných důležitých věcech. Samozřejmě nelze věřit, že by přístup k internetu vyřešil problémy spojené s chudobou, ale zcela určitě by k řešení různých problémů v chudších zemích mohl svými informacemi přispět[65].

[64] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 22-23.
[65] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha, 2012. s. 24.

3.2 Sociální sítě

Pod pojmem sociální sítě dnes především rozumíme službu na internetu, která registrovaným členům umožňuje si vytvářet osobní veřejný či částečně veřejný profil, komunikovat spolu, sdílet informace, fotografie, videa, provozovat chat a další aktivity[66]. Sociální síť se skládá z přihlašovací stránky, uživatelského účtu, profilu a spousty her a nástrojů, které umožňují zábavně strávit čas s přáteli[67].

Sociální sítě se začaly objevovat už v polovině 90. let minulého století v USA. Byly to sítě, které využívali ke komunikaci mezi sebou hlavně studenti. Už v nich se objevily stránky s prvními profily. Tyto sítě byly základem pro dnešní sociální sítě, z nichž nejznámější jsou Facebook, MySpace, Twitter a LinkedIn.

Dnešní sociální sítě jsou skutečně něčím mimořádným. Mají milióny uživatelů a nevyužívají je jen studenti, i když uživatelů z řad studentů je stále téměř polovina. Některé sítě mají specifické zaměření, například LinkedIn je typem sociální sítě, kde se ,,scházejí“ různé profese. Když je potřeba nějaký odborník, lze ho nalézt na LinkedIn (pouze pro Čechy znalé angličtiny)[68].

Každý uživatel sociálních sítí uvede své charakteristiky a vlastnosti a dá je tak veřejně k dispozici dalším uživatelům. Lidé se tak mohou vzájemně vyhledávat a vytvářet virtuální ,,komunitu“. Další možností je pak prohledávání sociálních sítí – nahlížení do seznamu přátel našich přátel, tedy hledání dalších známých. Na výše uvedené funkci jsou pak založené další vlastnosti sociálních sítí jako například možnost publikování různých informací, vkládání fotografií a alb apod. Druhou stránkou je však otázka bezpečnosti a jistoty o skutečné identitě uživatelů[69].

3.2.1 Historie internetových sociálních sítí

Pokusy o propojení skupin lidí pomocí počítačů se objevují už v počítačovém ,,pravěku“ 80. a 90. let minulého století, a to ve formě Bulletin Board Systemů (BBS).

BBS byl systém, který umožňoval uživateli přístup k centrálnímu systému (zpravidla přes modem), z něhož mohl stahovat programy a hry a zároveň v něm i

[66] SOCIÁLNÍ SÍTĚ. In *wikipedia: the free encyklopedia* [online]. Poslední aktualizace 23.3.2013 [cit. 5. března 2013]. Dostupné na WWW: <http://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5>.

[67] RYAN, P. *Social Networking*. New York, 2011. s. 7.

[68] KULHÁNKOVÁ, H., ČAMEK, J. *Fenomén Facebook*. Kladno, 2010. s. 9.

[69] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 125.

zanechávat zprávy ostatním uživatelům. Z důvodu vysoké ceny telefonního připojení byly takové sítě většinou lokální a ke komunikaci je využívali lidé, kteří se navzájem znali a tvořili určitou komunitu[70].

V roce 1995 vybudoval Randy Conrad první sociální síť classmates.com, která již byla podobná současným sociálním sítím. Tyto webové stránky pomáhaly registrovaným uživatelům udržovat vztahy mezi spolužáky, studenty a jinými známými, respektive tyto spolužáky vyhledávat. Dnes má tento web přibližně 40 milionů uživatelů, z nichž většina pochází ze Spojených států amerických a Kanady[71].

V roce 2002 se objevil Friendster jako další seznamovací síť. Zatímco většina seznamek se zaměřila na vzájemné představování lidí, kteří se neznali, Friendster byl postaven na myšlence opětovného setkání již známých kamarádů. Friendster ale nezvládl prudký nárůst uživatelů a nepříliš kvalitně postavená databáze se začala hroutit. K jeho zániku pomohly i falešné profily celebrit, které začal Friendster mazat. V důsledku těchto skutečností začalo mnoho lidí službu opouštět, což způsobilo její konec[72].

V roce 2003 vznikla řada dodnes populárních sociálních sítí, z nichž každá se zaměřovala na určitou skupinu lidí. Nejvýraznější z nich byla sociální síť MySpace, která získala vedoucí postavení na trhu.

V roce 2004 byl spuštěn Facebook, který byl v první fázi sociálním systémem určeným výhradně studentům Harvardské univerzity. V roce 2005 se Facebook rozšiřuje i na ostatní vysoké školy v USA a Evropě, následně i mezi zaměstnance vybraných společností a nakonec se otevírá i všem ostatním uživatelům.

V roce 2006 se rozjíždí Twitter. V roce 2008 Facebook předčil server MySpace a stal se největší sociální sítí (měřeno počtem unikátních návštěvníků)[73].

3.2.2 Druhy sociálních sítí

Jak je patrné z předchozí kapitoly pojednávající o historii počítačových sítí, existuje mnoho druhů sociálních sítí. I v České republice máme několik sociálních sítí

[70] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 131.

[71] *Estranky.cz.* Sociální sítě [online]. 2013 [cit. 6. března 2013]. Dostupné na WWW: <http://www.socialnisite.estranky.cz/clanky/historie-socialnich-siti.html>.

[72] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 133.

[73] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 134.

jako např. Lidé, Spolužáci, Líbímseti atd. Po celém světě nejznámější z nich jsou následující:

a) Facebook

Facebook je díky jedné miliardě registrovaných uživatelů největší a také nejúspěšnější sociální sítí světa. Průměrný uživatel Facebooku má 130 přátel a je připojen do 80 skupin, stránek či událostí. Každý měsíc přispěje na svůj profil devadesáti novými položkami (tj. v průměru třemi denně). V dnešní době je Facebook k dispozici ve více než sedmdesáti jazykových mutacích.

K Facebooku se lze připojit nejen z počítače, ale také z mobilního telefonu pomocí aplikace Facebook Mobile. Tuto aplikaci využívá více než 200 milionů aktivních uživatelů[74].

Protože je Facebook k dispozici v češtině, používá se v ČR nejčastěji, ale i ve světě je jednoznačně nejpoužívanější. Facebook má trochu jiný charakter. Souvisí to jednak se způsobem jeho vzniku, jak je zmíněno v následujících odstavcích zabývajících se jeho historií, a s tím, že omezený „pohyb“ pouze v rámci univerzity pomohl Facebooku získat mezi uživateli důvěru, jednak s tím, že přidal funkci vybraných příspěvků, které slouží k zobrazování aktuálních informací přátel. Když někdo přidá na Facebook novou fotografii nebo vzkaz, na stránce jeho přátel se o této aktualizaci zobrazí informace[75].

- **Historie Facebooku**

Zakladatelem Facebooku je bývalý student Harvardské univerzity, Mark Zuckerberg. Ve druhém ročníku vytvořil s pomocí ukradených fotografií stránku facemash.com, která umožnila hodnocení studentek z okolních kolejí. Na stránkách se zobrazily vedle sebe vždy dvě fotografie, přičemž uživatel měl za úkol vybrat hezčí dívku. Během prvních čtyř hodin Facemash přilákal 450 návštěvníků, kteří zhodnotili 22 000 fotografií. Stránka se velmi rychle rozšířila i na servery okolních kampusů, ale zanedlouho byla stažena vedením univerzity. Zuckerberg se dostal před disciplinární komisi, která šíření digitálních fotografií vyhodnotila jako úmyslné narušení bezpečnosti, porušení autorských práv, pravidel univerzity a narušení soukromí. Byl potrestán půlročním podmíněným vyloučením.

[74] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 136.
[75] KULHÁNKOVÁ, H., ČAMEK, J. *Fenomén Facebook.* Kladno, 2010. s. 9.

Následný projekt se snažil vytvořit web, kde by mohli studenti, profesoři a personál z Harvardské univerzity z vlastní vůle sdílet své poznatky, fotografie, osobní informace a jiné příspěvky s ostatními pomocí profilů. Měli by možnost vybrat si, s kým chtějí tyto informace sdílet. Cílem projektu bylo zjednodušit proces seznamování mezi lidmi a studentům prvního ročníku usnadnit orientaci v novém prostředí a v životě na univerzitě.

V lednu 2004 Zuckerberg začal programovat a 4. února téhož roku spustil své stránky pod názvem „Thefacebook“, který byl později změněn na „Facebook“. Členství v síti bylo zpočátku omezeno pouze na studenty Harvardské univerzity a 26. září 2006 byl Facebook zpřístupněn veřejnosti[76].

Zuckerberg byl několikrát obviněn, že při tvorbě Facebooku využívá cizí nápady. Je asi nutno připustit, že mnohé komponenty začínajícího Facebooku byly v praxi odzkoušeny už jinde a že jeho služba je následovníkem nápadů, jež se vyvíjely již 40 let[77].

- **Statistiky Facebooku**

Počet uživatelů Facebooku ve světě, neustále stoupá, jak ukazuje následující graf[78].

[76] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 136-137.

[77] KIRKPATRICK, D. *Pod vlivem Facebooku*. Brno, 2011. s. 59.

[78] KOLERUSOVÁ, M. *Sunitka.cz*. Proč přemýšlet o ppc reklamě na Facebooku? [online]. 2011 [cit. 8. března 2013]. Dostupné na WWW: <http://www.sunitka.cz/c/74-proc-premyslet-o-ppc-reklame-na-facebooku>.

V ČR mělo začátkem roku 2011 účet na Facebooku 3 076 000 uživatelů, a tím se ČR v počtu uživatelů umístila na 37. místě ve světě[79].

b) Twitter

Twitter vznikl v roce 2006, kdy Jack Dorsey vymyslel komunikaci lidí v malé skupině pomocí krátkých textových zpráv. Obsah těchto zpráv neměl být nijak složitý či závažný. Měly být o tom, co uživatelé právě dělají, o čem přemýšlí apod.

Jde o mobilní sociální síť a mikroblogovací službu, kde může každý uživatel psát krátké vzkazy (max. 40 znaků), tzv. tweety čili svůj vlastní blog. Tyto vzkazy se zobrazují jak na stránce autora, tak na stránkách uživatelů, kteří jsou jeho odběratelé. Tweety mohou být přístupné komukoli, ale lze je omezit jen na odběratele. Službu může uživatel využívat přes webový prohlížeč, externí aplikace na mobilním telefonu nebo prostřednictvím SMS zpráv[80].

c) LinkedIn

LinkedIn začal být vytvářen v roce 2002 a k jeho oficiálnímu spuštění došlo v květnu roku 2003[81].

LinkedIn je největší internetová sociální síť zaměřena na podnikatelské subjekty, která sdružuje profesionály v nejrůznějších oborech z celého světa. Své kontakty mezi sebou v lednu 2011 sdílelo 90 milionů profesionálních uživatelů ve více než 200 zemích. Slovem ,,profesionální" je míněno to, že síť je určena odborníkům. V současné době je síť dostupná v hlavních světových jazycích (v angličtině, francouzštině, němčině, italštině, portugalštině a španělštině)[82].

d) Myspace

Internetová sociální síť Myspace (dříve psána MySpace) vznikla v roce 2003. Kolem roku 2005 byla vedoucí sociální sítí ve světě. Zaměřuje se na hudbu, filmy, hry a různá témata k diskuzím ohledně aktuálního dění ve světě hudby, filmu či televize. Její

[79] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 137-138.

[80] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 145.

[81] LAUSCHMANN, J. *Cdr.cz.* Největší sociální sítě dneška [online]. 2012 [cit. 9. března 2013]. Dostupné na WWW: <http://cdr.cz/clanek/nejvetsi-socialni-site-dneska>.

[82] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 149.

snahou je spojit veškeré kulturní dění mezi lidmi v reálném čase, k čemuž jí napomohla skutečnost, že ji v roce 2005 koupil mediální konglomerát News Corp[83].

e) Google+

Sociální síť Google+ vznikla 28. června 2011, kdy Google oznámil její dlouho očekávané spuštění[84]. Google+ má svoji jedinečnou charakteristiku a tím se odlišuje od ostatních sítí. Ve své podstatě totiž nejde primárně o sociální síť, přestože svým uživatelům funkce sociální sítě nabízí. Cílem Googlu nebylo konkurovat již známým sítím jako Facebook, Twitter a LinkedIn; Google naopak jejich provozovatele vyzýval ke spolupráci, i když v té době nebylo jisté, zda věřil v úspěch takové nabídky, nebo zda mu šlo jen o získání dobrého jména.

Místo klasické sociální sítě se totiž Google zaměřil na to, aby vytvořil jednotnou sociální kostru, která by byla společná pro všechny jeho služby. Tato kostra by obsahovala jednotný login do všech služeb a mapu sociálních vazeb mezi uživateli. Nejlepším způsobem, jak toho dosáhnout, je logicky vytvoření sociální sítě a její integrace do všech ostatních produktů od vyhledávání, přes Google Photos až po YouTube[85].

3.2.3 Bezpečnost a soukromí v sociálních sítích

Internet je stále „územím nikoho“, a to jak z důvodu relativní anonymity účastníků, tak i z toho důvodu, že jakákoliv právní úprava je na rozdíl od internetu omezena na určité území. Nejvýznamnější úlohu má proto prevence – je třeba zabezpečit citlivé informace, které jsou přenášeny prostřednictvím internetu, a dále také zajistit soukromí uživatelů. Následná náprava škod způsobených zneužitím citlivých informací a narušením soukromí uživatelů by byla složitá a často i nemožná.

- **Legislativa**

Jak je výše uvedeno, právo je založeno na teritoriálním principu, a proto je právní úprava internetu problematická[86].

[83] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 153.

[84] ZÁŠKOLNÝ, J. *123abc.cz*. Informace o sociálních sítích na internetu ve světě i České republice [online]. 2011-2013 [cit. 9. března 2013]. Dostupné na WWW: <http://www.socialnisite.123abc.cz>.

[85] LAUSCHMANN, J. *Cdr.cz.* Největší sociální sítě dneška [online]. 2012 [cit. 9. března 2013]. Dostupné na WWW: <http://cdr.cz/clanek/nejvetsi-socialni-site-dneska>.

[86] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 161.

Vstupem komerčních subjektů na internet se určitá regulace internetového prostředí stala nutností a zákonodárci se jí začali zabývat. Často však vznikají zákony, ve kterých je zřetelně vidět snaha přizpůsobit současnou právní úpravu tak, aby pokryla i problémy způsobené vznikem nových médií. Tyto snahy o přizpůsobení však mohou být zcela v rozporu s původními principy dané právní úpravy a způsobit další nezamyšlené právní komplikace v původní zájmové oblasti.

Právní systém užitý při uzavírání obchodních a spotřebitelských smluv prostřednictvím komunikace na dálku (tedy i prostřednictvím internetu) je věcí dohody smluvních stran, stejně jako místní příslušnost soudů či rozhodčích orgánů v případných sporech. Pokud nejsou tyto otázky ve smlouvě upraveny, předpokládá se využití domovských institucí zákazníka (spotřebitele), ovšem vymahatelnost práv vzniklých na základě domácího právního systému je vůči zahraničním subjektům malá[87].

- **Licenční podmínky**

Vztah uživatele a provozovatele nových médií je běžně upravován licenčními podmínkami. Tyto podmínky většinou obsahují licenci uživateli k použití dané aplikace, licenci provozovateli k nakládání s daty uživatele, práva a povinnosti smluvních stran atd. Kvalita a rozsah vypracování těchto podmínek se různí. Navíc se mlčky předpokládá, že uživatel je dobře seznámen se svým domácím právním prostředím, případně je seznámen i s cizím právem, pokud souhlasil s jeho využitím. V praxi je však „právní gramotnost“ uživatelů internetu poměrně nízká a je třeba počítat s tím, že většina uživatelů se licenčními podmínkami nijak zvlášť nezabývá, pokud je vůbec čte. U velkých služeb je určitou zárukou mediální a odborná pozornost věnovaná provozovatelům těchto služeb, tedy i do jisté míry oprávněný předpoklad, že pokud by byly podmínky pro uživatele opravdu špatné, bude tato skutečnost medializována, případně na to upozorněno[88].

- **Ochrana osobních údajů**

Při registraci na sociální síti jsou vyžadována různá data a údaje. Mezi takové údaje patří např. jméno a příjmení, telefon, adresa bydliště. Jejich uvedení je často nepovinné, ale může mít vliv na úspěšnost vyhledání nebo zviditelnění uživatele.

[87] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 161-162.
[88] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 164-165.

Před zaregistrováním na některou síť by se měl každý uživatel ubezpečit, jak je v licenčním ujednání popsáno nakládání s osobními údaji ze strany provozovatele. Mnohé sociální sítě používají údaje z profilů uživatelů a nabízejí je třetím stranám. Může se tedy stát, že telefonní číslo uživatele nebo adresa zveřejněná na síti budou poskytnuty pro reklamní účely.

Některé sítě nabízejí ve svém rozhraní jiné aplikace, například hraní her, lokalizaci na mapě nebo sdílení obsahu. Každý uživatel by si měl pečlivě zkontrolovat, zda nedává svolení k odeslání jeho osobních dat, nebo dokonce neposkytuje adresář svých přátel. Obecně platí, že čím méně toho o sobě uživatel vyplní, tím méně se mu může stát. Nejčastěji je zveřejněný obsah zneužit pro vytváření falešných identit nebo ke kyberšikaně[89].

Ochrana osobních údajů je základním nástrojem ochrany soukromí osob. Cílem zákonné úpravy je řešit střety oprávněných zájmů subjektů v této oblasti, tak aby byly tyto zájmy vyváženy. Vyšší váha je ovšem vždy přisuzována zachování soukromí, protože jeho porušení je zásadně nezvratné (jednou zveřejněný údaj je velmi obtížné znovu utajit). V dnešní době můžeme ovšem pozorovat celkový odklon od striktní ochrany soukromí, a to v souvislosti s tzv. všeobecně prospěšnými aktivitami typu „boje proti terorismu“ či politických zdůvodnění prohlašujících, že „slušný člověk nemá co skrývat“.

Evropské společenství vydalo v roce 1995 směrnici komplexně upravující ochranu osobních údajů (tedy nakládání s takovými soubory dat, která mohou vést k identifikaci konkrétní osoby). V ČR je tato směrnice implementována v podobě zákona o ochraně osobních údajů (zákon č. 101/2000 Sb.). Lze usuzovat, že rozvoj užívání internetu a elektronických médií obecně přispěl k vydání tohoto zákona, který zavádí povinnou registraci správců osobních údajů, povinné náležitosti takového zpracování (zahrnující ukládání a přenos) týkající se bezpečnosti, protokolování apod. Přestože je tento zákon poměrně přísný, jeho dodržování je mnohdy spíše formální, mnohými subjekty je zcela ignorován, případně jsou dodržována jen některá jeho ustanovení[90].

---

[89] BEZPEČNÝ INTERNET. *Ochrana osobních údajů* [online]. 2008-2013 [cit. 10. března 2013]. Dostupné na WWW: <http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/ochrana- osobnich-udaju.aspx>.

[90] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 165-166.

- **Informační bezpečnost a důvěrnost vztahů**

Uložení informací (resp. dat) v informačních systémech a jejich toky lze považovat za bezpečné, pokud je adekvátně zajištěna jejich důvěrnost, integrita a dostupnost.

Samozřejmostí by mělo být zabezpečení datového úložiště vůči neoprávněnému přístupu a veškerých výstupů z tohoto úložiště obsahujících citlivá data. Uživatelé by měli být upozorněni na způsob zabezpečení a osobní zodpovědnost za jimi zveřejňovaná data.

Zajištění bezpečnosti nelze omezit pouze na opatření technického rázu a pomíjet lidskou stránku věci. V komunitě by měl vždy existovat systém pravidel (i nepsaný), jak zacházet se sdělovanými informacemi (vč. uživatelských jmen, přístupových hesel a obdobných údajů) a do jaké míry důvěřovat ostatním uživatelům. Právě trend zjednodušování reálných vztahů, když se promítají do technických systémů, jakými jsou například sociální sítě, je významnou bezpečnostní hrozbou - velmi různorodé reálné vazby nahrazují dvě možnosti vztahu - přátelení či nepřátelení se. Je logické, že jednotliví uživatelé vnímají důvěrnost této vazby různě – někteří se v rámci sociálních sítí „přátelí“ s kýmkoli, někteří se známými, jiný pouze se skutečnými přáteli.

Nerovnoměrnost vnímané důvěrnosti vazeb deformuje vztahy v sociálních sítích z hlediska bezpečnosti a ochrany soukromí a umožňuje úniky citlivých informací či zkreslování určitých sdělení[91].

- **Zajištění soukromí**

Zajištění soukromí znamená především ochranu proti nakládání s identitou uživatele a jeho daty bez jeho výslovného souhlasu.

Jak již bylo řečeno výše, základním prostředkem zajištění soukromí je vyloučení identifikace subjektu (tj. anonymita, pseudonymita, ochrana osobních údajů). Každý uživatel by si měl být vědom toho, co se může stát při zveřejnění údajů o jeho osobě. Stejně tak by si měli uživatelé uvědomovat, že svou publikační činností mohou ohrožovat soukromí nejen své, ale i osob, o kterých se zmiňují.

Zejména v případě uživatelů z řad dětí a mládeže je možné předpokládat určitou neznalost v této oblasti, jakož i lhostejnost vůči případným následným dopadům. Je

[91] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 167-168.

zcela na rozhodnutí provozovatele, zda zavede pravidla regulující publikování citlivých údajů (vč. specifikace takovýchto údajů) a do jaké míry bude regulaci provádět. Porušení takových pravidel je možné sankcionovat až tím, že bude zakázána další publikační aktivita uživatele.

Další používanou metodou ochrany soukromí je moderování příspěvků ještě před jejich zveřejněním. Na rozdíl od seberegulace uživatele jsou příslušné údaje uloženy v systému provozovatele a je s nimi seznámen moderátor. Moderování příspěvků je obvykle využíváno i jako nástroj cenzury příspěvků obsahujících vulgární, rasistický či jiný nepřípustný obsah, pokud nejsou pro tento účel používány automatické systémy založené na filtrování příspěvků[92].

Shrnutí

Teoretická část podala přehled o historii a vývoji počítačové kriminality. Byly rozebrány jednotlivé její formy a konkrétněji byla probrána kyberšikana, která patří mezi nejnovější druhy počítačové kriminality. Z uvedených informací vyplynulo, že počítačová kriminalita se přes svoji relativně krátkou dobu existence rozvinula do mnoha forem a značně rozšiřuje možnosti trestné činnosti.

Další kapitola se věnovala internetu, jeho historii a vývoji a jeho využití pro uživatele. V poslední kapitole teoretické části byly charakterizovány sociální sítě. Obsahem opět byla historie a vývoj sociálních sítí, druhy sociálních sítí a bezpečnost a soukromí na sociálních sítích.

Teoretická část bakalářské práce byla velmi důležitá pro výzkumnou část, která dále následuje. Teoretická část naznačila, jaká rizika může užívání internetu a sociálních sítí pro uživatele představovat. Ve výzkumné části bude podle vyhodnocení dotazníků popsáno, na kolik jsou si uživatelé těchto rizik vědomi a zda se před nimi chrání.

[92] PAVLÍČEK, A., *Nová média a sociální sítě*. Praha, 2010. s. 168-169.

4 Praktická část

4.1 Cíl dotazníkového šetření

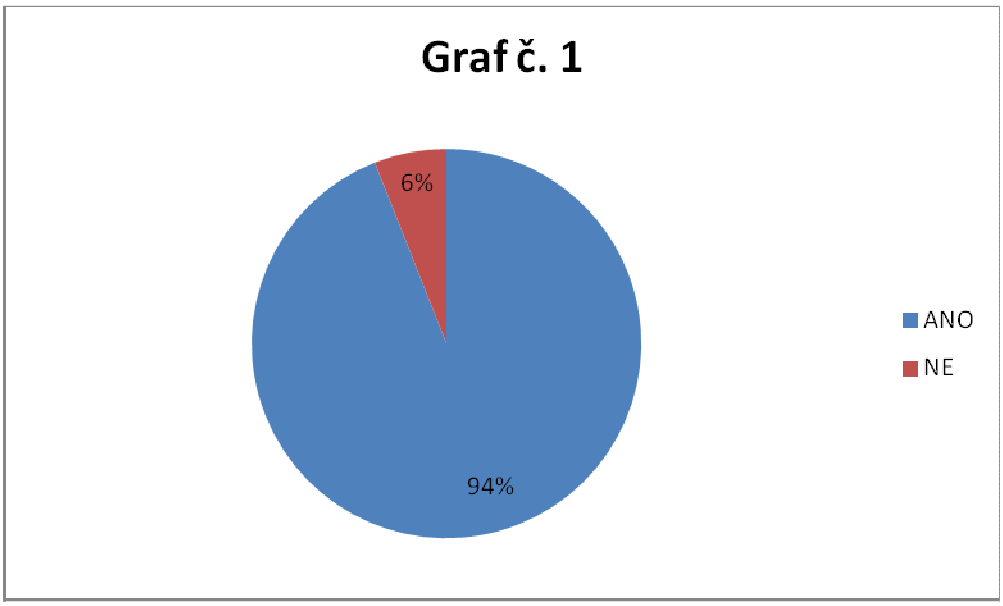
Cílem dotazníkového šetření bylo zjistit rozsah používání internetu a sociálních sítí, stav ochrany při tomto používání a znalosti, zejména informovanost o riziku, kterou uživatelé internetu a sociálních sítí mají. Výzkum byl proveden tak, že určitému okruhu uživatelů internetu a sociálních sítí byl předán dotazník, v němž byly otázky k těmto tématům. V zájmu jednoduchosti účastníci výzkumu vybírali odpovědi z nabídnutých možností.

4.2 Metoda šetření

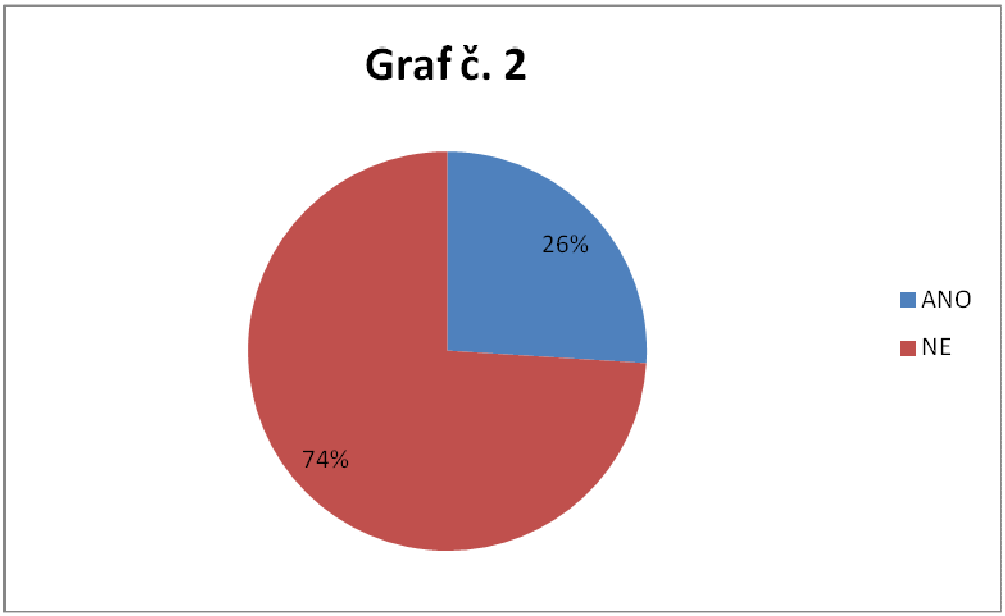
Metoda dotazníkového šetření nezohledňovala věk či pohlaví uživatelů. Dotazníky v papírové podobě byly rozdány mezi studenty a administrativními pracovníky, tedy uživateli ve věku 20 – 55 let. Bylo rozdáno 100 dotazníků s 11 otázkami a všech 100 dotazníků bylo vyhodnoceno. Otázky byly formulovány z mé strany a byly schváleny mým vedoucím bakalářské práce. Poté byly předány uživatelům internetu a sociálních sítí. Z dotazníkového šetření se budu snažit vyvodit závěry a navrhnout případná preventivní opatření.

4.3 Vyhodnocení dotazníku

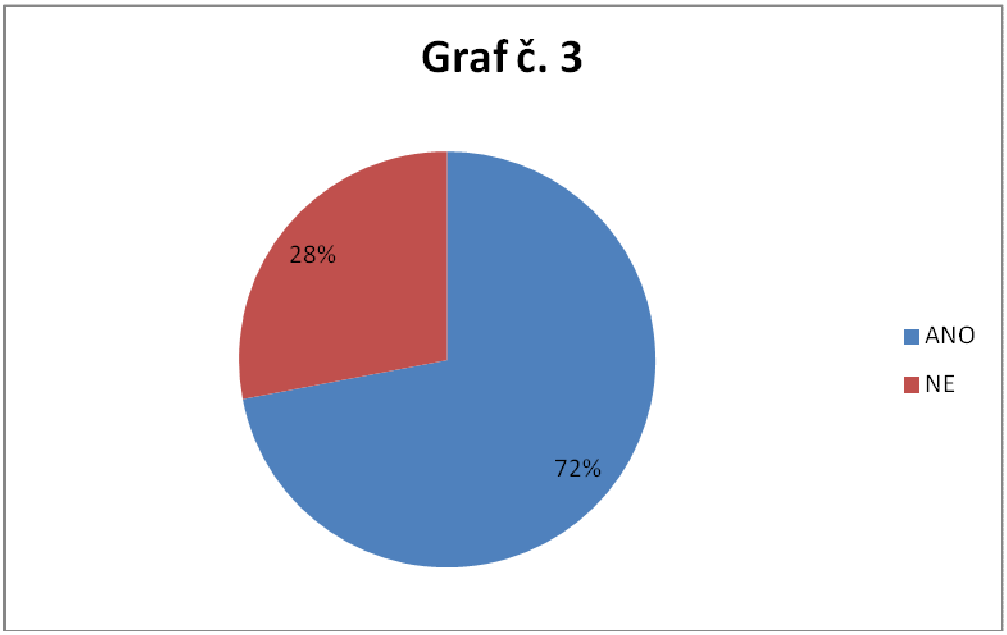
Otázka č. 1: Používáte internet každý den? Jak z grafu č. 1 vyplývá, dotazníkové šetření ukázalo, že internet každý den používá 94% ze 100 dotázaných uživatelů a 6% nikoli.



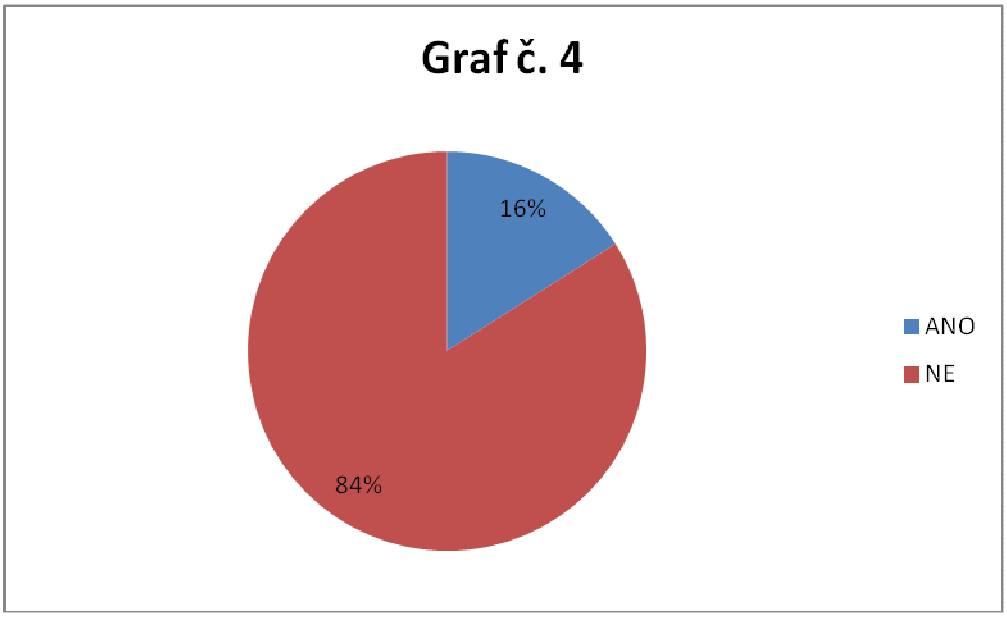
Otázka č. 2: Setkali jste se již s napadením vašeho počítače během surfování na internetu? Jak z grafu č. 2 vyplývá, dotazníkové šetření ukázalo, že s napadením počítače se již setkalo 26% ze 100 dotázaných uživatelů a 74% nikoli.



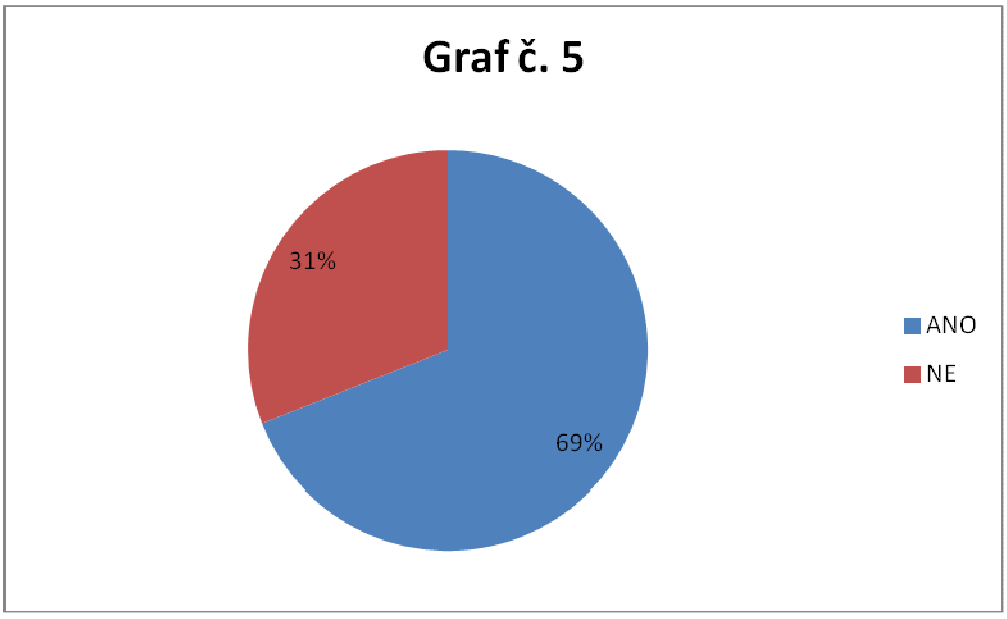
Otázka č. 3: Používáte legálně zakoupený antivirový program s pravidelnou aktualizací? Jak z grafu č. 3 vyplývá, dotazníkové šetření ukázalo, že legálně zakoupený antivirový program používá 72% ze 100 dotázaných uživatelů a 28% nikoli.



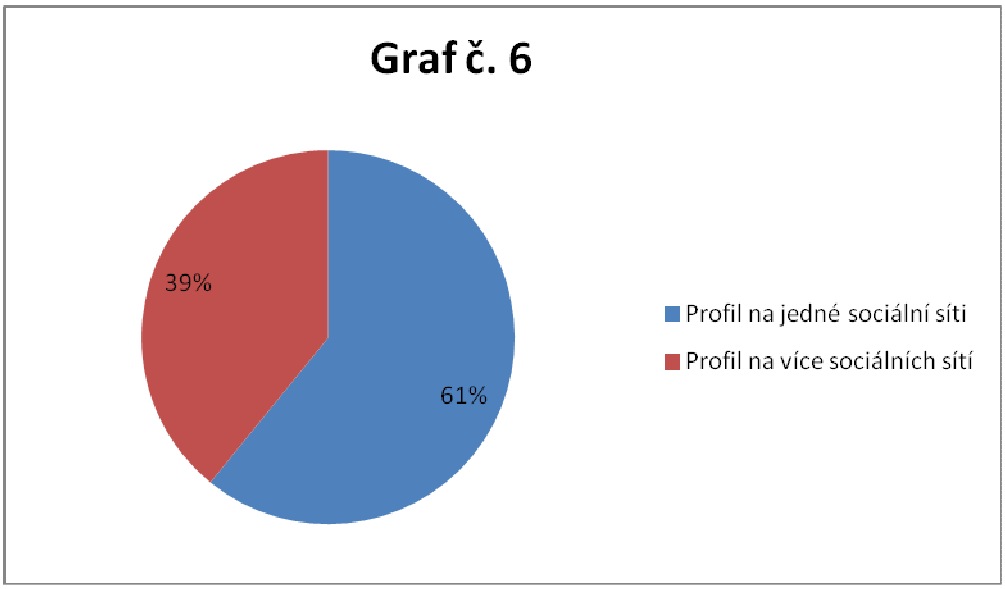
Otázku č. 4: Setkali jste se již s kyberšikanou na internetu, ať už vy sami nebo někdo z vašeho okolí? Jak z grafu č. 4 vyplývá, dotazníkové šetření ukázalo, že s kyberšikanou se setkalo 16% ze 100 dotázaných uživatelů a 84% nikoli.



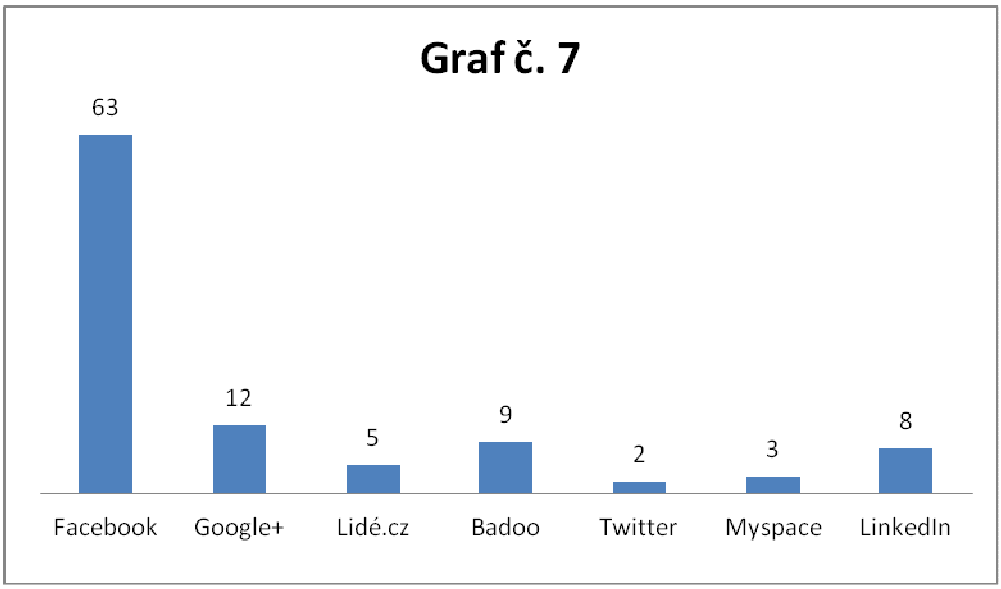
Otázka č. 5: Máte založený profil na sociální síti? Jak z grafu č. 5 vyplývá, dotazníkové šetření ukázalo, že profil na sociálních sítích má založeno 69% ze 100 dotázaných uživatelů a 31% nikoli.



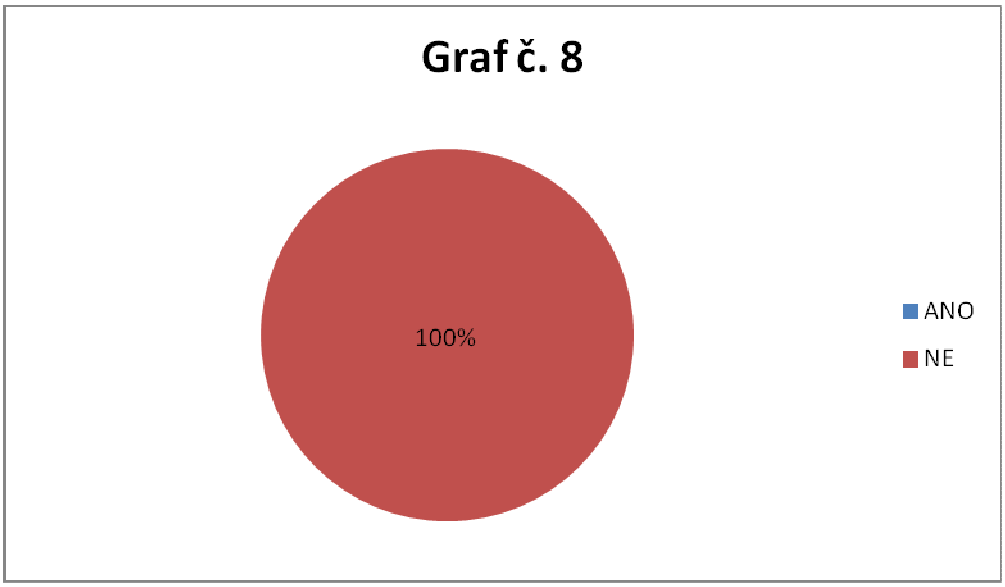
Další otázky byly určeny pouze uživatelům, kteří uvedli, že mají vytvořený profil na sociálních sítích. Odpovídalo už jen 69 ze 100 dotázaných uživatelů. Otázka č. 6: Máte profil na jedné nebo více sociálních sítích? Jak z grafu č. 6 vyplývá, dotazníkové šetření ukázalo, že profil na jedné sociální síti má založeno 61% z 69 dotázaných uživatelů a zbylých 39% má založeno profil na více sociálních sítích.



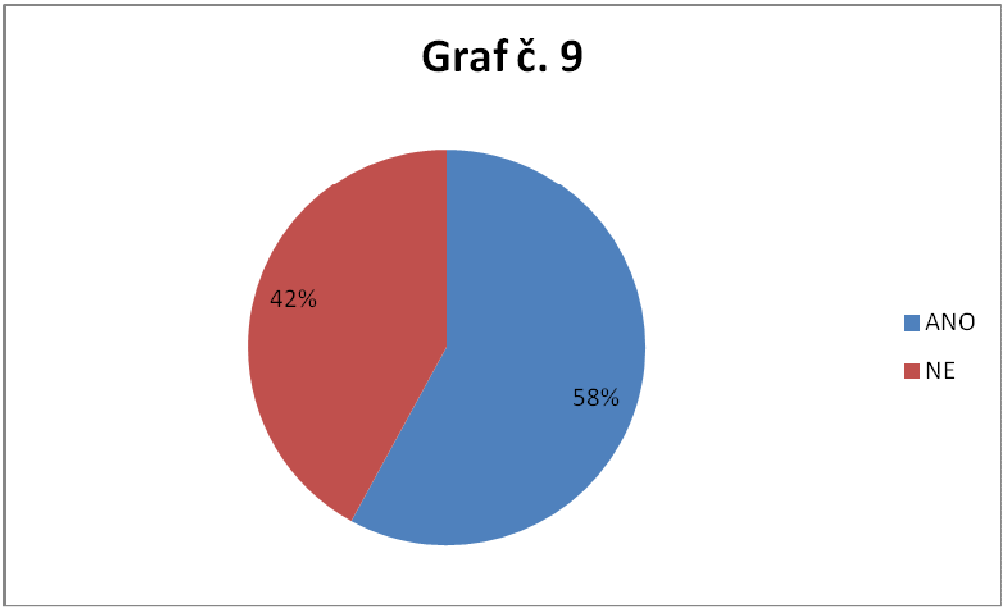
Otázka č. 7: Uveďte, na které sociální síti máte založený profil. Jak z grafu č. 7 vyplývá, dotazníkové šetření ukázalo, že z 69 uživatelů má sociální síť Facebook založeno 63 uživatelů, Google+ 12 uživatelů, Lidé.cz 5 uživatelů, Badoo 9 uživatelů, Twitter 2 uživatelé, Myspace 3 uživatelé a LinkedIn 8 uživatelů.



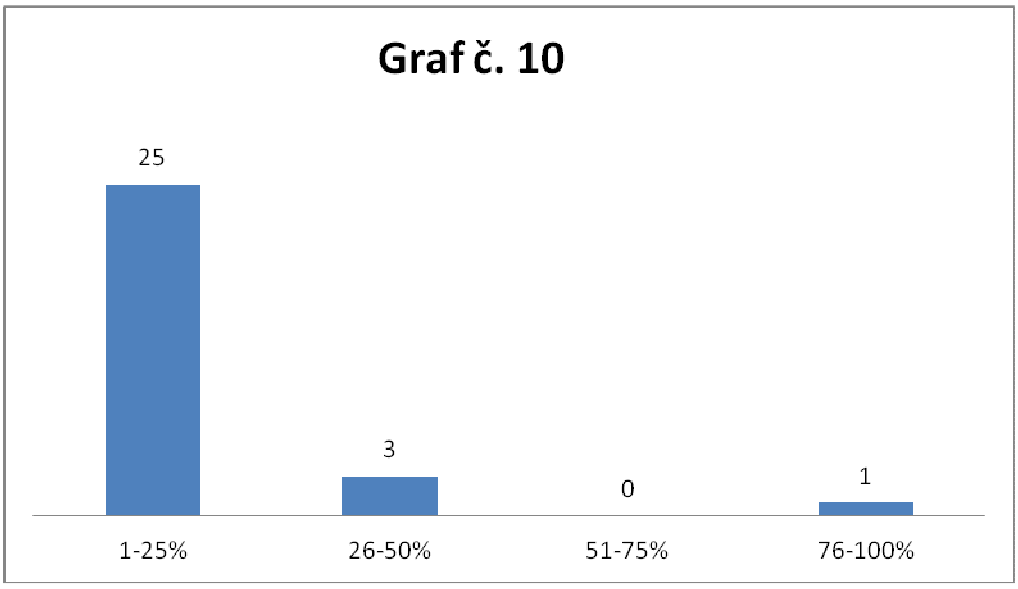
Otázka č. 8: Setkali jste se již s napadením vašeho profilu na sociální síti nebo zneužitím vámi uvedených údajů? Jak z grafu č. 8 vyplývá, dotazníkové šetření ukázalo, že se žádný z 69 dotázaných uživatelů nesetkal s napadením profilu na sociální síti.



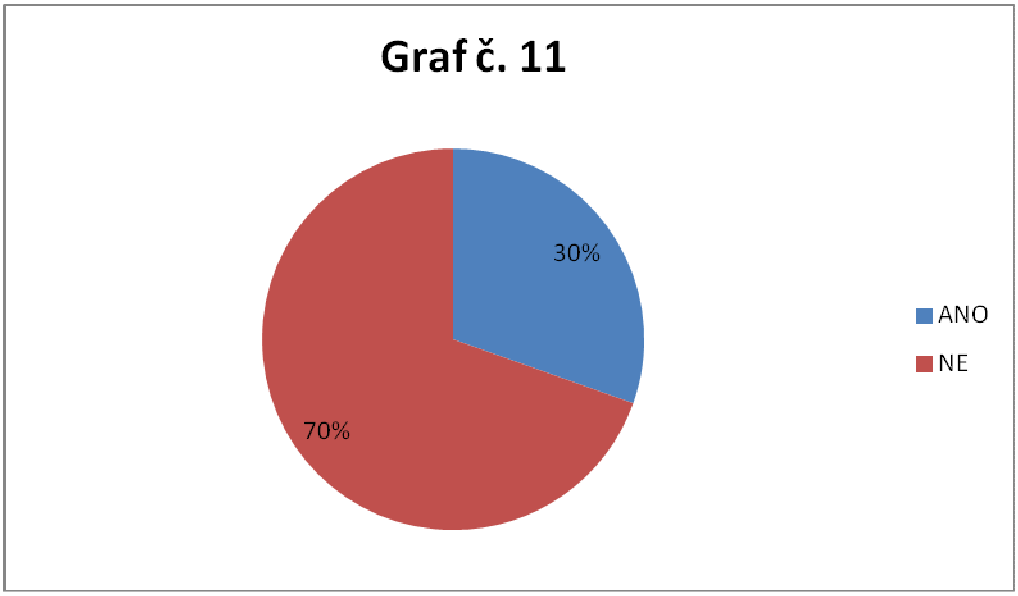
Otázka č. 9: Znáte osobně všechny „přátele“, které máte na sociálních sítích? Jak z grafu č. 9 vyplývá, dotazníkové šetření ukázalo, že 58% z 69 dotázaných uživatelů zná osobně všechny přátelé a 42% nikoli.



Otázku č. 10: V případě, že ne, v kolika procentech je neznáte? Na tuto otázku odpovídalo jen 29 z 69 dotázaných uživatelů. Jak z grafu č. 10 vyplývá, dotazníkové šetření ukázalo, že 25 uživatelů nezná svoje přátelé v rozsahu 1 - 25%, jen 3 uživatelé neznají svoje přátele v rozsahu 26 - 50% a pouze 1 uživatel nezná svoje přátele v rozsahu 76 - 100%.



Otázka č. 11: Máte strach ze zneužití vašich údajů na sociálních sítích? Jak z grafu č. 11 vyplývá, dotazníkové šetření ukázalo, že strach ze zneužití údajů na sociálních sítích má pouhých 30% z 69 dotázaných uživatelů a 70% nikoli.



4.4 Navrhovaná preventivní opatření

Prevence počítačové kriminality může mít různé formy a může být jednoduchá, nikdy však nezajistí vyloučení rizika určitého útoku. Z dotazníků sice vyplynulo, že většina z dotázaných uživatelů se s počítačovou kriminalitou osobně nesetkala, ale to neznamená, že k útokům nedochází.

Jako příklad lze uvést následující:

„Na uživatele Facebooku číhají zákeřné černé díry. Takzvané černé díry (blackhole), prostřednictvím kterých jsou do počítačů bez vědomí majitele distribuovány nejrůznější viry a trojské koně, se na internetu začaly vyskytovat už začátkem roku. Na pozoru by se před nimi měli mít nyní uživatelé Facebooku, varovala antivirová společnost AVG“[93].

Každý uživatel by se měl snažit předcházet počítačovým útokům, a měl by být tedy poučen o tom, jak jim lze předejít či se jim vyvarovat. Jak již bylo zmíněno, i se správnou prevencí se uživatel může stát terčem útoků, ale prevence rozhodně riziko těchto útoků snižuje.

Jako základní pravidla prevence lze uvést následující:

1) Udržovat aktuálnost svého počítače pomocí nejnovějších oprav a aktualizací.
2) Ujistit se, že počítač byl bezpečně nakonfigurován.
3) Zvolit si silná hesla a uchovávat je v bezpečí.
4) Chránit počítač pomocí softwaru zabezpečení.
5) Chránit své osobní údaje.
6) Pravidelně kontrolovat bankovní výpisy a výpisy z účtu kreditní karty[94].

Pokud jde o sociální sítě, uživatel by se měl seznámit s konkrétní sociální sítí, na které si chce založit svůj osobní profil a dokonale si pročíst veškerá nastavení a zabezpečení, která nabízí. Opět je na samotném uživateli, jaké údaje o své osobě zveřejní, aby předcházel riziku jejich zneužití. Logicky by měl o své osobě zveřejňovat co nejméně údajů a nezveřejňovat údaje na statusu, kde se právě nachází. Setkal jsem se

[93] *Novinky.cz.* Na uživatele Facebooku číhají zákeřné černé díry [online]. 2012 [cit. 29. března 2013]. Dostupné na WWW: <http://www.novinky.cz/internet-a-pc/bezpecnost/275993-na-uzivatele-facebooku-cihaji-zakerne-cerne-diry.html>.

[94] *Norton.com.* Nejlepší typy pro prevenci [online]. 1995 - 2013 [cit. 3. dubna 2013]. Dostupné na WWW: <http://cz.norton.com/prevention-tips/article>.

s případem, kdy si jeden z uživatelů dal oznámení do statusu, že v konkrétní den odjíždí na 14 dní na dovolenou. Tím logicky vystavil sám sebe nebezpečí, že si tento status přečtou všichni jeho „přátelé“, kteří se tak dozvědí, že jeho byt či dům je prázdný, a pro zločince to může být podmětem, aby ho šli vykrást.

S prevencí je podle mého názoru třeba začít už u samotných dětí. Měla by se zavést výuka na základních školách, aby byly děti poučeny o nebezpečích a nástrahách, které číhají na internetu a sociálních sítích. Je třeba je naučit surfovat po internetu bezpečně a správně a bezpečně používat sociální sítě.

Závěr

Počítačová kriminalita je velmi obsáhlé a aktuální téma a vyžaduje znalosti z trestního práva, kriminologie a prevence kriminality. Cílem mé bakalářské práce bylo rozebrat problematiku bezpečnosti na internetu a sociálních sítích. V práci byly shrnuty jak informace získané z dostupné literatury, tak informace získané analýzou výsledků výzkumu mezi uživateli internetu a sociálních sítí provedeného za účelem zjištění jejich informovanosti o riziku a nebezpečí, které jim hrozí, a byla navržena preventivní opatření pro zvýšení bezpečnosti používání internetu a sociálních sítí.

Teoretická část bakalářské práce podala přehled o historii a vývoji počítačové kriminality, rozebrala její formy a podrobně se zejména věnovala kyberšikaně. Dále se pak zabývala internetem a sociálními sítěmi. Seznámila s krátkou historií obou těchto fenoménu dnešní doby, jejich vývojem a významem. Problematika bezpečnosti a soukromí na sociálních sítích pak byla základem pro provedení výzkumu mezi uživateli internetu.

Ve výzkumné části byly zpracovány výsledky dotazníkového šetření, jehož cílem bylo zjistit rozsah používání internetu a sociálních sítí, stav ochrany při tomto používání a informovanost o riziku, kterou uživatelé internetu a sociálních sítí mají. Dotazníky byly rozdány mezi studenty a administrativními pracovníky, tedy uživateli ve věku 20 - 55 let. Bylo rozdáno 100 dotazníku s 11 otázkami.

Z odpovědí na otázky vyplynulo, že internet je užíván ve značném rozsahu, sociální sítě již v menším, ale nikoli malém. Příznivým zjištěním je, že z dotázaných uživatelů se s napadením počítače setkala jen cca jedna čtvrtina a s kyberšikanou 16% a že legálně zakoupený antivirový program s pravidelnou aktualizací používá přes 70% dotázaných uživatelů. Dotázaní uživatelé sociálních sítí se zatím nesetkali s napadením profilu na sociálních a většina ani nemá strach ze zneužití údajů. Ohledně ,,přátel“ na sociálních sítích se ukázalo, že 42% uživatelů nezná svoje přátele osobně, což je téměř polovina uživatelů. Přitom tato skutečnost může vést ke zneužití osobních údajů uživatele nebo kyberšikaně. Domnívám se, že uživatelé by si měli skutečně dávat do přátel pouze uživatele, které znají osobně.

Poslední kapitola bakalářské práce byla věnována navrhovaným preventivním opatřením, protože prevence je asi to jediné, čím lze rizika, která užívání internetu a

sociálních sítí doprovázejí, alespoň snížit, když ne úplně odstranit. Obecně doporučovaná preventivní opatření jsem doplnil i vlastním názorem.

Protože lze očekávat, že vývoj počítačových technologií půjde stále rychlým tempem kupředu, musí společnost počítat s tím, že i počítačová kriminalita bude stále aktuálním tématem. Bude proto třeba, aby tomuto tématu byla věnována celospolečenská pozornost.

Seznam zkratek

BBS - Bulletin Board System

CD - Compact Disc

CD-R - Compact Disc - Recordable

CD-ROM - Compact Disc - Read Only Memory

ČR - Česká republika

ČSFR - Česká a Slovenská federativní republika

ČVUT - České vysoké učení technické

DVD - Digital Versatile Disc

ENIAC - Electronic Numerical Integrator And Computer

IBM - International Business Machines Corporation

ICQ - I Seek You

IM - Instant Messaging

IRC - Internet Relay Chat

ISP - Internet Service Provider

MŠMT - Ministerstvo školství, mládeže a tělovýchovy České republiky

PC - Personal Computer

SIM - Subscriber Identity Module

SMS - Short Message Service

TZ - Trestní zákoník

USA - United States of America

WWW - World Wide Web

Použité zdroje

Literární zdroje

1. HARISS, S., HARPER, A., EAGLE., NESS, J., LESTER, M. *Manuál hackera*. Praha : Grada publishing a.s., 2008. 399 s. ISBN 978-80-247-1346-5.
2. HATCH, B., LEE, J., KURTZ, G. *Linux hackerské útoky. Bezpečnost Linuxu – tajemství a řešení.* Praha : Softpress s.r.o., 2002. 576 s. ISBN 80-86497-17-8.
3. HULANOVÁ, L. *Internetová kriminalita páchaná na dětech*. Praha : Triton, 2012. 217 s. ISBN 978-80-7387-9.
4. JAMES, L. *Phishing bez záhad*. Praha : Grada publishing a.s., 2007. 281 s. ISBN 978-80-247-1766-1.
5. JIROVSKÝ, V. *Kybernetická kriminalita*. Praha : Grada publishing a.s., 2007. 284 s. ISBN 978-80-247-1561-2.
6. KIRKPATRICK, D. *Pod vlivem Facebooku*. Brno : Computer press, 2011. 320 s. ISBN 978-80-251-3573-0.
7. KULHÁNKOVÁ, H., ČAMEK, J. *Fenomén Facebook.* Kladno : BigOak, 2010. 128 s. ISBN 978-80-904764-0-0.
8. LAPÁČEK, J. *Internet pro úplné začátečníky*. Praha : Computer press, 2000. 198 s. ISBN 80-7226-226-2.
9. MATĚJKA, M. *Počítačová kriminalita*. Praha : Computer press, 2002. 106 s. ISBN 80-7226-419-2.
10. PAVLÍČEK, A., *Nová média a web 2.0*. Praha : Oeconomica, 2007. 118 s. ISBN 978-80-245-1272-3.
11. PAVLÍČEK, A., *Nová média a sociální sítě.* Praha : Oeconomica, 2010. 181 s. ISBN 978-80-245-1742-1.
12. PEKÁREK, O., ČÍŽEK, V. *Práce s agenturními a elektronickými informacemi*. České Budějovice : VŠERS, o.p.s., 2007. 138 s. ISBN 978-80-86708-40-9.
13. PROSISE, Ch., MADIA, K. *Počítačový útok. Detekce, obrana a okamžitá náprava*. Praha : Computer press, 2002. 410 s. ISBN 80-7226-682-9.
14. ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha : Portál, 2011. 104 s. ISBN 978-80-7367-984-2.
15. SCAMBRAY, J., MCCLURE, S., KURTZ, G. *Hacking bez tajemství.* Praha : Computer press, 2002. 625 s. ISBN 80-7226-644-6.

16. SVATOŠ, R. *Kriminologie ve světle nového trestního zákoníku.* České Budějovice : VŠERS, o.p.s., 2010. 174 s. ISBN 978-80-86708-21-8.

Zahraniční literatura

1. RYAN, P. *Social networking.* New York : The Rosen Publishing Group, Inc., 2011. 48 s. ISBN 978-1-4488-1922-5.

Legislativní dokumenty

1. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Praha : Armex Publishing s.r.o., 2011. 172 s. ISBN 978-80-87451-03-8.

Elektronické zdroje

1. BEZPEČNÝ INTERNET. *Ochrana osobních údajů* [online]. 2008-2013 [cit. 10. března 2013]. Dostupné na WWW: <http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/ochrana-osobnich-udaju.aspx>.
2. BEZPEČNÝ INTERNET. *Sítě peer-to-peer* [online]. 2008-2013 [cit. 10. ledna 2013]. Dostupné na WWW: <http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/site-peer-to-peer.aspx>.
3. ČINČERA, J. *Ikaros.cz.* Mha přede mnou, mha za mnou - hoaxes útočí na lidskou solidaritu [online]. 2002 [cit. 16. ledna 2013]. Dostupné na WWW: <http://www.ikaros.cz/node/931>.
4. DŽUBÁK, J. *Hoax.cz.* Phishing [online]. 2008-2013 [cit. 30. prosince 2012]. Dostupné na WWW: <http://hoax.cz/phishing>
5. *Estranky.cz.* Sociální sítě [online]. 2013 [cit. 6. března 2013]. Dostupné na WWW: <http://www.socialnisite.estranky.cz/clanky/historie-socialnich-siti.html>.
6. KOLERUSOVÁ, M. *Sunitka.cz.* Proč přemýšlet o ppc reklamě na Facebooku? [online]. 2011 [cit. 8. března 2013]. Dostupné na WWW: <http://www.sunitka.cz/c/74-proc-premyslet-o-ppc-reklame-na-facebooku>.

7. LAUSCHMANN, J. *Cdr.cz.* Největší sociální sítě dneška [online]. 2012 [cit. 9. března 2013]. Dostupné na WWW: <http://cdr.cz/clanek/nejvetsi-socialni-site-dneska>.
8. *Norton.com.* Nejlepší typy pro prevenci [online]. 1995 - 2013 [cit. 3. dubna 2013]. Dostupné na WWW: <http://cz.norton.com/prevention-tips/article>.
9. *Novinky.cz.* Na uživatele Facebooku číhají zákeřné černé díry [online]. 2012 [cit. 29. března 2013]. Dostupné na WWW: <http://www.novinky.cz/internet-a-pc/bezpecnost/275993-na-uzivatele-facebooku-cihaji-zakerne-cerne-diry.html>.
10. SELIMOVIČ, M. *Zcu.cz.* Kriminalita a web [online]. 2002 [cit. 28. prosince 2012]. Dostupné na WWW: <http://home.zcu.cz/~mselimov/ins/Druhy.html>.
11. SOCIÁLNÍ SÍTĚ. In *wikipedia: the free encyklopedia* [online]. Poslední aktualizace 23.3.2013 [cit. 5. března 2013]. Dostupné na WWW: <http://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5>.
12. VAŇURA, M. *Novinky.cz.* Děti na internetu chytají do pastí falešné celebrity [online]. 2012 [cit. 1. března 2013]. Dostupné na WWW: <http://www.novinky.cz/internet-a-pc/272272-deti-na-internetu-chytaji-do-pasti-falesne-celebrity.html>.
13. ZÁŠKOLNÝ, J. *123abc.cz*. Informace o sociálních sítích na internetu ve světě i České republice [online]. 2011-2013 [cit. 9. března 2013]. Dostupné na WWW: <http://www.socialnisite.123abc.cz>.

Přílohy

Příloha - Dotazník

Dotazník na téma počítačová kriminalita a její příčiny

Dobrý den, jsem studentem 3. ročníku oboru Bezpečnostně právní činnost na VŠERS v Příbrami. Rád bych Vás poprosil o vyplnění dotazníku, který bude součástí mé bakalářské práce. Veškerá data budou zpracována anonymně. Děkuji

1. **Používáte internet každý den?**

   a) Ano b) Ne

2. **Setkali jste se již s napadením vašeho počítače během surfování na internetu?**

   a) Ano b) Ne

3. **Používáte legálně zakoupený antivirový program s pravidelnou aktualizací?**

   a) Ano b) Ne

4. **Setkali jste se již s kyberšikanou na internetu, ať už vy samy nebo někdo z vašeho okolí?**

   a) Ano b) Ne

5. **Máte založený profil na sociální síti?**

   a) Ano b) Ne

6. **V případě, že ano - Máte profil na jedné nebo více sociálních sítích?**

   a) Mám profil na jedné sociální síti b) Mám profil na více sociálních sítích

7. **Uveďte, na které sociální síti:**

   O) Facebook O) Twitter O) Myspace O) Google+ O) Jiný ……

8. **Setkali jste se již s napadením vašeho profilu na sociální síti nebo zneužitím vámi uvedených údajů?**

   a) Ano b) Ne

9. **Znáte osobně všechny „přátele“, které máte na sociálních sítích?**

   a) Ano b) Ne

10. **V případě, že ne, v kolika procentech je neznáte?**

    a) 1-25% b) 26-50% c) 51-75% d) 76-100%

11. **Máte strach ze zneužití vašich údajů na sociálních sítích?**

    a) Ano b) Ne