Využití informačních technologií v problému šikany z pohledu PČR

USING OF INFORMATION TECHNOLOGY IN BULLING PROBLEM OF VIEW THE PERSPECTIVE PCR

Ing. Jiří Zamazal

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ing. Jiří ZAMAZAL**
Osobní číslo:	**A09814**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Učitelství informatiky pro střední školy**
Téma práce:	**Využití informačních technologií v problému šikany z pohledu Policie České republiky**

Zásady pro vypracování:

1. **Zpracujte úvod do problematiky.**
2. **Vymezete základní pojmy.**
3. **Pojednejte o problému šikany, rozdělení druhy.**
4. **Proveďte vlastní průzkum – dotazníková akce.**
5. **Řešení problému z pohledu PČR.**
6. **Vyhodnoťte a vypracujte závěr.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ŘÍČAN,P.: Jak na šikanu, Praha Portál 1995, 95 s. ISBN: 80-7178-049-9**
2. **PöTHE,P.: Dítě v ohrožení, Praha : 1999 186 s, ISBN: 80-86103-21-8**
3. **ERB H., Násilí ve škole a jak mu čelit, Praha 2000, ISBN: 80-86299-22-8**
4. **GAJDOŠOVÁ E, HERÉNYOVÁ G.: Rozvíjení emoční inteligence žáků, prevence šikanování intolerance a násilí mezi dospívajícími, Praha : Portál, 2006 324 s. ISBN: 80-7367-115-8 (brož.)**
5. **CHROMÝ J.:Kriminalita páchaná na mládeži Praha 2010 239 s., ISBN:978-80-7201-825-3**
6. **WEBSTER-DOYLE : Proč mě pořád někdo šikanuje? Praha : Pragma, c2002 Fyzický popis: 144 s. ISBN: 80-7205-804-5 (brož.)**
7. **VANÍČKOVÁ E., Interpersonální násilí na dětech Praha 2009 37 s. ISBN: 978-80-7440-001-8 (brož.)**

Vedoucí diplomové práce: **RNDr. Ing. Miloš Krčmář**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **20. července 2011**

Termín odevzdání diplomové práce: **2. září 2011**

Ve Zlíně dne 26. července 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce je zaměřena na problematiku kyberšikany, která s vývojem informačních technologií zaznamenala prudký vzestup. Je popsána obecná problematika šikany z hlediska historického, psychologického, a gradace agrese v České republice.

Kapitola o kyberšikaně, je doplněna o charakteristiku kyber útočníků a prevenci proti nim.

Druhá polovina práce těží z vypracované dotazníkové akce, která je důležitým podkladem k vyhodnocení informací od respondentů. Obsahuje návod na zjišťování, odhalování IP adres a detekci mobilu, které jsou jedním z nejčastějších prostředků provozování kyberšikany.

Klíčová slova: Kyberšikana, informace, bezpečnost, hesla, IP adresa, Policie České republiky, počítačový útok, agrese, kyberútočník.

ABSTRACT

The work is focused on the issues of cyberbullying, which with the development of information technology has seen rapid growth. It describes the general problem of in historical and psychological terms and quantifies the gradation of aggression in the Czech Republic.

The chapter on cyber-bullying is accompanied by characteristics of cyber attackers and preventitive counter measures.

The second half of the work benefits from a prepared questionnaire, which is an important basis for the evaluation of information from respondents. It includes instructions for detecting, identifying IP addresses and cell phone identification, which is one of the most common mediums for cyberbullies.

Keywords: Cyberbullying, information security, passwords, IP address, the Czech Police, computer, attack, aggression, cyberattaker. .

Touto cestou bych rád poděkoval vedoucímu diplomové práce panu RNDr.Ing. Miloši Krčmářovi a dále panu Ing. Petru Vojtkovi (oba z UTB Zlín) za cenné rady při technickém popisu v praktické části diplomové práce.

Veškeré informace uvedené v této práci byly konzultovány s analyticko-operativním týmem Policie České republiky ve Zlíně a schváleny k publikování.

Prohlašuji, že

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

soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně:

…….

podpis diplomanta

OBSAH

ÚVOD

V dnešním světě plného násilí a teroru se šikana stává, zcela běžným, společenským, negativní jevem, který se v naší civilizaci objevuje se vzrůstající intenzitou.

Z klasické fyzické šikany, tak jak ji všichni známe, se vytvořil nový druh mnohem nebezpečnější podoby psychického násilí využívající možnosti informačních technologií.

V dnešní civilizaci zaujímají mobilní telefony a počítače postavení prostředků a nástrojů, kde se v současnosti odehrává skrytá hra mezi agresorem a jeho obětí.

Cílem práce není tedy již opakovat stále stejnou, formulku o klasické šikaně. Ta je dobře známá a popsaná ve stovkách článků, knih a odborných periodikách. Zaměřuje se na současný problém, který se rozehrává v naprosté anonymitě na poli informačních prostředků. Důležitou součástí práce je věnována historii šikany a biologickému základu agrese, zejména počátku zrodu agresora a jeho následným rozvojem v kyberútočníka, která je v knihách či článcích o šikaně velmi často opomíjená a neprávem odsunuta na vedlejší kolej, jako nesledovaná.

Motivem této práce je vysvětlení rozdílů mezi klasickou šikanou a kyberšikanou, obsahuje vyhodnocení výsledků průzkumu o kyberšikaně a způsoby odhalování nástrojů agresora vyhledáním jim používaných IP adres. V práci jsou uvedeny možné zákonné postupy Policie České republiky při odhalovaní této nové, závažné trestné činnosti, i způsoby, zda orgán činný v trestním řízeni je schopen svými schopnostmi a prostředky tuto trestnou činnost eliminovat na co nejnižší možnou úroveň.

INTRODUCTION

In today's world full of violence and terror, bullying is common; it is a negative social phenomenon that occurs in our civilization with increasing intensity. Conventional physical bullying, as we all know it, has spurned a new kind of -more dangerous form- of psychological violence. Which abuses the benign possibilities presented by information technology. In today's civilization many tools use mobile phones and computers giving the devices a high social importance; creating the oportunity for an agressor to exploit this to victimise another. The aim of work is therefore not to repeat the analysis of the classical bullying formula: It is well known and described in hundreds of articles, books and specialist periodicals. This text focuses on the current problem, which is increasing within the vastly anonymous data fields of information technology. An important part of the work, to set the subject in context, is devoted to the history of bullying and the biological basis of aggression; especially the early aggressor birth and subsequent development in kyberútočníka that is often overlooked and unjustly relegated to the sidelines, as untracked, in books or articles about bullying.
The motive of this work is to explain the differences between traditional bullying and cyberbullying; to this end it includes the evaluated results of a survey observing cyber-tools and methods of detecting the aggressor via the IP address system. The paper lists the possible legal procedures available to the Czech Police for detecting this new, serious crime; and ways that criminal proceedings is capable of curtailing the active criminals abilities, and means to reduce this crime to the lowest level possible.

I. TEORETICKÁ ČÁST

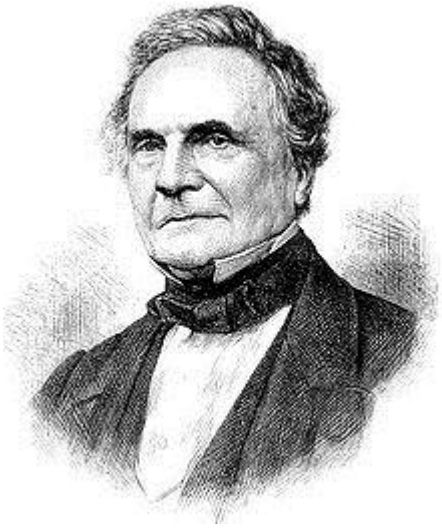
1 ZÁKLADNÍ INFORMACE

1.1 Počítač

Jedná se elektronické zařízení, které za pomocí vytvořeného programu zpracovává data. „Počítač se skládá z hardwaru, jedná se o fyzickou část počítače (procesor, monitor atd.) a ze software, který zahrnuje operační systém a vytvořené programy.

Počítač je ovládán uživatelem, který poskytuje počítači příkazy ke zpracování prostřednictvím periferních zařízení. V současnosti jsou počítače využívány téměř ve všech oborech lidské činnosti.“

Vynálezce počítače Charles Babbage, vymyslel v 19. století základní principy fungování mechanického stroje, který řešil složitější výpočty. Za první takto sestrojený a funkční počítač první generace lze považovat elektronkový ENIAC dokončený v roce 1946, který obsahoval až 17 468 elektronek, vážil 27 tun, zabíral 63 m² a spotřeba elektrické energie byla 150 kW. Samotný vývoj tohoto prvního počítače stál v tehdejší době okolo 500 000 dolarů ! Druhá generace počítačů proběhla v letech 1951 až 1965 s použitím tranzistorů, které zlepšily všechny parametry počítačů. Třetí generace je charakteristická použitím integrovaných obvodů a proběhla v letech 1965 až 1980. S rozvojem počítačových sítí, mikroprocesorů a se kterou vznikl Internet je charakteristická čtvrtá generace počítačů od roku 1981.[14]



Obr. 1 Charles Babbage

1.2 IP adresa

Jedná se o jedinečnou adresu počítače v síti, která se udává ve tvaru : yyy.yyy.yyy.yyy, kde yyy je číslo v rozsahu 0 až 255 - čili jeden bajt, jelikož jsou bajty 4, je tedy tato adresa 32 bitová (1 bajt= 8 bitů-> 4x8 = 32), to je standard IPv4, 128 bitová adresa je u standardu IPv6. IPv4 adresa může být například: *85.25.151.22,* kvůli lepší přehlednosti může IP adresa mít i přiřazeno tzv. doménové jméno.

IP adresa může vlastnit i mnohem více doménových jmen, jedná se o princip virtuálních serverů na jednom stroji, kdy příkladem může být webhosting. Jakákoliv společnost vlastnící jeden server poskytuje pro více zákazníků více domén. Jedno zařízení může vlastnit více IP adres.

Nezanedbatelným pojmem je zmínit se o reverzním záznamu IP adresy. Domain Name Server, neboli také DNS neposkytuje pouze mechanismus překladu doménových názvů na IP adresy, ale též poskytuje překlad na doménová jména z IP adres. Využití najdeme dnes především při doručování elektronické pošty. Mailserver, přijímající zprávu od odesilatele, přeloží IP adresu klienta na název (zde může jít o primární detekci odesílatele) a poté si získaný název přeloží zpětně na IP adresu. Za nedůvěryhodný zdroj zprávy může považovat už jen tu skutečnost, kdy mu získaná IP adresa nesouhlasí a může jej tedy odmítnout.

Samotné reverzní záznamy mohou napomoci při pátrání jako pomůcka po původu IP adresy. Pokud máme fiktivní případ, kdy na náš počítač se pokoušel připojit případný hacker či útočník z IP adresy 88.100.88.36. Vneseme-li dotaz na reverzní záznam k příslušné IP adrese, dozvíme se název „36.88.broadband5.iol.cz“ z kterého můžeme vyčíst, že je útočník připojen od poskytovatele IOL.cz zřejmě přes ADSL. Bohužel se musíme i ztotožnit s faktem, že reverzní záznamy nemusí odpovídat skutečnosti. [10]

1.3 Mobilní telefon

Jedná se o elektronické zařízení na dálkový přenos informace mluveným slovem, případně textovou nebo multimediální zprávou. Pomocí technologie WAP umožňuje připojení k internetu a provoz dalších elektronických služeb. Slouží k vysíláni i k přijímání dat v síti GSM za pomocí vložené aktivní SIM karty. U nejnovějších mobilů se používá konvenčního telefonního přepojování okruhů a kombinaci přenosu radiových vln. Mezi

nejznámější výrobce dnešních mobilů patří především značky : Nokia, Samsung, LG, Sony Ericsson, Apple a další. [8]

1.4 Policie České republiky

„Jedná se o jednotný ozbrojený bezpečnostní sbor, který je zřízený zákonem České národní rady ze dne 21. června 1991 a je podřízena ministerstvu vnitra. Úkolem Policie české republiky je chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Policie dále plní rovněž úkoly dle :

- trestního řádu
- úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony,
- předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky.

Policie České republiky je dále rozdělena na policejní prezidium, útvary s celostátní působností, na 14 krajských ředitelství policie, jejichž územní obvody se shodují s územními obvody 14 krajů České republiky. Policie České republiky k dnešnímu dni prezentuje zhruba 46 000 policistů a 11 000 zaměstnanců policie. Policie je podřízena Ministerstvu vnitra ČR. Inspekce policie, dříve Inspekce ministra vnitra prověřuje trestnou činnost policistů. Tísňová linka policie je 158 a je zdarma.

Priority činnosti Policie ČR:
bezpečnost osob a majetku
ochraňuje veřejný pořádek
Vede boj proti terorismu
Podílí se na odhalování pachatelů a trestných činů

v trestním řízení vystupuje jako policejní orgán
zajišťuje ochranu státních hranic
zajišťuje ochranu ústavních činitelů a bezpečnost chráněných osob
zajišťuje ochranu zastupitelských úřadů, ochranu sídelních objektů Parlamentu, prezidenta republiky, Ústavního soudu, Ministerstva zahraničních věcí, Ministerstva vnitra a dalších objektů zvláštního významu
zajišťuje bezpečnost a plynulost silničního provozu

Tabulka č.1

Policisté jsou dle zákona ve služebním poměru, který vymezuje také služební poměr pracovníků v dalších bezpečnostních sborech jako jsou hasiči či vězeňská služba.“ [12]

Obr 2. Aktuální barevné označení policie na služebních vozidlech

1.5 Mládež

Jedná se o sociálně-demografickou skupinu v rozmezí věku od 15 do 30 let. Tato sociální vrstva se vyznačuje charakteristickými rysy, vlastnostmi a specifickými zájmy, které jsou odlišné od jiných generací. Období mládeže bývá charakteristické prvním kontaktem s

výdělečnou činností, přijímáním a postupným zdokonalováním společenských norem a pravidel a s formováním vlastního pohledu na život.

Z právního hlediska byl pojem „mládež“ obsažen již v trestním zákoníku z roku 1961. V současné době je aktuální trestní zákoník č. 40/ 2009 Sb. [1]

1.6 Kriminalita

Jedná se o páchání trestných činů či přestupků. Věkové rozmezí pro kriminalitu mladistvých je od 15 do 18 let, kriminalita dospělých je definována nad hranicí 18 let. Je nutné dále rozlišovat tzv. mladé dospělé s věkovou hranicí od 18 do 24 let.

U kriminality mladistvých je charakteristické věkové rozmezí od, kdy toto období je považováno jako kritické. U jedince v téhle fázi věku formují hlavní rysy osobnosti. Vliv vrstevníků bývá zde velmi silný a jedince jí často velmi vyhledává už jen pro pochopení svých soc. potřeb a názorů, které ve většině případech u generaci starších rodičů většinou nedostává. Mezi nejčastější delikty u mladistvých můžeme zahrnout : násilí proti jednotlivci či skupině , opilství a výtržnictví , vandalismus či toxikománie. [1]

1.7 Netiketa

Jedná se o soubor pravidel chování ve virtuálním světě, který vymezuje tzv. pojem netiketa, které je odvozeno z anglického slova *net*, nebo-li síť a dále ze slova *etiketa*. Pravidla chování na internetové síti jsou stejné, nebo velmi podobná jako jsou ve skutečném životě.

Na rozdíl od reálného světa je internetová síť odlišná ve své anonymitě, která může zakrývat i někdy nepříjemnou realitu. Dále je charakteristická svojí neosobností, kdy uživatelé se chovají jinak než při osobním setkání z očí do očí a naivně se domnívají, že v tomto virtuálním světě je není možno nikdy dohledat. [6]

2 ŠIKANA

2.1 Historie šikany

Hovořit o historii šikany znamená zmínit se o historii školního vyučování. U dětí je naprosto typické, že silnější jedinec ubližuje těm slabším, ať již z důvodu zlomyslnosti či krutosti. Ve staré Anglii byla na internátních školách šikana na denním pořádku, kdy starší chlapci si podřizovali mladší, ponižovali je, bili je a museli jim sloužit. Za poslední dekádu vzrostla celková agresivita mládeže, kterou dokládá statistika násilných trestných činů. Starší pedagogové a především odborníci upozorňují také na zcela nový a překvapující druh tzv. nemotivované násilí, kdy jde o krutost bez prožitku vzteku, nenávisti, a bez sadistického uspokojení. Chlapec bezdůvodně udeří do hlavy dívku, kterou vůbec nezná, a to vše jenom tak. Dle výzkumu ze Spojených státu Amerických přiznalo 25 % dětí strach ze šikany jako největší obavu, která souvisí s návštěvou školy.

I když byla šikana popsána v desítkách, ne-li stovkách knih a publikací, vědecká diskuse o tomto problému však začala až v roce 1969 ve Skandinávii. Tak markantní zpoždění ve výzkumu šikany doposud nebylo vysvětleno. Jak je možné, že tak důležitý problém šikany byl tak dlouho přehlížen ? Problém šikany byl zpočátku chápán, jako akce větší skupiny, která se bez „sebekontroly“ vrhá na svoji oběť. Z hlediska sociální psychologie je tento jev velmi zvláštní, abnormálně nebezpečný, ale ne příliš častý jev. Dan Olweus začátkem sedmdesátých letech pracoval na vědecké práci, kdy šikanu definoval jako neustálou a opakovanou agresi jedince nebo skupiny proti slabší skupině obětí či slabému jedinci. [7]

Obr. 3 Dan Olweus, Ph.D.

Dan Olweus ve své vědecké práci upozorňoval na skutečnost, že šikana je jedním z nejrozšířenější problémů, který ohrožuje mravní a především duševní vývoj dětí.

Do podzimu 1982 ignorovaly školské úřady v Norsku výsledky, kterých dosáhl během svého výzkumu tento norský odborník. Místní noviny tehdy zveřejnily tři případy sucidií studentů od 10-14 let v severním Norsku, kdy příčinou byla šikana z řad spolužáků. Veřejnost byla pobouřená touto událostí, která nakonec přinutila ministerstvo školství k celostátní kampani v boji proti šikaně na všech školách.

Koncem osmdesátých let minulého století se začaly objevovat první studie a knihy s problematikou šikany také v Anglii, ve Spojených Státech Amerických, Austrálii a v Japonsku, dokládající závažnost tohoto problému. K problému šikany se pořádají světové konference a šikana se stává nezanedbatelným problémem.

Dan Olweus a další badatelé se podrobněji zabývali tímto problémem, studovali např. jaká osoba se stává nejčastěji obětí agrese, charakterem útočníků, z jaké společenské vrstvy nejčastěji pochází, i jaké postavení k šikaně zaujímají učitelé a rodiče apod. Neméně důležité jsou i sekundární vlivy šikany, zda na oběti zanechá dlouhodobé následky, nebo jakého vývoje může chování agresora až dosáhnout. Poslední výzkumy jsou zaměřeny především zaměřeny na mladistvé, na jejich obecný vztah k šikaně i na analýzu jejich chování při kontaktu se šikanou. Prioritou nadále zůstává hledání a oživování nejúčinnějších postupů v prevenci a v boji proti šikaně.

V České republice se věnuje problému šikany ve škole uznávaný odborník a zkušený poradce Michal Kolář, známý při řešení závažných případů na středních odborných učilištích a školách již od počátku osmdesátých let. Pod jeho záštitou v roce 2004 proběhla první celostátní konference o šikanování ve školních lavicích..Z nejznámějších knih a publikací ,zabývající se tímto tématem ,lze doporučit Říčanovu knihu „Agresivita a šikana mezi dětmi“ z roku 1995, „Skrytý svět šikanování“ od M. Koláře vydaná v roce 1997 a „Bolest šikanování“ publikovaná před deseti lety. [7]

2.2 Biologický základ agrese

Pokusme si zodpovědět otázky, které si klade většina lidí :„Kde se bere v některých jedincích tolik agrese ? Je agrese již vrozená,nebo se dotyčný stává agresivním až průběhu svého života, například vlivem nesprávného způsobu výchovy ?

Už v přírodě se můžeme setkat s tím, že samotní živočichové se chovají agresivně ke stejnému druhu vlivem svých vrozených instinktů. U lidí také dochází k agresivitě na základě svých vrozených instinktů,ale vznik agresivity je mnohem složitější než je tomu u zvířat. Pokud se člověk například žene za velmi důležitým cílem a má ho již na dosah a někdo mu jeho záměr překazí – dochází z jeho strany k agresivnímu chování. Zvířata mají na rozdíl od člověka , na různé situace již předem dané vrozené reakce.

Vrozené instinktivní reakce můžeme u člověka přirovnat k „programu“, který nás instruuje k tomu, abychom v jistých případech napadli jiného lidského jedince, v další situaci například abychom mu podali pomocnou ruku a jindy se mu obloukem vyhnuli atd. Naše instinkty nám vládnou jen omezeně, člověk je může a musí potlačit svým rozumem .i když v některých situacích je vliv instinktů nemalý.

Vlivem prostředí se u jedince vyvine ze skupiny instinktů pud, tedy vnitřní puzení k formování svého chování . U člověka existuje větší či menší pudová energie, kterou jedinec potřebuje filtrovat a může hledat možnost k jejímu vybití.

Položme si tedy otázky: „Je lidská agrese pud? Existuje v jedinci jakési puzení, které si vynucuje a někdy i stupňuje, abychom na jedince z okolí zaútočili, vedli s ním boj a snažili se mu přivodit bolest, ponížení a vyhrát nad nim ?“

Každý člověk nosí v sobě, buď silnější nebo slabší agresivní potenciál, který následně přechází do citového uspokojení při jeho vybití ,a šikana je jedna z možností, kde i nejmladší z nás si svoji agresivní energii vybíjejí.

Je nutné si uvědomit i další faktory :

- Nejedná se o stejnou energii, jako ve fyzice. Když se člověk pro něco nadchne, a současně nepůsobí podněty, které by projevy agresivního pudu „spouštěly“, tato energie se neshromažduje.
- Energie, která se nashromáždí vlivem agresivního pudu lze vybít sportem nebo fyzickou i duševní činností [7]

- Neméně důležitou roli, zde zaujímá kultura. Naše společnost je silně soutěživá a proto zde mezi jedinci dochází k agresivitě při touze vítězit, což má v důsledku vliv i na potomky, které jsou součástí naší společnosti.
- Agresivita chlapcům vůči dívkám bývá spojena se sexuální zájmem.

Velmi nebezpečné jsou pro člověka pudy, které bývají nejmocnější co se týče energetický potenciálu jedince. Nejednou se můžeme setkat s tím, že rozumová kontrola selže vlivem působení velkého vzrušení a tlakem k jejímu uplatnění. Hovoříme-li o agresi, překvapuje nás její existence při násilích ve válkách, u fascinace a nepopsatelné rozkoši jedince při účasti na popravách , při ponižování , při mučeni druhých. Už z historie víme, že lidé se často zúčastňovali veřejných popravy. Všechny společnosti směřují k tomu, aby přirozená agresivita byla utlumena na přijatelnou úroveň a navíc, aby byla pozitivně využita.

U ponižování a mučení dochází u některých jedinců ke zvláštnímu druhu uspokojeni spojené často s neobvyklými a těmi nejtajnějšími přáními s nim spojené, na které se obecně ‚špatně hledá odpověď. Ponižovat či mučit člověka, se považuje vždy za experiment: „Jak se zachová dotyčná oběť ve strachu z bolesti a jaké jsou možnosti a hranice tohoto druhu experimentu ?“

To je velmi vzrušující otázka, možná tím více vzrušující, že zároveň víme: Na tuto otázku nemáme právo! Mučitel (i mučený) cítí, že takováto situace člověka duševně obnaží , takže je možno podívat se až na dno jeho bytosti, která je v tu chvíli jako by rozložena. Jde o to vypáčit z člověka jeho tajemství.

2.2.1 Definice pojmu šikana

Pod pojmem šikana je zahrnuto ubližování , ponižování jedince nebo skupiny lidí, které bývá opakované nebo jednorázové. Jde o ubližování jedinci mající nejen stejné společenské postavení jako agresor (kolega na pracovišti, mezi spolužáky), ale i o ubližování jedinci z jiné společenské vrstvy (žáka-agresor napadá svého vyučujícího pedagoga). Nastává zde tzv. osobní asymetrický vztah moci, kdy si je oběť vědoma, kdo je v roli agresora a zná už jeho destruktivní záliby a manýry. [7]

- Pro šikanu je celkově charakteristické, že oběť se nemůže bránit, což bývá zapříčiněnou rozumovou, osobní či tělesnou zaostalostí, nebo jen početní převahou agresorů nad oběti.
- Příčina šikany je velmi individuální, prioritu však drží vlastnosti oběti, i agresora.
- Motivy šikany zahrnují celou škálu možností od pobavení spolužáků až po sadistické uspokojování agresora z potlačování lidské důstojnosti oběti , vedoucí k upevnění moci v kolektivu. Agresorovi přináší šikana nejen materiální zisk (ukradené peníze či věci), ale i další služby spojené s zotročováním své oběti na dobu neurčitou.

2.2.2 Druhy šikany

Šikanu rozlišujeme na **:**

*Přímou šikanu***,** která je pro agresora charakteristická agresivním chováním, jako je ničení a zmocnění osobních věcí oběti např. části oděvů, školních pomůcek, stravy , ale také i verbálními urážkami jednotlivce. Tento druh šikany je charakteristický i zotročováním oběti, jako jsou různé druhy úslužných prací.

*Nepřímou šikanu***,** která je typická v sociální izolaci žáka, kterého ostatní schválně přehlížejí. Takový způsob šikany bývá v některých případech mnohem nebezpečnější než první forma šikany. Oběť na důkaz solidarity s kolektivem si nechá klidně zhoršit školní prospěch, a to jen aby zapadl mezi spolužáky.

Velmi často se kombinují oba druhy šikany, kdy přímá šikana přechází postupně v nepřímou či naopak. Různé bývají i formy šikany, kdy převládá bud sexuální či rasově motivovaný zájem agresora.

Podle Koláře (2005) lze rozlišit tyto druhy agrese :

- Agrese za použití fyzické síly, kterou agresor používá k ovládnutí své oběti
- Verbální agrese a vyvolání strachu, kterou agresor psychicky paralyzuje svoji oběti a manipuluje s ní.
- Odcizení, znehodnocení věcí – zde dochází k destruktivnímu jednání agresora zaměřené na školní pomůcky (sešity nebo psací potřeby aj.) patřící oběti. [3]
- Příkazy agresora – jedná se o příkazy směřované za účelem uspokojení

agresora tím, že oběť vykonává všestranné a nepříjemné úkoly uložené agresorem.

2.2.3 Charakteristické rysy oběti :

Různí autoři zabývající se problematikou šikany popisují charakteristické rysy oběti následovně :

- Jde o bezbranného jedince, který se vymyká od vrstevníků (např. obezita, nošení optických brýlí aj.)
- Není na dostatečné fyzické úrovni jak vrstevníci, bývá spíše plaché povahy a tak moc nenavazuje osobní kontakt s ostatními.
- Duševně jde o nadprůměrného jedince, který vyniká v oboru. Je jiné národnosti a v uvažování nebývá bystrý jak vrstevníci. [4]

2.2.4 Charakteristické rysy agresora

Charakteristické rysy agresora popisuje M. Kolář z roku 1997 takto :

- Jde o tělesně nadprůměrného jedince s arogantním jednáním a s celkovými kázeňskými problémy.
- U vrstevníků je oblíbený zastávající funkci „nejvyššího“, méně nadaný, ale velmi nebezpečný pocházející většinou z psychicky nevyrovnané či jinak „postižené“ rodiny.
- Často kryje své agresivní jednání za zcela něco normálního a běžného a možnost nevhodného chovaní si nepřipouští, alibi mu poskytují jeho příznivci. [4]

2.2.5 Typy agresora

Rozdělení agresorů popisuje Říčan (2010) následovně :

- **Hrubý typ agresora"** – ne příliš inteligentní jedinec s impulsivním chováním, neuznává autoritu jiného, bývá členem podobně smýšlející skupiny. Jde o jedince z narušené rodiny a své oběti šikanuje bezlítostně a tvrdě
- **Elegantní typ agresora"** – společenský, inteligentní se zvýšenou psychickou citlivostí a s rafinovaným šikanováním své oběti.

- **"Smíšek"** – velmi veselé povahy, citově nestabilní se značným sebevědomím, prosazující v kolektivu rád své názory. Svoji oběť vystavuje šikaně pro pobavení své a svých vrstevníků. [7]

2.2.6 Následky oběti šikany

Popisuje Řezníčková (2008) ve své publikaci následovně :

- Jedná se o nenávratné psychické a mnohdy i fyzické poškození, který zapříčiňuje u dítěte další negativní následky jeho psychického vývoje.
- U dítěte zapříčiňuje dlouhodobá šikana jakékoliv přetrhání citových kontaktů mezi blízkými.
- Dochází ke ztrátě z autority a ke ztrátě o pozitivním smyslu života, kdy oběť přestává doufat o ochranu či podporu ze strany společnosti. [13]

2.2.7 Postup při podezření ze šikany

Internetového portál na www.zsmikulasezhusi.cz radí následující :

- Velmi důležitá je psychická podpora oběti a dále je důležité snažit se vypátrat veškeré informace k případu
- Oběť nechat lékařsky ošetřit a ponechat mimo kontakt s útočníky.
- Důležité je v tomto případě osobní řešení, nikoliv telefonické či dokonce po mailu a požádat o pomoc kompetentní pracovníky, v krajním případě i školní inspekci.
- Dítě, které se stalo obětí šikany nechat ve škole mimo kontakt s útočníky, nejlépe přeřazeni na jinou školu.
- Kontaktovat Policii České republiky pokud máte podezření na páchání trestného činu ze strany útočníka.

2.2.8 Trestní odpovědnost pachatelů šikany

Pojem šikana je v právní praxi používán jako synonymum pro „úmyslné jednání, které je namířeno proti jinému subjektu, útočící na jeho důstojnost". Není důležité, zda k němu dochází slovními útoky, fyzickou formou nebo hrozbou násilí. Dále musí být splněny tyto podmínky:

- pachatel se dopustil jednání, které splňuje znaky konkrétního trestného činu
- musí být prokázán úmysl pachatele dopustit se takového jednání a míra společenské nebezpečnosti
- jeho jednání dosahuje intenzity uvedené v zákoně

Musí být prokázán úmysl pachatele dopustit se takového jednání a musí být prokázána míra
společenské nebezpečnosti.V současnosti dle nového trestního zákoníku mluvíme o společenské škodlivosti, společenská nebezpečnosti již neexistuje. Dále dle ust. § 13 a § 14 nového trestním zákoníku dělíme trestné zločiny, dle trestní sazby. činy na přečiny a v současnosti již musíme postupovat dle nového trestního zákoníku č. 40/2009 Sb., a ne podle trestního zákona č. 140/1961Sb. [12]

Šikana bývá nejčastěji postihována podle ustanovení trestního zákoníku č. 40/2009Sb., a to jako:

- trestný čin (pokud půjde o odst. 1,2, tak jde o přečin, pokud půjde o odst. 3, 4, tak jde o zločin- omezování osobní svobody dle ust. § 171 trestního zákoníku
- trestný čin (pokud půjde o odst. 1, tak jde o přečin, pokud půjde o odst. 2,3,4 jde o zločin) vydírání dle ust. § 175 trestního zákoníku
- trestný čin útisku (pokud půjde o odst. 1, 2 , jde o přečin, pokud půjde o odst. 3, jde o zločin útisk dle ust. § 177 trestního zákoníku
- trestný čin - zločin loupeže dle § 173/1,2,3 trestního zákoníku
- trestný čin ublížení na zdraví (pokud půjde o odst. 1 jde o přečin, pokud o odst. 2, 3, 4 jde o zločin dle ust. § 146 trestního zákoníku.
- trestný čin poškozování cizí věci (pokud půjde o odst. 1,2,3 jde o přečin, pokud o odst. 4 zločin dle ust. § 228 trestního zákoníku
- trestný čin - zločin znásilnění dle ust. § 241/1,2,3,4 trestního zákoníku (neboť již v prvním odstavci je stanovena trestní hranice pět let)
- trestný čin - zločin pohlavního zneužívání dle ust. § 187/1, 2, 3, 4 trestního zákoníku. [5]

„K tomu, aby byl pachatel postižen, musí být starší 15 let (15-18 let mladiství). Děti mladší 15 let trestně odpovědné nejsou, jsou však předány do péče orgánu sociálně - právní ochrany, případně mohou být postiženi jejich rodiče. Nezletilému pachateli je možné nařídit ústavní výchovu, může nad ním být stanovený dohled. Pokud jde o trestní sazby, je v případě šikany možný i jednočinný skutek, tzn. že jedno jednání může být kvalifikováno jako více trestných činů. Pokud k šikanování došlo v průběhu vyučování, nese plnou odpovědnost škola. Prokáže-li se zanedbání ředitele školy nebo některého pedagoga, může být právně nebo pracovněprávně potrestán. Na školském zařízení lze v oprávněných případech požadovat i náhradu škody vzniklé v důsledku šikany. A to jak náhradu na věcech, tak na zdraví, včetně způsobené psychické újmy. Pokud dítě v důsledku šikany nemohlo např. docházet do školy (vyšší stupeň šikany), nese školské zařízení odpovědnost i škody vzniklé rodičům dítěte v důsledku např. uvolnění ze zaměstnání, zajištění hlídání dítěte, zajištění doprovodu do a ze školy apod.“ [1]

2.2.9 Postavení dítěte v roli poškozeného v trestním řízení

„V právní terminologii je poškozený ten, jemuž bylo ublížení na zdraví, způsobena majetková , morální nebo jiná škoda. Má právo činit návrhy na doplnění dokazování, nahlížet do spisů, zúčastnit se hlavního líčení a veřejného zasedání konaného odvolání a před skončením řízení se k věci vyjádřit. Na základě konstantní judikatury se uzavírá, že nezletilé osoby nemohou v trestním řízení vykonávat práva poškozených samy. Způsobilost nezletilců k právním úkonům zde není dána v plném rozsahu, a proto na tyto případy dopadá ustanovení § 45 odstavce 1 trestního řádu, aby výkony práv poškozených činili jejich zákonní zástupci. Zákonnými zástupci jsou v první řadě rodiče nezletilého. kteří ve smyslu § 36 ZOR zastupují dítě při právních úkonech a disponují plnou rodičovskou odpovědností. Jestliže se rodiče nezletilce neshodnou na tom, kdo z nich bude nezletilce v trestním řízení zastupovat, rozhodne soud v řízení ve věcech péče o nezletilé podle § 176. V případech, že žádný z rodičů nemůže zastoupit – vykonávat práva poškozeného dítěte – soud ustanoví dítěti opatrovníka, který bude při právním úkonu dítě zastupovat. Rozsah práv a povinností opatrovníka se vymezí z hlediska účelu, pro který byl opatrovník ustanoven. Opatrovník dále odpovídá za řádné provedení úkolů, kdy jeho funkce skončí provedením těchto úkonů – respektive skončením těchto úkonů.

Zákonným zástupcem nezletilého při uplatňování práv poškozeného v trestním řízení může být i poručník a to v případě, že oba rodiče zemřeli, byli zbaveni rodičovské zodpovědnosti, výkon jejich rodičovské zodpovědnosti byl pozastaven nebo nemají způsobilost k právním úkonům v plném rozsahu dle § 78 ZOR. V trestním řízení plní poručník výkon práv poškozeného nezletilce z hlediska zájmu nezletilce, odpovídá soudu za řádné plnění této funkce a podléhá jeho názoru.

Nezletilého poškozeného může zastupovat i osvojitel § 63 ZOR, neboť osvojením vzniká mezi osvojitelem a osvojencem takový poměr, jaký je mezi rodiči a dětmi. Osvojitelé mají rodičovskou zodpovědnost při výchově dětí.“ [1]

Výslech osoby mladší patnácti let v trestním řízení :

„Trestní řád neobsahuje zvláštní ustanovení, které by se vztahovalo k výslechu osoby poškozené. Na výslech této osoby se užijí tytéž ustanovení jako na výslech svědka, neboť postavení poškozeného zpravidla zakládá i postavení svědka jako nositele důkazu. K výslechu dětí lze přistupovat značně individuálně.

Podle § 101 odst, 1 trestního řádu platí, že před výslechem svědka je třeba vždy zjistit jeho totožnost, jeho poměr k obviněnému, poučit jej o právu odepřít výpověď, a je-li třeba, též o zákazu výslechu nebo o možnosti postupu podle § 55 odstavce 2 trestního řádu , jakož i o tom, že je povinen vypovědět úplnou pravdu a nic nezamlčet. Poučen musí být o významu svědecké výpovědi z hlediska obecného zájmu a o trestních následcích křivé výpovědi.

Hlavní odchylka pro výslech osoby mladší patnácti let stanoví § 102 trestního řádu. Základním předpokladem je, že tato osoba má být vyslýchána o okolnostech, jejichž oživování v paměti vy vzhledem k věku mohlo nepříznivě ovlivňovat její duševní a mravní vývoj. Posouzení těchto okolností závisí na orgánu činném v trestním řízení. Pokud je osoba mladší patnácti let vyslýchána o okolnostech, jejichž oživování v paměti by vzhledem k věku mohlo nepříznivě ovlivňovat její duševní a mravní vývoj, obligatorně se přibere pedagog nebo jiná osoba mající zkušenosti s výchovou mládeže, která by se zřetelem na předmět výslechu a stupeň duševního vývoje přispěla ke správnému vedení výslechu. Pedagogem se rozumí osoba rozdílná od vyslýchajícího, mající odpovídající pedagogické vzdělání. Jestliže by za splnění podmínek § 102 odstavce 1 trestního řádu došlo k opomenutí přibrat k výslechu pedagoga nebo jinou osobu mající zkušenost s výchovou mládeže, tato vada zakládá důkazní nepoužitelnost provedené výpovědi.

Výslech osoby mladší patnácti let se zpravidla provádí v přípravném řízení v souladu s § 164 odstavce 1 trestního řádu. Tento výslech se provede také v případě, že se jedná o neodkladný a neopakovatelný úkon. Při výslechu mladší patnácti let se zdůrazňuje prostředí, v němž výslech probíhá. Má být příjemné a pohodlné, aby mu skýtalo pocit bezpečí. Důraz je kladen na emociálně pozitivní atmosféru vedení výslechu, zdržení se hodnotících soudů a vkládání subjektivismů vyslýchajícího.“ [1]

3 KYBERŠIKANA

Kyberšikanu nebo-li cyberbullying lze definovat jako zneužití informačních komunikačních technologií k nezákonné komunikaci agresora s obětí., která ponižuje, vydírá a končí psychickým i fyzickým poškozením oběti.

Dle internetových portálů se nabízí i další možnost definice : „Kyberšikana (též kybernetická šikana, počítačová šikana či cyberbullying) je druh šikany využívající elektronické prostředky, mezi nejčastějšími internet, mobilní telefony, e-maily a dále pagery nebo blogy, kdy tyto samotné projevy můžou spadat do oblasti kriminálních činů. Mezi nejčastější právě řadíme zasílání urážejících, agresivních mailů nebo SMS, vytváření stránek či podobných blogů která ponižuje lidskou důstojnost skupiny či jednotlivce. Dalším způsobem kyberšikany je, že může posilovat klasické formy šikany. Mezi nejčastěji případy jsou uváděny : nahrávání situací na mobilní telefon, případně další rozeslání kamarádů či známým nebo samotné vystavení nahrávky na internetovém portálu. Pro dotyčnou oběť to většinou znamená mnoho násobně zvýšení utrpení z ponížení a v konečném důsledku i v změna či úplná ztráta společenského postavení.

U kyberšikany se jedná o specifickou formou klasické šikany, kdy jde o chování, jehož cílem je opakovaně agresivně útočit, ohrožovat jedince či skupinu lidí a to v „tváří v tvář“. Kyberšikana představuje virtuální realitu a to především tím, že nabízí jiné možnosti či nástroje ubližování a tím mění charakter celého procesu šikanování. Pro lepší názornost tomuto jevu bývají vyzdvihovány některé jeho charakteristické rysy uvedené v následujících odstavcích. [2]

3.1 Závislost na virtuálním světě

Každý z nás zná svojí nějakou osobní závislost. Někdo preferuje tabákové výrovky jiný alkoholické nápoje, ale s rozvojem informačních technologií dochází i k závislosti na internetu, u které zatím dle názorů psychiatrů neexistuje přesná diagnóza tohoto druhu problému. Samozřejmě existují určité indície, které napoví o tomto druhu závislosti, kdy mezi ty nejčastější ukazatele patří např. zda dotyčná osoba tráví u internetu více času než původně plánovala, cítí potřebu uspokojení z trávení času na internetu, nebo dokonce má psychické poruchy pokud zůstává delší čas mimo internet atd.

V souvislostí s kyberšikanou je nutné se zmínit o závislosti na vztahu prostřednictvím nejrůznějších profilů a webových seznamek tj. na kyber vztahu a na ještě mnohem nebezpečnějším tzv. kyber sexu, který se odehrává ve fantazii dotyčného přes chaty, skype a různé druhy komunikátorů a poskytují tak dotyčnému uspokojení někdy i několikanásobně větší, než osobní kontakt . Nemusí jít v tomto případě výhradně o návštěvu nejrůznějších porno a sex. stránek.

3.2 Anonymita

S využitím informačních technologií se kyberšikana oproti klasické formě šikany odlišuje už jen tím, že útočník může zůstat zcela anonymní a dotyčná oběť se nikdy nemusí dozvědět, kdo byl původcem tohoto druhu šikany. Oběť může znát dotyčného agresora, stejně i tak se s ním v životě nemusela nikdy potkat, protože si ji agresor vybral náhodou, třeba jen dle telefonního seznamu či jiné indície. Agresoři se skrývají za nejrůznější přezdívky, smyšlené emailové adresy. Internetové portály jim umožňují útoky stupňovat a dovolit si mnohem větší agresi než ve skutečném životě

3.3 Nezávislost na místě a čase

Agresor diky informačním technologiím nemusí být přítomen na stejném místě, jako jeho dotyčná oběť. Od klasické šikany se kyberšikana vyznačuje tím, že před ní nemůžeme se nikam schovat a to díky masmediálnímu rozšíření a snadné dostupnosti informačních technologií.

Kyberšikana nás může dostihnout prakticky kdykoliv a to i na místech dříve cítili bezpečných, jako je například domov. Agresorovi úplně postačí když vyvěsí na webu foto, nahrávku své dotyčné oběti, kterou si může kdokoli zkopírovat, stáhnout a šířit dále nejen po samotném internetu. [2]

3.4 Proměna útočníka a jeho oběti

Narozdíl od klasické šikany není zapotřebí proti kyberšikaně zapotřebí fyzická síla, ale především zdatnost a celkový přehled v informačních technologiích, kterou může mít v dnešním civilizovaném světě prakticky kdokoliv. Oběťmi útoků už nemusí být pouze outsideři z řad vrstevníků, mladších nebo slabších. Kybeberšikana se dnes odehrává nejen mezi kamarády a vrstevníky, ale může být i mezi různými generacemi, kdy není podstatný

či důležitý věk ani pohlaví. Významnou skupinou kybešikany se stává učitelský sbor na všech stupních a školách, které je charakterkteristická zveřejněním ponižujících a urážlivých materiálů na veřejných portálech s vysokou návštěvností. Riziko zde samozřejmě hrozí i těm nejmladším, které jsou již na mobilech nebo počítačích či internetu závislé.

3.5 Nesnadná kontrola a šiřitelnost u kyberšikany

U tohoto druhu šikany nejsou klasické znaky jako u normální šikany, kterých by si mohlo třeba rodiče dotyčné oběti všimnout, jelikož zprávy z Internetu nejsou snadno kontrolovatelné. Než se detekuje problém nebo možné nebezpečí, uplyne většinou delší doba. Proto se může kyberšikana mnohem rychleji šířit než klasická šikana, která probíhá většinou v uzavřeném okruhu.

3.6 Typy kyberšikany

Rozlišujeme tyto typy kyberšikany :

- **přímé útok**y, kdy jsou elektronické zprávy posílané od útočníka přímo obětem
- **kyberšikana v tzv. zastoupení,** která využívá ostatní pro šikanu ve virtuálním prostoru. Tento typ šikany je nebezpečnější, jelikož spolu agresoři se jí účastní nevědomky.

3.6.1 Přímé útoky

- Zveřejňování soukromých/ neveřejných informací nebo pomlouvání na blogu
- Přes zprávy SMS, po e-mailu nebo icq posílání nevhodných až výhružných zpráv
- Zneužívání hesel a poté i zneužití přivlastněného účtu.
- Odtajnění a následné zveřejňování intimních nebo nepravdivých informací a grafických podkladů či fotografií na internetových stránkách, či případné jejich rozesílání přes mobilní telefon – v tomto případě se jedná o nahrávky jak klasické šikany či nelidského zacházení s oběti.

- Rozesílání ponižujících fotografií přes mobil či pomocí mailové pošty – v nejčastějších případech jde o posílání fotografií či nahrávek kamarádů nebo pedagogů, kde bývá dotyčná oběť zesměšňována či ponižována.
- Typy otázek v hlasování na internetovém portálu, kde pouhý námět či samotná otázka má oběť zesměšňovat či ponižovat a které jsou vytvořeny blízkou osobou či osobou z blízkého okolí. Jde o nový způsob šikanování, kdy agresor své blízké či kamarády může takto šikanovat online.
- Při hraní online her bývají vrstevníci v živém spojení přes chat nebo na různých internetových portálech s kýmkoli, kdo je momentálně ve hře online. Vrstevníci se slovně urážejí, blokují hrací místnost, vypouštění mezi kolegy/hráče falešné zprávy, či se nabourávají do jiných účtů.
- Posílání elektronickou formou oběti různé nebezpečné kódy jako viry, spyware apod.
- Rozesílání neslušných či obtěžujících zpráv, kdy agresor své dotyčnou oběť registruje v různých nevyžádaných zpráv (u pornografie pak může otec či matka podezírat svého potomka ze sledování erotických linek na internetu).
- Změna identity - kdy vydávají dotyčnou oběť za někoho jiného. [2]

3.6.2 Kyberšikana prováděná v zastoupení

Pokud si agresor pro svoji nelegální práci najme jinou osobu, hovoříme zde o tzv. kyberšikaně v zastoupení, která bývá považována za mnohem nebezpečnější, jelikož dotyčný spolupachatel neví, že je zneužíván k obtěžování jedince či skupiny lidi.

Ve vyjímečných situacích jsou nevědomými spolu agresory i rodiče oběti. A to v případě, jestliže útočník umí navodit situaci, která vypadá že oběť dělá něco nepřístojného a jeho rodiče se o tom nějakým způsobem dozví.

Hovoříme-li o kyberšikaně v zastoupení je tedy nutné si uvědomit, že útočník se pouze vydává za svoji oběť a to s cílem zmást „druhou stranu“ či jinak poškodit dotyčnou oběť. Nejznámějším příkladem ze života, jsou například podezřívající manželé či manželky, které někdy i se štěstím se dostanou do mailové pošty svého protějšku či na jiný profil na internetu, kde se vydávají za dotyčného s jasným cílem poškodit či jinak zablokovat co

nejvíce hovorů, případně i smazat celý profil. Kyber agresor, ale může být v tomto případě i vynalézavější, jelikož může nejen odcizit přístupové heslo, ale pozměnit ho a rozesílat všem vulgární či jinak nevhodné zprávy po neomezenou dobu, které poškozují dotyčnou oběť. [6]

3.7 Typy kyber agresorů

Pomstychtivý andílek“

Tento typ agresora si nepřipouští možnost, že by se on sám dopouštěl něčeho špatného. Prezentuje se jako ten, který sám napravuje zlo a tedy chrání své okolí.

Většinou jde o jedince, který už tento druh šikany v minulosti sám prožil a v současnosti se snaží vše oplácet svým obětem. Pomstychtivci pracují ve většině případů sami, ale mohou své aktivity sdílet se svými nejbližšími přáteli a těmi, které snímají jako oběti nyní kyberšikanovaného agresora. „Pomstychtivý andílci“ si potřebují uvědomit, že nikdo by neměl prosazovat spravedlnost na vlastní pěst a že oplácet zlo ještě větším zlem situaci jen a jen zhorší.

Toužící po moci

Další typ kyberútočníků ukazuje prostřednictvím informačních technologií svojí moc a převahu nad ostatními, kdy oběť ve strachu před tímto agresorem vykoná vše, co mu jeho trýznitel nařídí. Tento druh kyberagresorů touží nejen po moci, ale i po ohlasu ze strany publika a to většinou ze strany kamarádů či studentů ze třídy. Když se ohlasy od publika nedostavují, útoky zesilují až do doby, než se nějaké pro agresora „pozitivní“ ohlasy dostaví. Tento typ kyberútočníka je charakterizován jako inteligentní, počítačově zdatný jedinec, který se ve virtuálním světě chová naprosto odlišně, než v tom reálném a zcela eliminuje svoji nemalou závažnost svých kyberútoků.

„Vulgární holky“

V této skupině, jak už název napovídá, převládá většinou ženské pohlaví za účelem pobavení sebe i svého blízkého okolí. Kyberagresoři většinou páchají, nebo plánují své útoky. Stejně jako předchozí typ kyberútočníka, tak i zde je vyžadováno pro agresora „ pozitivního „ ohlasu ze strany publika. Kyberútočník si v tomto případě přímo přeje, aby se vědělo kdo za útoky proti své oběti stojí, resp. kdo je naplánoval. Útoky většinou trvají do

té doby, dokud útočník cítí podporu a ohlasy ve své skupině či okolního publika. Pokud tomu tak není, útoky ve většině případů utichnou.

Neúmyslný kyberagresor

Tento typ kyberútočníka si vůbec nepřipouští, že by vůbec mohl jednat jako kyberútočník a je charakteristický svým předstíráním silného a vyrovnaného jedince, který bohužel odpovídá na dotazy neuvážlivě, bezhlavě nebo arogantně a zprávu bez dalšího zvážení odešle. Jelikož tito jedinci vystupují ve virtuálním světě, jako někdo zcela odlišní mohou tedy i zcela nevědomky rozesílat agresivní poštu. U tohoto typu kyberútočníka existují dva druhy motivů. První je, že prostě „může“ a druhým motivem jeho konání bývá prosté pobavení z jeho činnosti, které páchá kyberagresor většinou sám. [2]

3.8 Kybergrooming

Pod tímto názvem se skrývá chování útočníků, kdy účelem je vyvolání a získání důvěry s následným reálným setkáním a pohlavním zneužitím své oběti. Tento druh nepravdivé komunikace ve virtuálním světě má s tématem kyberšikany úzkou souvislost. Zločinci v těchto případech jsou již dávno za hranicí plnoletosti a rádi se dostávají zpět do stavu rané mladosti, kterou se svojí obětí intenzivně prožívají. Pachatel, v tomto případě tzv. groomer s dotyčným jedincem si píše i řádově i několik měsíců, než dosáhne kýženého výsledku. Když groomerovi selže jeho způsob navázání vztahu v reálném světe přicházejí na řadu různých typů výhrůžek (zveřejnění intimních fotografií) a jiné nekalé metody, které vedou k zastrašení oběti a k termínu kyberšikany. [2]

3.8.1 Obrana proti groomerům

- Zvažte komunikaci ve virtuálním světě s lidmi na netu, kteří se chovají a vypadají až moc ideově, už zde je první příznak, že něco není v pořádku.
- Čtěte důkladně všechny vaše rozhovory se všemi se kterými navazujete komunikaci, zde už můžete zjistit případné chyby vašeho rozhovoru (popřípadě si rozhovory archivujte).

- Dobře si rozmyslete, než někomu sdělíte vaše citlivé nebo osobní data a především zvažte důvod, proč je máte sdělit dotyčnému.
- Odmítejte sexuální či podobnou komunikaci ve virtuálním světě.
- Buďte vždy na pozoru před pochybnými sliby dotyčného jedince o nádherném (skoro až idylickém) vztahu, který jistě nebude nabízet jenom Vám.
- Vyvarujte se poskytování jakýchkoliv osobních dat vedoucí k Vaší identitě a to jak na mailu, chatu či na jiných seznamovacích profilech
- Držte se pravidla, že přátelé na internetu by měly zůstat dál přáteli po internetu, nebojte se říct ne nabídce osobní schůzky. [2]

Čím se vyznačuje kybergroomer

Dle Řezníčkové je charakteristika následující :

- Abnormálně velkou trpělivostí
- Dokáže udržovat kontakt se svojí obětí neskutečně dlouho, řádově i několik měsíců než naplánuje setkání se svojí obětí na živo.
- Jsou velmi přátelští a velmi jim záleží na vztahu se svojí obětí, který bude udržovat v přísném utajení.
- Groomer rád hovoří o nádherném lásky plném vztahu, který bude i dále pokračovat při osobním setkání
- Vyžaduje od své oběti fotografie se sexuální tématikou, kterou rád navazuje i při komunikaci se svojí obětí. [6]

3.9 Stalking

V současné době stále více používaný termín mezi běžnou populací, kterému je jistě zapotřebí se věnovat. Výklad tohoto pojmu z hlediska kriminologie znamená úmyslné pronásledování a obtěžování jiné osoby, který není zakotven v právním řádu České republiky. V stávajícím právním systému se jedná o trestný čin, který právní řád upravuje ustanovením § 353 Nebezpečné vyhrožování a § 354 Nebezpečné pronásledování trestního zákoníku nebo o trestný čin omezování osobní svobody. Ze stránky občanskoprávní se jedná o porušování práva na ochranu osobnosti.

V jiných zemích například v USA je stalking již přes dvě dekády označen za trestný čin, který se díky mnohonásobně lepším technickým možnostem dokáže s velkou pravděpodobností odhalit a detekovat útočníka. Tito "kyber stalkeři" pomocí internetu, emailů a mobilu svojí oběť vyhledávají, selektují a následně obtěžují a psychicky trýzní. Policie České republiky nedisponuje instrukcemi ani metodické pokyny na postup v případě stalkingu. [15]

3.9.1 Rozdělení stalkingu

Dlouhodobě a opakovaně podezřelý kontaktuje oběť a to prostřednictvím poštovních dopisů či dárků, e-mailů nebo prostřednictvím telefonických kontaktů.

- **Zastrašování oběti a demonstrace síly útočníka**

  Jde o fyzické pronásledování a kontrolování oběti, či pouhé vyčkávání na svojí obět na patřičných, vytipovaných místech. Patří sem také sexuální obtěžování, výhrůžky násilí až po vyhrůžky smrti.

- **Poškozování a destrukce věcí**

  .Do této kategorie je nutné zahrnout vše od zasílání spamů, virů až přes poškozování obydlí, osobních věcí až po likvidaci domácích zvířecích miláčků.

3.9.2 Profil a typy stalkera

Podstatou stalkera, je ubližovat a trýznit svojí obět a to tak dlouho, než dosáhne požadovaného cíle. Zároveň existuje několik možností vztahu stalkera ke své oběti. Agresor se svoí obětí se navzájem znají, nebo jej zná, ale neví že on je tím podeřelým a nebo jej nézná vůbec. Nejčastější stalkeři bývají právě byvalé lásky, kamarádi či manželé, kdy jejich zloba je spjatá s malou sebeúctou, negativní náladou či chorobnou žárlivostí. Nebezpečnějším typem stalkera je většinou žena, typická svojí houževnatostí a cílevědomostí z konečné pomsty.

- **Odmítnutý stalker**

Většinou jde o bývalo lásku, manžela či manželky, nebo i o dobrého kamaráda, který neunesl tíhu ukončení vztahu. Cílem bývá msta dotýčné oběti za ukončení vztahu s nadějí na jeho obnovení.

- **Intimní útočník**

Útočníkovi jde v tomto případě o sexuální poměr či o akceptaci s vyhlídnutou oběťí v domnění, že oběť bude jeho city opětovat. Nečástějšími oběti jsou v tomto případě známé tváře, jako herci či zpěváci a jiní.

- **Nekompetentní nápadník**

Tento typ chce nějaký poměr, ale nehledá intimitu ani opětovný vztah, ale hledá rande nebo sexuální schůzku. Tuto skupinu tvoří sociálně a interpersonálně málo způsobilí jedinci.

- **Nazlobený útočník**

Stalker v tomto případě vytrvale sleduje svojí oběť, kvůli psychické újmě, která mu jeho oběť přivodila. Tento typ stalkera je specificky svojí vytrvalostí v naplnění svých vyhůžek formou zastrašování.

- **Nekompromisní útočník**

Oběť je v tomto případě podrobena útočným, nebo dokonce sexuálnímu chováním, která je charakteristická prvotním sběrem informací o obětí a svojí systematičností v jednotlivých bodech útoku při její likvidaci. [15]

3.9.3 Kroky k obraně proti stalkingu

- „ odstřihněte“ se od jakýchkoliv odpovědí stalkerovi, dejte najevo přímo jeho nezájem vyhýbejte se osobnímu styku
- vyhýbejte se často navštěvovaným místům, které útočník zná a o všem informujte někoho blízkého s kterým se budete moc radit a svěřit se
- noste u sebe ochranné prostředky proti případnému fyzickému útoku ze strany stalkera
- pokuste se uchovat pokud možno veškeré projevy a důkazy stalkera vůči vám pro případné šetření policie, nebo pro soudní či jiné šetření

3.9.4 Rešení stalkingu dle PČR

Přínosem práce bylo zdokumentovat postup Policie České republiky při odhalování trestných činů v souvislosti s kyberšikanou :

Poškozený podá trestní oznámení, kdy policejní orgán z obsahu trestního oznámení kvalifikuje skutek o jaké protiprávní jednání jde.
Trestní zákoník upravuje v ust. § 354 odst. 1 písm. a), c) trestního zákoníku -nebezpečné pronásledování, nebezpečné vyhrožování dle ust. § 353 odst. 1 trestního zákoníku.
Policejní orgán požádá poškozeného o předložení důkazů, (SMS komunikace - fotodokumentace kriminalist. technikem, nebo se prostřednictvím datového kabelu data s telefonu stáhnou na CD-R, tisk internetové komunikace)
Dále policejní orgán podá na příslušný Okresní soud žádost o vydání příkazu k zjištění údajů o uskutečněném telekomunikačním provozu dle telefonního čísla za požadované období.
Okresní soud na základě žádosti vydá "Příkaz ke sdělení údajů o uskutečněném telekomunikačním provozu", kdy na základě tohoto policejní orgán „Odbor analytiky“ oddělení kriminálních analýz - požádá operátory o sdělení požadovaných informací. (počet telekomunikačních spojení + SMS zprávy za konkrétní období z účastnického čísla podezřelého na účastnické číslo poškozené) - výsledek slouží jako důkaz pro trestní řízení.(př. za období od 01.01.2011 do 01.03.2011 - počet telekomunikačních spojení 700, SMS zpráv 2.000 .

Podezřelý se vyslechne dle ust. § 158/5 tr. řádu, kdy má právo se vyjádřit k podezření z přečinu.
Na základě důkazů - výpověď poškozené, internetová SMS komunikace, výslechy svědků, zprávy z Intervenčního centra, poraden, přestupkového oddělení, kdy se poškozená již v minulosti obracela na uvedené instituce se žádostí o pomoc k řešení její ne dobré situace.
Na základě shromážděných důkazů se vypracuje usnesení dle ust. § 160/1 tr. řádu - které se doručí podezřelému a tento se okamžikem doručení stává obviněným.
Obviněný má opětovně právo se vyjádřit co se mu v usnesení klade za vinu, nebo má právo odmítnutí výpovědi. Dle kvalifikace skutku a trestní sazby má právo na nutnou obhajobu dle ust. § 36 trestního řádu .
Policejní orgán pokud jsou dány důvody vazby dle ust. § 67 trestního řádu (může uprchnout, působit na dosud nevyslechnuté svědky, pokračovat ve svém jednání a vykonat čin, kterým hrozil (např. zabít, unést děti), podává státnímu zástupci návrh na vazbu.
Příslušný soud rozhodne o vazbě. Dále policejní orgán dle příslušných lhůt daných trestním řádem pokračuje ve vyšetřování, které ukončí návrhem na podání obžaloby státnímu

zástupci, který předá společně se spisovým materiálem na OSZ.
Soud nařídí hlavní líčení, kde rozhodne o vině a trestu, případném vyhoštění pokud jde o cizince (jedna z forem trestu), a odškodnění pokud vznikla hmotná škoda na majetku. V případě odškodnění může soud odkázat poškozeného na občanské řízení. [5]

Závěrem teoretické části uvádím několik případů z kyberšikany, které jsou všeobecně známé :

Případ G.Raza : Kanada.

V roce 2002 natáčí čtrnáctiletý klučina své domácí amatérské video na počest svých oblíbených Hvězdných válek. Netuší, že toto amatérské video se dostane do rukou jeho vrstevníků, kteří jej umístí na internet. Ghysian Raza je během následujících 24 hodin světoznámý a posměšky se mu kromě tisíců lidí na světě dostává i od řady slavných tvůrců animovaných postaviček, které jeho dílo pobavilo. Výsledek ? Totální psychické zhroucení, absence ve výuce a odmítáni venkovního světa atd. O dopadení a potrestání viníků chybí více informací. Jedná se o jeden z prvních případu zaznamenané kyberšikany ve světě.

Případ Patrick Halligana, USA New York

7. října 2003 : První oficiální zaznamenaný případ kybešikany. Patrick Ryan Halligan je obětí skupiny trýznitelů, kteří za pomocí jedné dívky z gangu se dozví, že tento třináctiletý chlapec je ve skutečnosti homosexuální. Ryan na začátku školního roku zjistí, že informace, které sdělil oné dívce (z gangu) byly zveřejněny na internetu. Výsledek ? Dle pitevní zprávy se škrtí Ryan na provaze necelých 5 minut. O trestu pro vrstevníky nebyla nalezena žádná zmínka.

Případ Aničky : Polsko, Gdaňsk

20. 10 2006 : Anna Halmanová byla ve své třídě o přestávce obětí tvrdé šikany (i sex. obtěžování) ze strany čtyř spolužáků, kdy vše bylo filmově zachyceno na kameru a poté i zveřejněno na internetu. Výsledek ? Anička pod náporem tlaku z ostudy ve třídě a obavy o

svůj další život spáchal na druhý den sebevraždu. Případ byl medializován a pachatelé umístěni do nápravných ústavů pro mladistvé. [2]

II. PRAKTICKÁ ČÁST

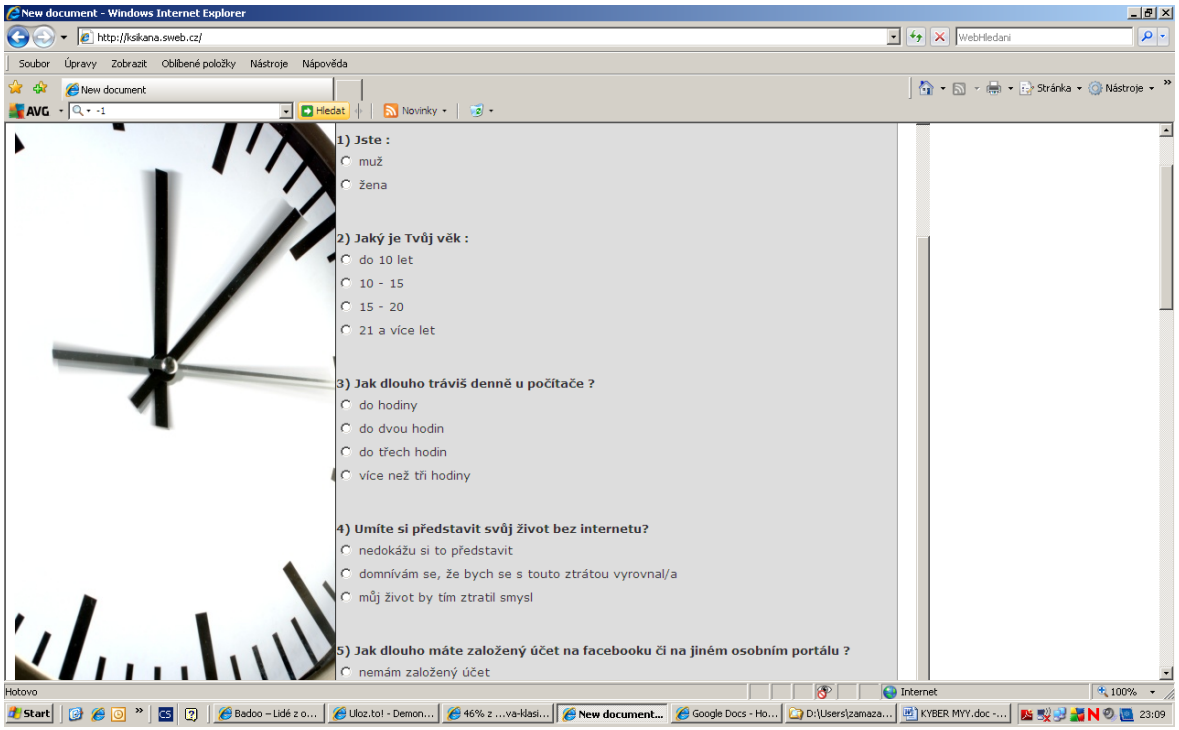
4 VLASTNÍ PRŮZKUM

Přínosem této práce byl vypracovat, zdokumentovat a vyhodnotit, zda kyberšikana v prostředí škol se vyskytuje a pokud ano, pak s jakým výsledkem.

4.1 Dotazníková akce

Od počátku měsíce března do poloviny měsíce května 2011 se zúčastnily vybrané školy ve Zlínském kraji anonymní dotazníkové akce ohledně téma kyberšikany.

Dotazník jsem vytvořil za pomocí odkazu na www.google.com, v kategorii dokumenty po přihlášení a zadání hesla, kde jsem za pomocí znalosti informační techniky, nastavení, šablon a nástrojů vytvořil dotazník vhodný pro můj výzkum, který jsem aplikoval na stránce : www.ksikana.sweb.cz, kde stránka www.sweb.cz je vyhrazená pro vytváření internetových stránek zcela zdarma.

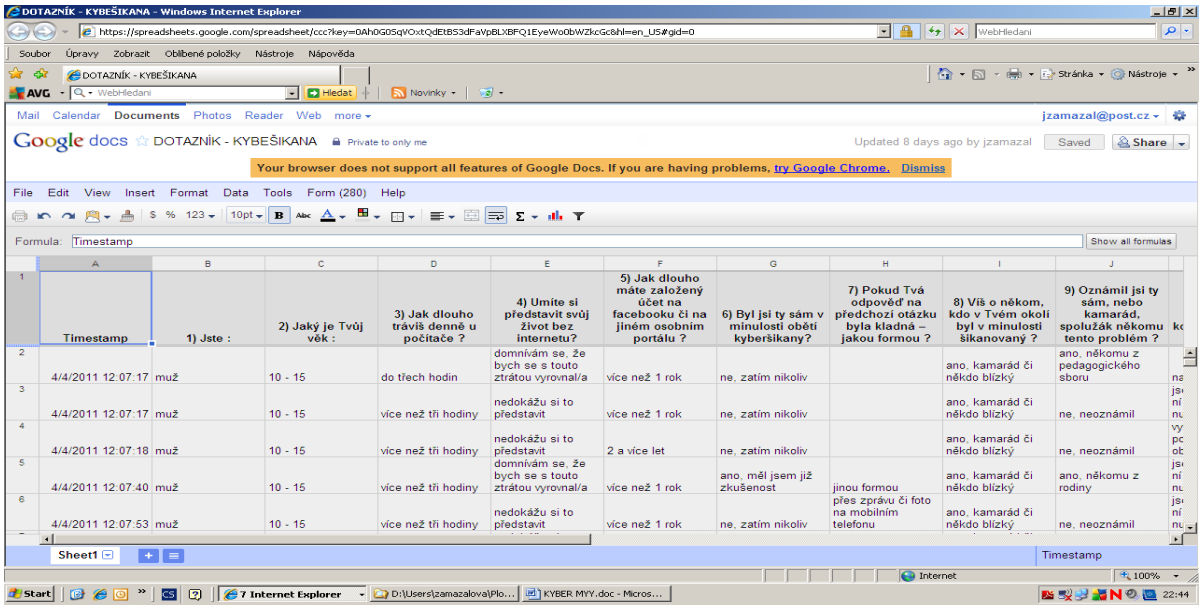


Obr 4. Ukázka dotazníku na www stránce

Celkem se zúčastnilo 223 žáků ze základních a středních škol a to : Základní škola TGM v Otrokovicích, základní škola v Tlumačově a Gymnázium na ul.tř. Spojenců 907

v Otrokovicích, kdy žáci odpovídali na těchto 12 otázek s výběrem 3 až 5 možností na odpověď:

1) Jakého jste pohlaví ?
2) Jaký je Tvůj věk ?
3) Jak dlouho trávíš denně u počítače ?
4) Umíš si představit život bez internetu ?
5) Jak dlouho máš založen účet na net portálu ?
6) Byl jsi ty sám v minulosti obětí kyberšikany ?
7) Jakou formou ? (pokud odp. byla na předch. otázku kladná)
8) Víš o někom v okolí, kdo prodělal kyberšikanu ?
9) Oznámil jsi ty či někdo jiný tento problém ?
10) Jak vnímáš ty sám kyberšikanu ?
11) Podílel jsi se ty sám na kyberšikaně ?
12) Domníváš se , že je kyberšikana nebezpečná ?

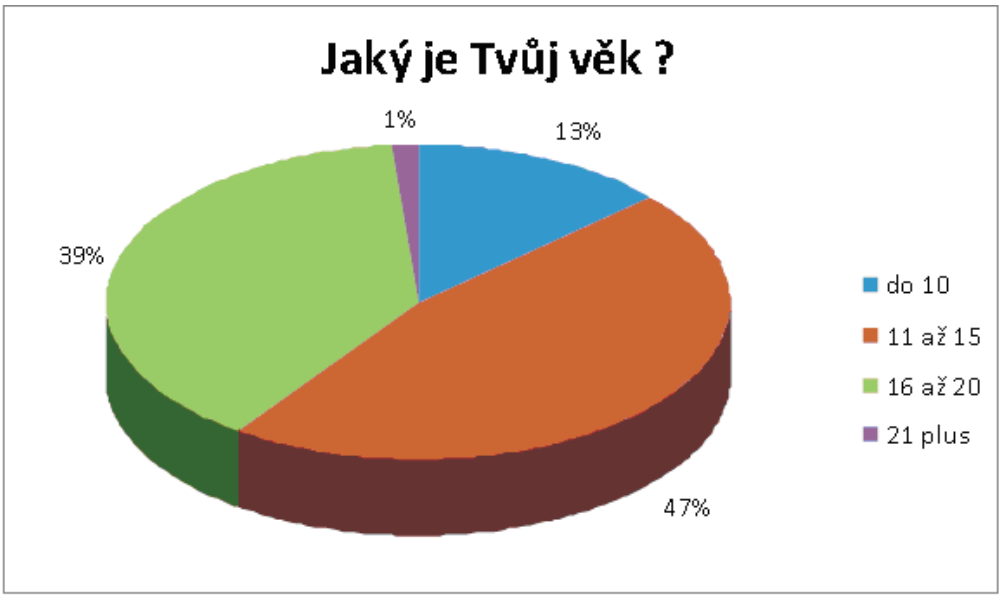


Obr 5. Výsledky výzkumu na google.com

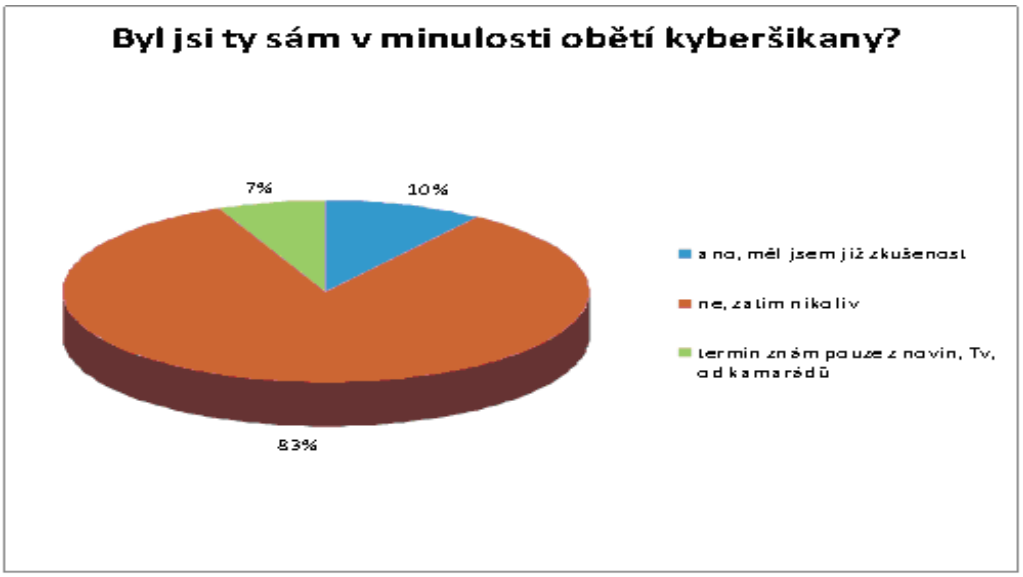
4.2 Vyhodnocení průzkumu

Všechny otázky byly pro můj výzkum relevantní, a sedm hlavních otázek ,které byly prioritou tohoto testu jsem vyzdvihl a zpracoval ve formě grafu , k dalšímu využití. Výzkum jsem realizoval kvantitativní formou a výsledky průzkumu jsem matematicky zpracoval v programu Excel formou grafů:

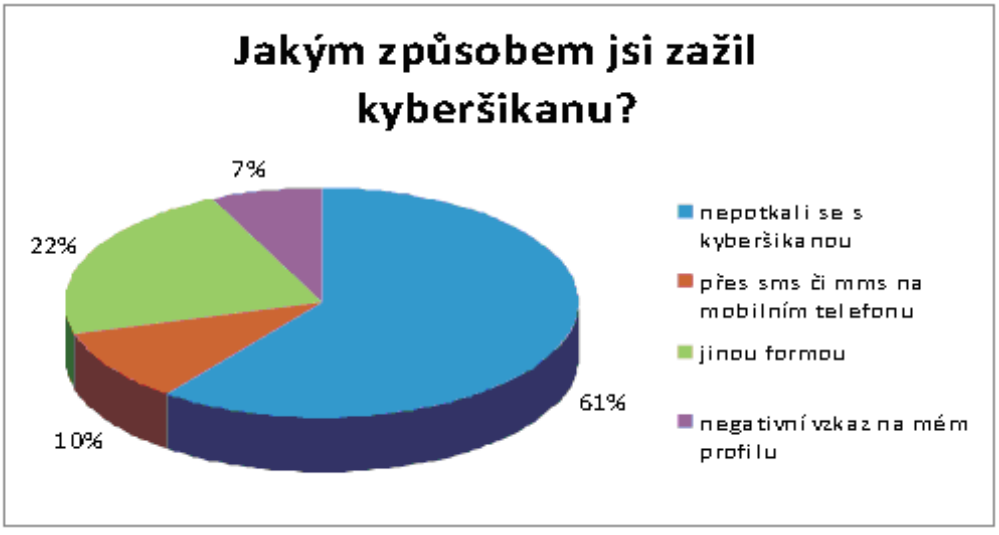
Graf z výzkumu č.1



Graf z výzkumu č.2

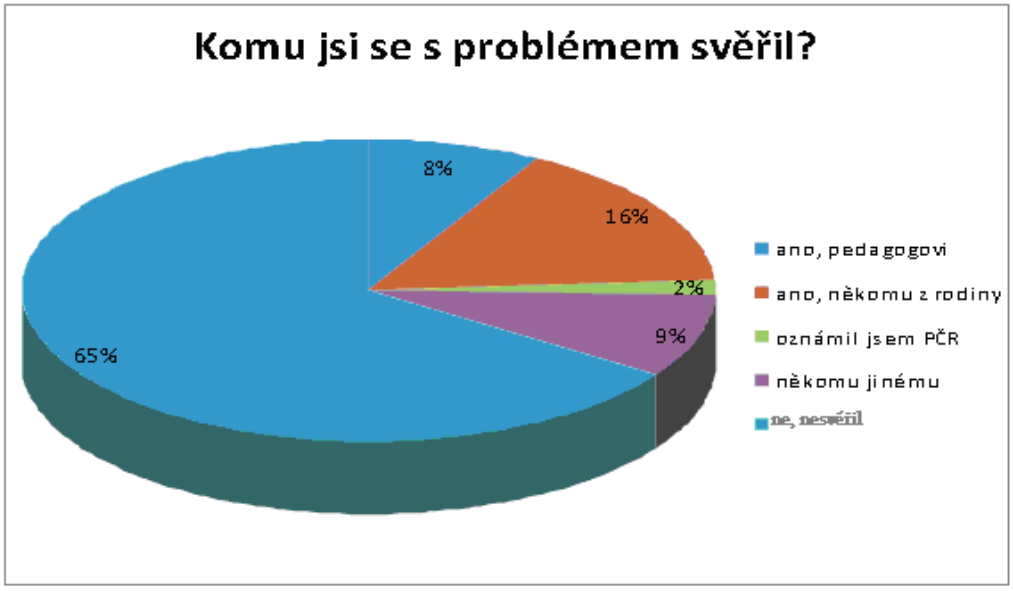


Graf z výzkumu č.3

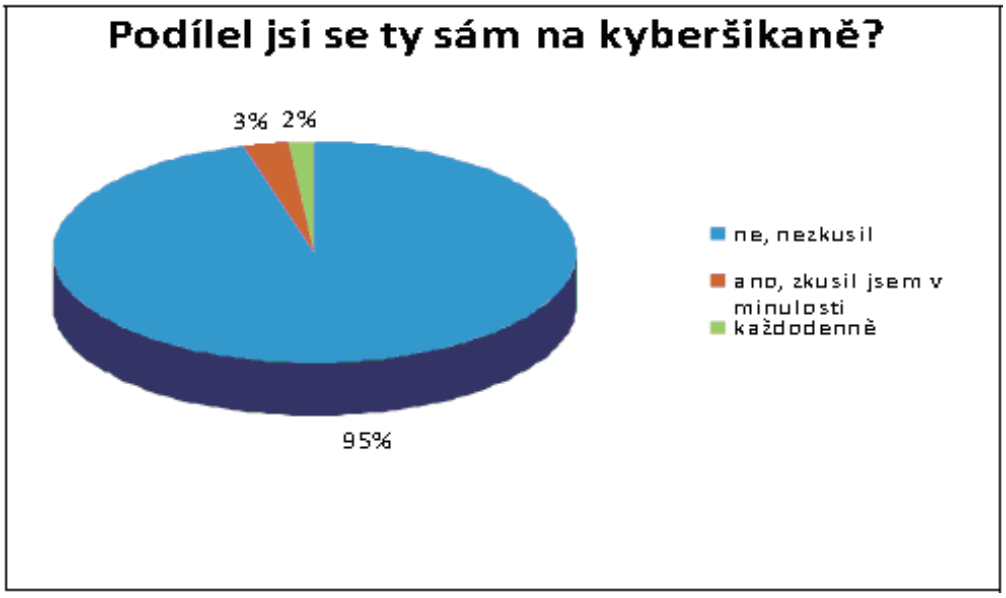


Graf z výzkumu č.4

Graf z výzkumu č.5



Graf z výzkumu č.6



Graf z výzkumu č.7

V průzkumu byli zastoupeni stejnoměrně chlapci a dívky, což přispělo k objektivitě výsledků.

Z uvedených výsledků průzkumu vyplynulo, že se s problémem kyberšikany setkala jen desetina respondentů,(stejný výsledek zaznamenala i Nadace O2 ve svém průzkumu dostupné z http://www.nadaceo2.cz/pro_media). Nejčastěji používaným způsobem kyber šikany jsou textové či grafické zprávy přes mobilní telefony a výhružné vzkazy na osobních portálech.

Zajímavosti je, že pokud by studenti přišly do kontaktu se šikanou přes informační technologie, tuto skutečnost by většina respondentů neoznámila. Z dalšího grafu vyplynulo, že oběť šikany by tuto skutečnost nejčastěji oznámila rodinným příslušníkům, překvapivý je zde i výsledek pro důvěru v Policii České republiky. Pozitivní je zjištění, že většina respondentů by se žádné šikany nezúčastnila.

5 ŘEŠENÍ PROBLÉMU ŠIKANY Z POHLEDU PČR

Jeden z podkladu pro vypracování této práce bylo popsat postup Policie České republiky při odhalování pachatelů.

5.1 Postup při vyhledávání tel. čísla z pohledu PČR

- prvotním faktem je znát mobilní číslo útočníka resp. vyhledávaného mobilu
- tel. číslo dle § 66 zák. číslo 273/2008 Sb., se zasílá písemný požadavek na ÚZČ SKPV sídlící v Brně, který provede detekci a vyhledání tel. čísla za období požadované odesílatelem
- dle trestního řádu může Policie české republiky využít výpis od ÚZČ SKPV poznatky pro další šetření, kdy na výpisu je uvedeno : z jakého tel. přístroje bylo dané číslo volané (zda nedošlo k výměně SIM karty), jak dlouho se volalo, s kterým číslem byla komunikace navázána, IMEI, buňka počáteční lokality volání, buňka konečné lokality .....
- Policie České republiky využívá i dále tzv. svůj interní poznatkový fond (který nese spec. označení), kdy především tyto informace a data pro další šetření, zásobují svými poznatky z terénu řadový policisté, ale i další útvary PČR.
- negativní a bohužel relevantní skutečnost je, že odpověď na písemný dotaz od ÚZČ SKPV trvá i řádově několik měsíců, pokud nemá dotaz speciální prioritu od odesílatele !

Způsob odposlouchávání mobilů .

V dnešní době není prakticky nikdo, kdo by neznal mobilní telefon. Již 15 rokem můžeme mobilní síť GSM odposlouchávat i všechny uskutečněné hovory z mobilního telefonu.

U GSM je mobilní komunikace kódovaná, což vede k nejednomu problému k odposlouchávání této sítě, kromě Policie České republiky.

Logy mobilních operátorů

Většina lidí je seznámeno s tím, že jakákoliv komunikace na mobilu se ukládá a archivuje celých 5 let. Toto logování přikazuje příslušný zákon, který je platný v ČR.

Zajímavostí je fakt, že v České republice se musí, a to povinně logovat veškerá komunikace. Policie České republiky si musí vyžádat povolení k těmto logům od soudu, kdy do měsíce března roku 2011 měla 99,9 % všech žádostí na odposlechy vyřízeno vždy s pozitivním výsledkem. [8]

Lze odposlouchávat předplacené karty ?

Pro Policii České republiky není předplacená karta ničím neřešitelným. Tento způsob je velmi efektivní, jelikož předplacenou kartu může útočník či jakákoliv další osoba použít jako jeden hovor (1 předplacená sim karta = 1 hovor). Důležitým faktem je se zmínit, že dotyčná osoba se musí tohoto mobilu i následně zbavit. S tímto druhem karty se lze samozřejmě připojit i k internetové síti, což nahrává k anonymitě útočníka. Za zmínku stojí samozřejmě skutečnost, že operátoři vlastní databázi účastníků tohoto druhu karet a je tedy velmi pravděpodobné, že u tohoto čísla mobilního telefonu jsou uvedeny dále osobní informace (jméno, příjmení, bydliště).

Co se týče kriminality u nás, byl tento druh karet nejvíce zneužíván u organizovaného zločinu. Před sedmi lety dostala Poslanecká sněmovna na stůl návrh na zrušení tohoto druhu karet, bohužel s negativní odezvou. Vlastníci těchto předplacených karet by byli nuceni podepsat smlouvu s dotyčným operátorem na používání tarifní telefonování.

Lze lokalizovat mobilní telefon ?

Samozřejmě lze dotyčný mobil vyhledat resp. lokalizovat a to i v případě, i když není mobil aktivní (vyjímku tvoří vyjmutí baterie resp. zdroje z mobilu). Ve městě lze mobilní telefon detekovat s přesností řádově na metry, mimo obec lze detekovat s přesností jednoho kilometru. Detekci mobilního přístroje podporuje systém T-mobile Navigátor. [8]

Důležité informace k lokalizaci mobilu :

- Je mylné se domnívat, že používáním několik sim karet u jednoho mobilu, zabrání možnosti odposlechu nebo detekce mobilu, jelikož policii prioritně zajímá IMEI telefonu, sim karta je až sekundární způsob detekce.
- PČR za pomocí Agáty umí detekovat v síti nejen zadaná slova, ale i lokalizovat dotyčného dle jeho hlasu.
- Hovor u odposlouchávaný mobilu není co se týče kvality zcela čistý resp. bez šumu, z důvodu odposlechu v co možná nejvyšší kvalitě.
- Archivace telefonátu u operátora je celých pět let
- Ztížit samotný odposlech, může dotyčná osoba i tak, že hovor bude probíhat např. u tekoucí vody, což je velmi účinná metoda jak do samotného hovoru tzv. přimíchat další zvukovou stopu, kterou již nelze z tohoto hovoru nijak vymazat.

Lze odposlouchávat pevnou linku ?

S přibývajícími roky dnes podstatně klesá majitelů s pevnou linkou.

Tento druh linky (na rozdíl od mobilů) lze mnohem snadněji odposlouchávat, jelikož je síť pevné linky zcela digitalizována. Speciální software na odposlouchávání, je naprogramován tím způsobem, že pokud zachytí v hovoru zadaná slova či dotyčné telefonní číslo, odposlech se aktivuje.

Lze zabránit odposlechu telefonického hovoru a SMS zpráv ?

- šifrovaný telefon, který zcela zabrání odposlechu i policii, je s přibývajícími roky na trhu stále více, kdy nevýhodou bývá pořizovací cena v řádově desítek tisíc korun českých.
- v dnešní době je možné si nahrát tzv. šifrovací přístroj telefonních hovorů, který bohužel funguje za předpokladu nainstalování tohoto druhu programu na obou stranách.

- SMS zprávy je možné zašifrovat pomocí programu SMS 007, který obsahuje speciální zabezpečovací kód a funguje za pomocí symetrické šifry AES, kdy výsledkem u odposlouchávajícího bývá skupina nesourodých znaků. [8]

5.2 Systém Agáta

Policie ČR disponuje nejmodernější vybavením na detekci a odposlech zvaný Agáta.

První zmínky o tomto nejmodernějším vybavení přišlo před osmi lety, kdy policie tehdy zabránila mladé dívce v pokusu o sebevraždu, která měla u sebe v onen osudný okamžik naštěstí zapnutý mobil. Jak policie zabránila tomuto pokusu o sebevraždu ?

Diky aktivnímu mobilu dívky a systému s názvem Agáta, který umí detekovat místo volajícího či posílajícího sms zprávu, se podařilo dívce zabránit onomu hroznému činu.

Policie samozřejmě tento systém co nejvíce maskuje a dělá vše proto, aby Agáta zůstala zcela v anonymitě, jelikož ho používá především při odhalování nejen vrahů násilníků, ale i například podsvětí.

5.2.1 Agáta nahradí i vysílač

Systém Agáta neodposlouchává žádné hovory, ale je nezbytnou součástí systému sloužící na tuto činnost, kdy Agáta slouží především k detekci pohybu sledované osoby nebo k dotyčnému vyhledávání místa. Zároveň také k detekci telefonního čísla u předplacených SIM karet. Velké procento zločinců právě používá předplacené karty, ke které nepotřebuje volající osobní data u tohoto druhu karty. U předplacených SIM karet operátoři na rozdíl od klasických paušálních klientů nevědí, kdo takové karty používá.

Můžeme Agátu nějakým způsobem identifikovat ? Jedná se o menší nákladní vůz, na kterém je zabudována a zamaskovaná parabolická anténa s velkým počítačem umístěným v interiéru dodávky s několika menšími počítači.

Asi nejdůležitějším faktem je, že tento systém umí zaujmout pozici tzv. „vysílače BTS“ mobilních operátů, které lze snadno identifikovat. Je složen ze stožáru s parabolickými anténami, které bývají umístěné na nejvyšším bodě v terénu. Za nepřítomnosti těchto „bétéesek“, by jsme nemohli komunikovat s ostatním světem. Přes „vysílač“ a následný sdružovač a ústřednu se signál nese z mobilního přístroje na druhý. [9]

5.2.2 Detekce mobilu

Agáta vyjede na místo, kde se nachází „zájmová osoba“, kterou je zapotřebí detekovat. Je zapotřebí znát telefonní číslo dotyčného jedince a pravděpodobné místo kde se bude pohybovat. Systém Agáta kontroluje možné místa detekce a jednou za čas se oživí a nahradí nejbližší vysílač BTS. Tím se Agáta stává přijímačem všech hovorů a vysílací zařízení daného operátora, který je po dobu zapojení Agáty zcela vyřazen.

Hledanou osobu pak i v hustě zástavbě s přesností na metry najde dle signálu telefonu, který vysílá.

U odposlechu předplacené karty, kterou zájmová osoba používá, je nutné znát její co možná nejpřesnější polohu. Následně stačí Agátu přiblížit k místu odposlouchávání a dle síly vysílacího signálu zjistí, jaký mobilní telefon a zároveň i číslo dotyčná osoba právě používá.

5.2.3 Kde se nachází centrum s odposlechy

Státem schválené odposlechy telefonů nebývají nijak v dnešní době technicky složité, jelikož nikde se nemusí instalovat tzv. štěnice na odposlouchávaní hovorů apod. a policie si tak vystačí pouze s počítačem.

V centru našeho hlavního města sídlí Almerův Úřad zvláštních činností, který je jak jinak bez jakéhokoliv označení a to kvůli anonymitě. U vchodu je na zvonku nápis : „TA Katrich“. (což byla cca před 15ti lety nejznámější hospoda všech mafiánů a lidi z podsvětí).

Další důležité sídlo, sloužící k odposlechu se nachází o kousek dál, kde přicházejí žádosti o odposlech. S písemným povolením od soudu předá žádost o odposlech Almerovu úřadu zaměstnanec PČR, vyšetřující dotyčný případ. Dotyčný úřad pak písmeně vyrozumí dotyčného zaměstnance mobilního operátora, že soud schválí odposlech dotyčného telefonního čísla.

Hovory „spadnou“ do obřího PC

Operátor všechny hovory dotyčného čísla zašle speciální cestou na další pracoviště Almerova úřadu a zde se archivuji ve velkém počítače, který data kopíruje a archivuje a přeposílají na požadované oddělení policie, bud ve formě speciální linky či uchované na CD-ROM. Informace o hovorech dostane policista až po skončení odposlouchávaní, vyjímku tvoří zvláště závažné případy, kdy je odposlech on-line. [9]

Může policie odposlouchávat všechny hovory ?

Hovory odposlouchávané osoby se na písemné povolení od soudu zaznamenají a archivují a to jak příchozí tak i ty odchozí. Policie tak monitoruje i hovory, které nesouvisí s dotyčným případem (např. intimní hovory, manželské rozepře, pracovní věci). Tyto hovory musí policie následně pod úředním dohledem skartovat a to i v těch případech že se dozví během odposlechu o dalším, třeba i závažnějším trestném činu.

Lze Agátu identifikovat ?

Jde o menší nákladní vozidlo v bílé provedení tovární značky Ford či VW s neexistujícím logem např. natěračské firmy na exteriéru vozu.

Součástí vozu je integrovaná parabolická anténa, kterou není možno z venku nějak identifikovat a dále je vůz tvořen větším počítačem s několika menšími.

Hovory, které byly odposlechnuty jsou umístěné do počítače na Almarově speciálním pracovišti, se nearchivují se a při kopírování na CD-ROM nebo na počítač policejního důstojníka, se tyto data zcela smažou. Pracovníci a zaměstnanci nejen z řad PČR, patřící do tohoto systému, jsou povinni projít bezpečnostní prověrku spolehlivosti.

Při porušení povinností, týkající se zneužití informací hrozí trestní stíhání za porušení telekomunikačního zákona. Operátorovi může být i v některých případech odejmuta licence.Zajímavostí je i cena takto vybaveného vozu se systémem Agáta, který stojí okolo patnácti miliónu českých korun. [9]

Obr 6. Vozidlo pro systém Agáta

5.3 Zásady při postupu detekce IP adresy z pohledu PČ

Jaké jsou obecné zásady při postupu detekce IP adresy u PČR ?

1. U incidentů je důležité správné určení (interpretace) času kdy k rozhodné události došlo – dle časové zóny. Cíl mailové pošty je znám, důležité je zjištění zdroje a přesného času odeslání maximálně na minuty z důvodů dohledání.
2. Pozor na spamy pro oběť – hlavička mailu, e-mailová adresa odesílatele uvedená v položce „From:“ nemusí být pravá, může být podvržená – lze snadno záměrně nastavit např. v konfiguraci libovolného e-mailového klienta, u spamů to běžně podvrhují viry nebo spamoví roboti nemusí být vždy pravá.
3. Důležitá je IP adresa (např. v Outlooku zjistíme v kategorii : vlastnosti mailu a následně zobrazení hlavičky), hlavička má pro nás velmi velký význam, jelikož je zde popsán kromě použitého programu, také pro nás důležitý celkový pohyb dat – který server předal data dalšímu serveru a tím se detekuje cesta, která už jen udává, který poštovní server zprávu předal dalšímu serveru. Pro zjišťování původce je nejdůležitější první server a hlavně počítač, z kterého e-mail odešel.
4. Pro veřejné adresy můžeme pro snad detekci IP adresy použít z některých dostupných programů (jedná se o databázi) např. www.ripe.net , což je evropská organizace, které má na starosti správu domén a registr IP adres. Vyhledává organizace zodpovídající za užívání přiděleného bloku IP adres a kontakt na administrátora dané sítě.

Hlavička e-mailu

K detekci hlavičky e-mailu napomáhají úspěšně tyto osvědčené internetové odkazy :

http://www.soom.cz/index.php?name=articles/show&aid=29

http://fch.upol.cz/skripta/intz/add/Mail_head.htm

http://www.uoou.cz/uoou.aspx?menu=0&submenu=23&loc=486

http://forum.security-portal.cz/viewtopic.php?t=60

Vyhledávání v databázích

IANA – organizace zodpovědná za celosvětovou koordinaci přidělování IP adres a Root DNS : http://www.iana.net/

Správa IP adres je delegována do pěti autonomních systémů dle jednotlivých kontinentů :

http://www.iana.net/numbers/

Každý z kontinentálních registrátorů udržuje databázi o přidělených IP adresách (komu, kdy byly IP příslušné bloky IP dres přiděleny, kontakty na organizace a zodpovědné administrátory). V jednotlivých databázích je možno vyhledávat přímo nebo pomocí služby whois:

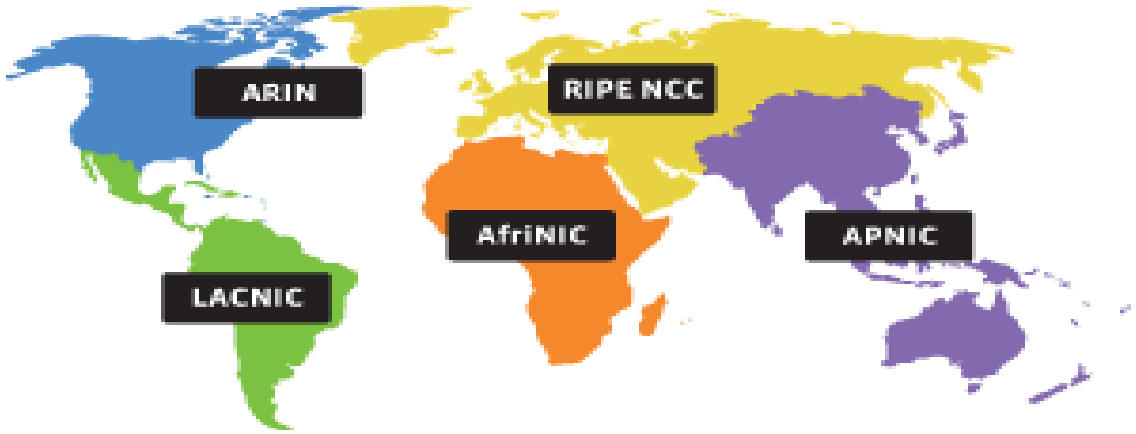
http://www.ripe.net/

http://www.apnic.net/

https://www.arin.net/

http://www.lacnic.net/

http://www.afrinic.net/



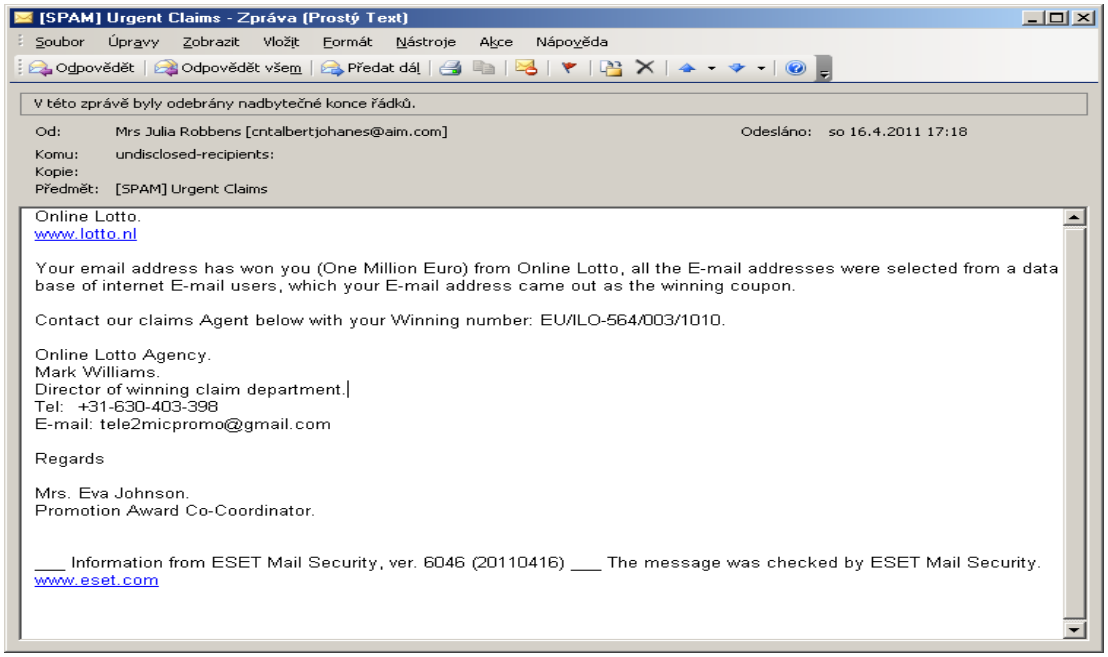
Obr 7. Rozdělení jednotlivých databází

Příklady whois vyhledávačů: http://whois.smartweb.cz/ nebo http://www.whois.net/

CZ.NIC - organizace pro registraci a správu CZ domén, vyhledávání údajů o CZ doménách: http://www.nic.cz

5.4 Příklad postupu zjištění původce e-mailu.

Příklad e-mailu (v tomto případě se jedná o SPAM, který byl navíc označen anti spamovým filtrem na serveru příjemce pro uživatele viditelným označením [SPAM] v předmětu zprávy)



Obr 8. Ukázka spamu

1. Zobrazení kompletní hlavičky e-mailu (ve vlastnostech e-mailu):

Return-Path: <cntalbertjohanes@aim.com>

Delivered-To: Vojtek@mailbox.utb.cz

Received: from sun.utb.cz (unknown [192.168.1.13])

by mailbox.utb.cz (Postfix) with ESMTP id E25867827EA3

for <Vojtek@mailbox.utb.cz>; Sat, 16 Apr 2011 17:21:44 +0200 (CEST)

Received: from sun.utb.cz (localhost [127.0.0.1])

by nod32.utb.cz (Postfix) with ESMTP id D55B334094174

for <Vojtek@mailbox.utb.cz>; Sat, 16 Apr 2011 17:21:44 +0200 (CEST)

X-Virus-Scanner: This message was checked by ESET Mail Security

for Linux/BSD. For more information on ESET Mail Security,

please, visit our website: http://www.eset.com/.

Received: by sun.utb.cz (Postfix, from userid 1000)

id D47753409416C; Sat, 16 Apr 2011 17:21:44 +0200 (CEST)

X-Spam-Flag: YES

X-Spam-Checker-Version: SpamAssassin 3.2.3 (2007-08-08) on sun.utb.cz

X-Spam-Level: *****

X-Spam-Status: Yes, score=5.5 required=5.0 tests=AWL,BAYES_50,

FORGED_MUA_OUTLOOK,HELO_LH_LD,KAM_LOTTO1,MSOE_MID_WRONG_CASE,RDNS_NONE,

SPF_NEUTRAL autolearn=no version=3.2.3

X-Spam-Report:

* 1.2 HELO_LH_LD HELO_LH_LD

* 0.7 SPF_NEUTRAL SPF: sender does not match SPF record (neutral)

* 0.0 BAYES_50 BODY: Bayesian spam probability is 40 to 60%

* [score: 0.4373]

* 0.8 MSOE_MID_WRONG_CASE MSOE_MID_WRONG_CASE

* 2.9 KAM_LOTTO1 Likely to be a e-Lotto Scam Email

* 0.1 RDNS_NONE Delivered to trusted network by a host with no rDNS

* 0.0 FORGED_MUA_OUTLOOK Forged mail pretending to be from MS Outlook

* -0.3 AWL AWL: From: address is in the auto white-list

Received: from localhost.localdomain (unknown [211.169.247.194])

by sun.utb.cz (Postfix) with ESMTP id 335263409416C

for <vojtek@utb.cz>; Sat, 16 Apr 2011 17:21:35 +0200 (CEST)

Received: from User ([86.34.152.238])

(authenticated bits=0)

by localhost.localdomain (8.14.3/8.12.9) with ESMTP id p3GFHBSg015817;

Sun, 17 Apr 2011 00:17:16 +0900

Message-Id: <201104161517.p3GFHBSg015817@localhost.localdomain>

Reply-To: <contactjgomez@gmail.com>

From: "Mrs Julia Robbens"<cntalbertjohanes@aim.com>

Subject: [SPAM] Urgent Claims

Date: Sat, 16 Apr 2011 17:18:04 +0200

MIME-Version: 1.0

Content-Type: text/plain;

charset="Windows-1251"

Content-Transfer-Encoding: 7bit

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2600.0000

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

To: undisclosed-recipients:;

X-Spam-Prev-Subject: Urgent Claims

Důležitý je modře zvýrazněný údaj s IP adresou nejpravděpodobnějšího původce:

Received: from User ([86.34.152.238])

2. Dotaz do registračních databází nebo služby whois na IP adresu 86.34.152.238 – výpis:

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
```

```
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '86.34.0.0 - 86.34.255.255'

inetnum:        86.34.0.0 - 86.34.255.255
netname:        ROMTELECOM
descr:          Romtelecom Data Network
country:        RO
admin-c:        AL3618-RIPE
tech-c:         ANOC7-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-ARTELECOM-LIR
mnt-lower:      MNT-ARTELECOM-LIR
mnt-routes:     MNT-ARTELECOM-LIR
mnt-domains:    MNT-ARTELECOM-LIR
source:         RIPE # Filtered

role:           ARtelecom LIR
address:        Garlei 1B sector 1 013721 Bucuresti Romania
abuse-mailbox:  abuse@romtelecom.ro
admin-c:        DC478-RIPE
tech-c:         CD297-RIPE
mnt-by:         MNT-ARTELECOM-LIR
nic-hdl:        AL3618-RIPE
source:         RIPE # Filtered

role:           ARtelecom Network Operation Center
address:        100 Calea Vitan Str.
address:        Bucuresti,sect 3, Romania
phone:          +40-21-3029767
fax-no:         +40-21-3130730
remarks:        trouble:      +-----------------------------------------------------
remarks:        trouble:      | Operational issues:     noc@artelecom.net         |
remarks:        trouble:      | AS & Peering issues:    route-admin@artelecom.net |
remarks:        trouble:      | Abuse and Spam issues:  abuse@romtelecom.ro       |
remarks:        trouble:      | * IN CASE OF HACK ATTACKS ILLEGAL ACTIVITY,       |
remarks:        trouble:      | * VIOLATION, SCANS, PROBES, SPAM, ETC. *          |
remarks:        trouble:      | DNS issues:             hostmaster@artelecom.net  |
remarks:        trouble:      +-----------------------------------------------------
remarks:        24x7 @ +40-21-3029768
admin-c:        AI134-RIPE
tech-c:         CD297-RIPE
tech-c:         CI84-RIPE
tech-c:         DEM5-RIPE
nic-hdl:        ANOC7-RIPE
mnt-by:         ARTELECOM-MNT
source:         RIPE # Filtered

% Information related to '86.34.0.0/16AS9050'

route:          86.34.0.0/16
descr:          Romtelecom Data Network
origin:         AS9050
mnt-by:         MNT-ARTELECOM-LIR
source:         RIPE # Filtered
```

Z uvedeného zjistím, že IP adresa patří do sítě Romtelecom Data Network se sídlem v Bukurešti v Rumunsku. Kliknutím na odkazy **admin-c** nebo **tech-c** (administrační nebo technický kontakt) zjistím kontakty na konkrétní zodpovědné administrátory sítě. Ty pak mohu kontaktovat, popř. pro stížnost mohu použít tzv. „abuse“ kontakt, v tomto případě abuse@romtelecom.ro.

Pro bližší zjištění identity konkrétního počítače v síti už je nezbytná součinnost administrátorů dané sítě.

5.5 Odhalování na Facebooku

Internetová síť facebook je pro svojí mimořádnou navštěvovanost jeden z nejčastějších možných virtuálních míst, kde se kyberšikana často vyskytuje. Je vůbec možné identifikovat útočníka i na tomto portálu ?

Prvním základní bodem je definovat, zda je útočník aktivní nebo jestli tzv. stopuje někoho, kdo již není na facebookovém portálu aktivní. Pokud je aktivní a navštěvuje častěji facebook, je snahou získat jeho IP adresu, z které přistupuje na sít a tvářit se jako jeho další možná oběť. Pokud se podaří navázat, bylo by vhodné ho vylákat na net stránku, kde se zapamatuje jeho veřejná IP adresa (např. vytvořením vlastní jednoduché stránky, na kterou když se podívá, přesměruje útočníka na nějakou další, ale moje adresa si zapamatuje jeho IP adresu). Potom nastává již klasický postup (jako u zjišťování mailu), kdy přes RIPE či WHOIS se zjistí, na koho je adresa registrována a vyžádá se přes administrátora log, což je záznam serveru, který prozrazuje kdy byl uživatel a v jakém čase připojen a z jaké adresy.

Pokud je útočník již pasivní, je možné se obrátit na samotnou organizaci, která na starosti provoz facebooku v České republice a požádat je o sdělení IP adresy.

5.6 Pravidla ochrany a obrany před kyber útočníky

Z průzkumů prováděné ve Velké Británii, Spojených státech , Kanadě či Austrálii mezi lety 2005-2007 je zřejmé, že obětí tohoto druhu šikany se stalo 25-35 % dětí.

V České republice zatím nedošlo k podrobnému průzkumu, ale dle šetření projektu E-Bezpečí ukazuje, že výsledky nebudou odlišné, než jak tomu je ve světě.

Úplná, tedy 100% ochrana před agresory kyberšikany samozřejmě neexistuje (pokud se samozřejmě nevzdáme tohoto druhu komunikace). Míru rizika za použití následujících pravidel či požadavků ovšem můžeme snížit :

- Velice dobře uvažte, CO a především KOMU data posíláte
- Respektujete ostatní uživatele na síti.
- I u internetu se řiďte heslem : „dvakrát měř a jednou řež“
- Hesla nejen k el. poště nikomu nesdělujte, vždy je po určité době zcela vyměňte a pokud máte hesel více – zapisujte si je na Vámi přístupné místo.

- Neposílejte nikomu neznámému svojí civilní a už vůbec ne intimní fotografii a vyhýbejte se sdělování svých osobních údajů (rodné číslo, telefon apod.)
- Každou informaci na Internetu si prověřte, pokud je možné i u více zdrojů.
- Velmi podrobně se seznamte a přečtěte s pravidly chatu či diskusního portálu.
- Komunikujte jen s tím, koho uznáte za vhodného. Více portálů dnes nabízí možnost blokování druhé strany. Případné i smazaní vlastního profilu.
- Nedomlouvejte si schůzku po Internetu, aniž byste o tom řekli někomu jinému (nejlépe alespoň jednomu z rodičů či důvěryhodné osobě).
- Pozor na spamy a především viry od útočníka. Zvýšenou opatrnost věnovat zprávám s přílohu zprávy, od neznámé odesilatele (nejlépe zprávu neotevírat a ihned odstranit)

ZÁVĚR

Hovořit v dnešním světě o šikaně znamená hovořit současně i o kyberšikaně. I když oba negativní společenské jevy jsou spojeny s násilím a ponižováním, každý se odehrává na zcela jiném poli.

Na virtuálním světě je pozitivní, že zcela eliminuje jakékoliv hranice, zároveň ale přináší také nemálo problémů. Příkladem může být vyhledávání kyber útočníků, které bývá v některých případech i velmi složité. U problému s detekcí mobilního telefonu bylo donedávna nutné vlastnit povolení k telefonním odposlechům, jelikož Police České republiky musí postupovat dle zákonů, norem a pravidel, narozdíl od pachatelů. .

Moji práce bohužel poznamenalo řada negativních faktorů. Na začátku práce jsem netušil, jaký problém nastane, když jsem žádal studenty škol ve Zlínském kraji, aby se zúčastnit mého dotazníku přes internet. Nebyl jsem totiž sám, kdo měl podanou podobnou žádost u ředitelů škol. Rodiče studentů si nepřáli, aby jejích dítě bylo podrobováno jakýmkoliv mimoškolním činnostem a dále aby se vyloučilo vše, co se netýká osnovy školního vyučování. Proto se nakonec vybraného testu zúčastnily pouze tři školy, s celkovým počtem 223 studentů. Tento výsledek byl i přes jisté obtíže dostatečně vypovídající a splnil svoji funkci.

Dalším problémem v průběhu psaní práce bylo rozhodnutí Ústavního soudu ze dne 22.03.2011, o zrušení lokalizačních údajů a jejich předávání orgánům oprávněným k jejich využívání. Pro další šetření těchto druhů případů bude tedy na zvážení soudu, zda povolí či nikoliv Policie České republiky si tyto data vyžádat a pracovat s nimi.

V současné době se Policie České republiky prostřednictvím rozsáhlé kampaně zaměřuje na prevenci kyberšikany a klasické šikany a také na obranu proti obětem šikany. Projekt oslovuje i samotné útočníky a pomocí sportovních a jiných činností odvádí pozornost od jejich negativních záměrů a využívá je ve smysluplnějších oblastech.

Je nezbytné si i položit otázku jaká bude budoucnost v boji proti kyberšikaně ? Stejně jako v atomovém věku lidstva, kdy nelze zcela už vymazat jaderné zbraně, tak kybernetický zločin již nelze zcela vymítit z světa informačních technologií. Ovšem prostřednictvím prevence, zákonů a tvrdých sankcí ji lze eliminovat na co nejnižší možnou úroveň. Jedním z řešení, doporučené odborníky na počítačovou bezpečnost, by bylo adekvátní, zavést

s postupem času tzv. digitální pasy, které by identifikovaly osobu připojenou na celosvětovou síť.

I přes jisté problémy jsem přesvědčen, že tato práce přinesla rozšíření vědomostí spojené s tématem šikany, která je narůstajícím problémem v současném civilizovaném světě a se kterou se musí za pomocí prevence a legislativy neustále bojovat.

CONCLUSION

To speak of bullying today is also to speak cyber-bullying. Although both negative social phenomena are associated with violence and humiliation, each takes place on an entirely different field.

The positive aspects of the virtual world is that completely eliminates any boundaries, unfortunately it also brings quite a few problems. For example it might be, in some cases, very difficult searching for cyber attackers. The problem with detection of the mobile phone was you had to have permission to tap a telephone, since the Police of the Czech Republic must follow the laws, norms and rules, even though offenders don t .

My job unfortunately was affected by a number of negative factors. At the beginning of this dissertation I had no idea what the problem might have been; before I asked school students in the Zlín Region, to participate in my questionnaire via the Internet. I was unaware that many others had submitted similar requests to school principals: Unfortunately the parents of many students did not want their child to be subjected to any extracurricular activities and to eliminate everything that is not part of their schooling. Therefore, only three schools participated, with a total of 223 students. The result, despite some difficulties, is sufficiently meaningful to fulfill its intention.

Another problem in the course of writing this work was the decision of the Constitutional Court dated March 22, 2011, to restrict the access of location and transmission dataand curtail the bodies authorized to use them. Further investigation of these types of cases will therefore be at the discretion of the court; and whether or not to authorize the Police of the Czech Republic to the data request and work with them.

Currently, the Police of the Czech Republic, through an extensive campaign aimed at preventing cyberbullying and bullying, as well as the classic defense against the victims of bullying. The project addresses and forwards itself and through sports and other activities diverts attention from their negative intentions and use it in more meaningful areas.

It is also necessary to ask what the future will bring in the fight against cyber-bullying? As in the nuclear age of mankind, when it can not completely erase nuclear weapons, and cyber crime can not be completely eradicate from the world of information technology. However, through prevention, laws and harsh penalties, it can be reduced to the lowest possible level. One of the solutions recommended by experts in computer security would be adequate over time to introduce the digital passports that would identify the person

connected to the global network. Despite some problems I believe that this dissertation has expanded the knowledge related to the topic of bullying, which is a growing problem in today's civilized world and one that needs to be controlled through legislation to prevent and fight constantly.

SEZNAM POUŽITÉ LITERATURY

[1] CHROMÝ Jakub : Kriminalita páchaná na mládeži počítačového útoku, Linde Praha. 2010. 240 s., ISBN 978-80-7201-825-3

[2] KAVALÍR Aleš, ROTTOVÁ Nina : Kyberšikana a její prevence [online] [cit. 2007-03-29] Dostupný z URL: http://www.varianty.cz/download/pdf/texts_160.pdf

[3] KOLÁŘ, Michal. Skrytý svět šikanování ve školách : Příčiny, diagnostika a praktická pomoc. Praha : Portál. 1997. 127 s. ISBN 80-7178-123-1

[4] KOLÁŘ, Michal. Bolest šikanování [předmluvu napsal doc. PhDr. Bohumil Stejskal CSc.] Praha: Portál, 2005. 272 s. ISBN 80-7367-014-3.

[5] NOVOTNÝ František Kolektiv : Trestní zákoník 2010, Praha Eurounion 2010, 838 s. ISBN 978-80-7317-084-4

[6] ŘEZNÍCKOVÁ, Eva. Analýza kybernetické šikany jako nového fenoménu v oblasti šikanování. Zlín: Univerzita Tomáše Bati, Fakulta humanitních studií, Ústav pedagogických ved, 2008. 83s.

[7] ŘÍČAN Pavel, JANOŠOVÁ Pavlína : Jak na šikanu, Grada Publishing Praha 2010. 160 s., ISBN 978-80-247-2991-6

[8] Portál o odposlechu mobilů [online] [cit. 2011-03-29] Dostupný z URL: <http://bestpage.cz/komunikace.html >

[9] Portál o systému Agáta [online] [cit. 2011-05-29] Dostupný z URL: < http://bestpage.cz/komunikace/agata.html >

[10] IP adresa [online] [cit. 2011-05-29] Dostupný z URL: < http://darkhell.mysteria.cz/>

[11] IP adresa [online] [cit. 2011-06-02] Dostupný z URL: < http://cs.wikipedia.org/wiki/IP_adresa>

[12] Šikana a řešení PČR [online] [cit. 2011-03-30] Dostupný z URL: http://www.policie.cz/clanek/preventivni-informace-sikana.aspx

[13] Šikana a postup řešení [online] [cit. 2011-06-01] Dostupný z URL:

http://www.zsmikulasezhusi.cz/view.php?cisloclanku=2008020004

[14] Počítač [online] [cit. 2011-06-03] Dostupný z URL:

http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D

[15] Stalking – nebezpečné pronásledování [online] [cit. 2011-06-01] Dostupný z URL:

http://www.trosky.cz/stalking/stalking.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ÚZČ	Útvar zvláštních činností PČR SKPV
SKPV	Služba kriminální policie a vyšetřování
GSM	**G**lobální **S**ystém pro **M**obilní komunikaci.
CLIR	Calling Line Idenfication Restric, služba mobilních operátorů.
IP	Internet protokol
BTS	Base Transceiver Station, Základnová převodní stanice
SMS	Služba krátkých textových zpráv
MMS	Multimediální zpráva
WWW	World Wide Web, soustava propojených hypertextových odkazu
PČR	Policie České republiky
SIM	subscriber identity module
WAP	Wireless Application Protocol

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK - KYBERŠIKANA

Dotazník nás má informovat o faktech, zda se dnešní mládež setkává s problémem kybešikany, tj. s novým druhem šikany prováděnou pomocí inf. technologií. V jakých podobách se uskutečňuje a jaké jsou názory mezi dnešní mládeží.

---

1) Jste :

- muž
- žena

2) Jaký je Tvůj věk :

- do 10 let
- 10 - 15
- 15 - 20
- 21 a více let

3) Jak dlouho trávíš denně u počítače ?

- do hodiny
- do dvou hodin
- do třech hodin
- více než tři hodiny

4) Umíte si představit svůj život bez internetu?

- nedokážu si to představit
- domnívám se, že bych se s touto ztrátou vyrovnal/a
- můj život by tím ztratil smysl

5) Jak dlouho máte založený účet na facebooku či na jiném osobním portálu ?

- nemám založený účet
- ano, mám pár měsíců
- více než 1 rok
- 2 a více let

6) Byl jsi ty sám v minulosti obětí kyberšikany?

- ano, měl jsem již zkušenost
- ne, zatím nikoliv
- tento termín znám pouze ze sdělovacích prostředků, od kamarádů ....

7) Pokud Tvá odpověď na předchozí otázku byla kladná – jakou formou ?

- přes zprávu či foto na mobilním telefonu
- telefonicky na mobilu či na pevné lince
- negativní vzkaz na mém profilu
- nahrávka či nedůstojné foto umístěné na internetu
- jinou formou

8) Víš o někom, kdo v Tvém okolí byl v minulosti šikanovaný ?

- ano, kamarád či někdo blízký
- ne, žádného takového neznám

9) Oznámil jsi ty sám, nebo kamarád, spolužák někomu tento problém ?

- ne, neoznámil
- ano, někomu z rodiny
- ano, někomu z pedagogického sboru
- ano, informoval jsem policii
- někomu jinému jsem se svěřil

10) Jak ty konkrétně vnímáš kybešikanu ?

- vyvolává ve mne pocit strachu a obavy
- naprosto jí odsuzuji
- jsem odhodlaný s ní v případě nutnosti bojovat
- nezajímá mě, i když se to týká mě či mého okolí

11) Podílel jsi si ty sám na nějaké formě kyberšikany ?

- ne, nikdy
- v minulosti jsem již zkusil něco podobného
- ano, provozuji jí často
- každodenně

12) Domníváš se Ty sám, že je kyberšikana nebezpečná?

- ano
- ne, nemyslím si to
- nevím co si mám o tom problému myslet

PŘÍLOHA P II: § 66 ZÁKON Č. 273/2008 SB., O POLICII ČR

Získávání informací z evidencí

(1) Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z evidence provozované na základě jiného právního předpisu. Správce evidence nebo zpracovatel poskytne informace bezplatně, nestanoví-li jiný právní předpis jinak. Správce evidence nebo zpracovatel jsou povinni žádosti bez zbytečného odkladu vyhovět, nestanoví-li jiný právní předpis pro poskytnutí informací policii jiný režim[19)].

(2) Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací z databáze účastníků veřejně dostupné telefonní služby[20)], agendového informačního systému evidence občanských průkazů[21)], agendového informačního systému evidence cestovních dokladů[22)], agendového informačního systému evidence diplomatických a služebních pasů[22)], agendového informačního systému evidence obyvatel[23)], evidence údajů o mýtném[24)], katastru nemovistostí[25)], základního registru obyvatel[33)], základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci[33)], základního registru územní identifikace, adres a nemovitostí[33)], základního registru agend orgánů veřejné moci a některých práv a povinností[33)], informačního systému územní identifikace[33)], registru silničních vozidel[34)], centrálního registru silničních vozidel[34)], registru historických a sportovních vozidel[34)], registru řidičů[10)] a centrálního registru řidičů[10)] způsobem umožňujícím dálkový a nepřetržitý přístup; v případě agendového informačního systému evidence občanských průkazů a agendového informačního systému evidence cestovních dokladů lze informace poskytnout pouze způsobem umožňujícím nepřetržitý přístup; v případě databáze účastníků veřejně dostupné telefonní služby se informace poskytne ve formě a v rozsahu stanoveném jiným právním předpisem[20)].

(3) Policie může v případech stanovených zákonem a v rozsahu potřebném pro plnění konkrétního úkolu žádat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup,

nestanoví-li jiný právní předpis[20)] jinak. Tyto osoby jsou povinny žádosti vyhovět bez zbytečného odkladu, ve formě a v rozsahu stanoveném jiným právním předpisem.

(4) Policie žádá o poskytnutí informací podle odstavců 1 až 3 pouze způsobem, který umožní policii uchovávat identifikační údaje o útvaru policie nebo o policistovi, který o poskytnutí informací žádal, a o účelu, k němuž bylo o poskytnutí informací žádáno, nejméně po dobu 5 let. O skutečnostech podle věty první jsou správce evidence nebo zpracovatel povinni zachovávat mlčenlivost.

(5) Za účelem zajištění ochrany osoby, o níž lze důvodně předpokládat, že by mohl být ohrožen její život nebo zdraví, nebo pro účely pátrání po hledané anebo pohřešované osobě mohou policie nebo ministerstvo požadovat od zpracovatele nebo správce evidence vedené na základě jiných právních předpisů, aby policii oznamovali každý výdej osobních údajů.

PŘÍLOHA P III: NÁLEZ PL. ÚS 24/10

Z odůvodnění nálezu Pl. ÚS 24/10 ze dne 22.03.2011, který zrušuje § 97 odst. 3 a 4 zákona č. 127/2005 Sb. *dnem vyhlášení nálezu ve Sbírce zákonů*:

„Nedostatky, které vedly ke zrušení napadené právní úpravy, nejsou respektovány ani zvláštními právními předpisy, s nimiž napadené ustanovení § 97 odst. 3 zákona o elektronických komunikacích nepřímo počítá. Zejména pak citované ustanovení *§ 88a trestního řádu předestřené ústavněprávní limity a požadavky zdaleka nerespektuje, a z toho důvodu se Ústavnímu soudu jeví rovněž protiústavním.* Nicméně vzhledem ke skutečnosti, že navrhovateli nebylo v návrhu napadeno, Ústavní soud považuje za nezbytné apelovat na zákonodárce, aby v důsledku derogace napadené právní úpravy zvážil i změnu citovaného ustanovení § 88a trestního řádu tak, aby se stalo ústavně konformním. *Použitelnost již vyžádaných údajů pro účely trestního řízení bude třeba zkoumat ze strany obecných soudů z hlediska proporcionality zásahu do práva na soukromí v každém jednotlivém individuálním případu. Soudy budou muset především vážit závažnost trestného činu, který měl být naplněn skutkem, pro nějž je vedeno trestní řízení, ve kterém mají být vyžádané údaje využity.“*

Zákon č. 127/2005 Sb.

§ 97 - zrušená ustanovení

(3) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací *je povinna uchovávat **provozní a lokalizační údaje**, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací…..*Právnická nebo fyzická osoba, která provozní a lokalizační údaje podle věty první a druhé uchovává, je na požádání povinna je bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu….

(4) Rozsah, dobu uchovávání, způsob předávání orgánům oprávněným k jejich využívání a dobu uchovávání a způsob likvidace údajů stanoví prováděcí právní předpis.

§ 90 – ustanovení, které zakotvuje ***jiné*** důvody pro uchovávání provozních údajů

(1) Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.

(2) *Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, který zpracovává a ukládá **provozní údaje, včetně příslušných lokalizačních údajů**, vztahujících se k uživateli nebo účastníku, **je musí smazat nebo učinit anonymními, jakmile již nejsou potřebné pro přenos zprávy, s výjimkou případů uvedených v ustanoveních odstavců 3 až 6.*** Povinnost právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací zachovávat provozní a lokalizační údaje podle § 97 zůstává nedotčena.

(3) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací *je povinen uchovávat provozní údaje* služby poskytnuté účastníkovi nebo uživateli do doby rozhodnutí sporu podle § 129 odst. 2 nebo *do konce doby, během níž může být vyúčtování ceny nebo poskytnutí služby elektronických komunikací právně napadeno nebo úhrada vymáhána.*

(4) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací *může zpracovávat provozní údaje nezbytné pro vyúčtování ceny za službu poskytnutou účastníkovi nebo uživateli za přístup pouze do konce doby, během níž může být úhrada vymáhána*.

(6) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací může pro účely marketingu služeb elektronických komunikací nebo pro poskytování služeb s přidanou hodnotou zpracovávat údaje uvedené v odstavci 1 pouze v rozsahu a v trvání nezbytném pro tyto služby nebo marketing, *pokud k tomu dal souhlas účastník nebo uživatel*, ke kterému se údaje vztahují. Účastník nebo uživatel může svůj souhlas se zpracováním provozních údajů kdykoliv odvolat.