Analýza rizika kybernetické šikany

Radek Slovák

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2014/2015

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

Jméno a příjmení:	**Radek Slovák**
Osobní číslo:	**L11291**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Analýza rizika kybernetické šikany**

Zásady pro vypracování:

1. **Vymezte teoretická východiska spojená s danou problematikou**
2. **Analyzujte jev kyberšikany a popište její typy**
3. **Proveďte kvantitativní výzkum dotazníkovou metodou**
4. **Navrhněte možná preventivní opatření**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] DEVITO, Joseph A. Základy mezilidské komunikace. Praha: Grada Publishing, 2001, 420 s. ISBN 80-7169-988-8

[2] KOPECKÝ, Kamil. Kybergrooming, nebezpečí kyberprostoru. Olomouc: NET University, 2010. 16 s. ISBN 978-80-254-7573-7

[3] ŠEFČÍK, Vladimír. Analýza rizik. 1. vyd. Zlín: Univerzita Tomáše Bati, 2009. ISBN 978-80-7318-696-8

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **doc. PhDr. Ferdinand Mazal, CSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. září 2014**

Termín odevzdání bakalářské práce: **19. září 2014**

V Uherském Hradišti dne 11. srpna 2014

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

prof. PhDr. Ivo Barteček, CSc.
děkan

doc. PhDr. Ferdinand Mazal, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v archivu Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval/a samostatně a použitou literaturu jsem citoval/a. V případě publikace výsledků budu uveden/a jako spoluautor/ka
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti dne 10.9.2014

.....

podpis studenta/ky

ABSTRAKT

Práce na téma analýzy rizika kybernetické šikany je rozdělena na dvě části. V první, teoretické části osvětlíme základní pojmy z oblasti komunikace, on-line komunikace, sociální sítě a pojmy z analýzy rizik. V části druhé, praktické, se budeme věnovat samotnému jevu, a to riziku kybernetické šikany. Dotazníkovým šetřením zjistíme znalosti dané sociální skupiny o problematice a prevenci.

Klíčová slova: Analýza rizik, Facebook, Kybergrooming, Kyberšikana, Sociální síť

ABSTRACT

The present thesis on the analysis of cyberbullying is divided into two parts. The theoretical part highlights basic terms used in communication, online communication, social networking and risk analysis. The practical part is devoted to the dangers of cyberbullying, in which a certain social group knowledge considering the problem of cyberbullying is investigated by a questionnaire.

Keywords: Risk Analysis, Facebook, Kybergrooming, Cyberbullying, Social Network

Děkuji tímto svému vedoucímu bakalářské práce panu doc. PhDr. Ferdinandovi Mazalovi, CSc. za vedení, věcné připomínky, pomoc a hlavně čas, který mi věnoval během vypracování této práce. Mé poděkování patří taky paní Mgr. Kristýně Hruškové, za její čas a užitečné rady k tématu práce.

Motto: *„Svět není nebezpečný kvůli zlým lidem, ale kvůli těm, kteří s tím nic nedělají“*.

Albert Einstein

OBSAH

ÚVOD

S rozvojem moderních technologií obzvláště komunikačních, vzrůstají globální rizika s nimi spojená. Začíná to zasíláním nevyžádaných e-mailů, pokusy ukrást identitu k získání přihlašovacích údajů na sociální sítě nebo do internetového bankovnictví a končí kybernetickým terorismem či napadáním kritické infrastruktury. Problematika rizik internetu a sociálních sítí je tedy velmi široká.

Tématem této práce je riziko kybernetické šikany. Tato problematika je velmi obsáhlá, proto se převážně zaměříme na místo jejího nejčastějšího výskytu, a to jsou sociální sítě. Právě na nich jsou nejčastěji uloženy materiály s touto tématikou, ať už se jedná o fotografie, videosoubory, údaje osobního charakteru apod.

Teoretická část je pojata tak, aby seznámila s východisky části praktické. K těm patří i komunikace, respektive on line komunikace. Obě části krátce popíšeme. Zmíníme rovněž nejrizikovější sociální sítě, nastíníme jejich výhody i nevýhody stejně jako nejběžnější rizika, která na nich mohou hrozit. Rovněž ujasníme základní pojmy z oblasti analýzy rizik a popíšeme metodologii této práce.

V praktické části se budeme věnovat samotné analýze, které bude vystaven v našem případě jeden z nejčastějších jevů vyskytujících se na sociálních sítích. Tím jevem je kybernetická šikana. Budeme se zabývat jen tou nejpodstatnější a nejrizikovější částí.

Rovněž budou zmíněny druhy kybernetické šikany, jako je např. kybergrooming, který je dle mínění odborné veřejnosti nejrizikovějším druhem kybernetické šikany, na jehož konci může být až dětská pornografie. Rovněž nesmíme zapomenout na v poslední době hodně medializovaný kyberstalking, dále na kybersexting, happy slapping, outing. Zároveň stručné popíšeme nový pojem spojený se závislostí, který dostal od odborníků označení FOMO. Netýká se klasických druhů kyberšikany, nicméně se o něm přesto krátce zmíníme, protože i závislost pro nás může představovat jisté nebezpečí.

Kvantitativní analýza formou dotazníkového šetření nám pomůže zjistit problematiku daného tématu u předem vybrané skupiny respondentů. Na základě výsledků budou graficky zpracovány souhrny šetření. V samotném závěru práce se pokusíme najít opatření ke zlepšení prevence, zamezení vzniku, snížení dopadu nebo úplné eliminace rizikových faktorů.

I. TEORETICKÁ ČÁST

1 KOMUNIKACE

Jak uvádí Mikuláštík *„Komunikace je slovo latinského původu a znamená něco spojovat. Může být použito jako označení pro dopravní síť, přemisťování lidí, materiálu, ale také myšlenek, informací, postojů, pocitů, od jednoho člověka k druhému“*.[6] Jde o proces dorozumívání se.

Mezi komunikační prostředky řadíme jazyk, poštu, telegraf, telefon, počítač, denní tisk, časopisy, reklamní materiály, rozhlas, televizi, rovněž autobusy, vlaky a letadla. Komunikaci tedy používáme v řadě různých vědních oborů, ale většinou v oborech spojených s používáním nějakého jazyka. Právě kybernetika přispěla k jeho obohacení. [6]

1.1 Základní charakteristika komunikace

DeVito popisuje proces komunikace jako vzájemnou výměnu informací a projevů, při které dochází v rámci čtyř základních oblastí:

- *intrapersonální komunikace,*
- *interpersonální komunikace,*
- *komunikace v malých skupinách,*
- *veřejná komunikace*. [1]

V případě **intrakomunikace** dochází ke komunikaci jedince se sebou samým. Naproti tomu **interpersonální** komunikace bývá označována také jako mezilidská komunikace. Jde tedy o vzájemnou výměnu informací mezi komunikanty. V případě komunikace v malých sociálních skupinách jakými jsou rodina nebo pracovní tým, dochází ke vzájemnému působení mezi jednotlivými členy.[2]

Vše, co bylo jednou vyřčeno již nelze vzít zpět. Nevratnost sdělovaného je tedy zcela jednoznačná. Dodatečné sdělení, vysvětlení, popřípadě jiná forma, jsou jediné možnosti zmírnění účinků již zaslané či vyřčené informace.

1.2 Verbální a neverbální komunikace

Komunikaci můžeme nejvýstižněji rozdělit na dvě formy.

Verbální komunikace, tedy komunikace pomocí jazykového prostředku, je princip komunikace, který může být zprostředkovaný nebo živý, přímý oproti nepřímému a nebo forma

mluvená či psaná. Verbální komunikace má oproti neverbální výhodu přímého fyzického kontaktu a okamžité zpětné vazby. Pokud se tohoto typu komunikace účastní více komunikantů, stává se však hůře kontrolovatelnou.[7]

Neverbální komunikace je oproti komunikaci verbální, komunikace jinými prostředky, jakými jsou mimika (výraz tváře), gestika (pohyby rukou), proxemika (vzdálenost), posturikou (postoj těla), kinezika (pohyb těla), haptika (dotek) apod. [7]

1.3 Komunikační proces

Pokud je komunikace založená na jednosměrném předávání informací, od toho co mluví k tomu, co ho poslouchá, hovoříme o tomto typu komunikace jako o lineárním modelu.

Do lineárního modelu komunikace zahrnujeme tyto subjekty komunikace:

- ***komunikátor*** (mluvčího, iniciátora komunikace),
- ***komunikant*** (posluchače) při přenosu informace od jednoho účastníka k druhému. Komunikátor v tomto zjednodušeném případě informace (komuniké) pouze vysílá a posluchač je přijímá. Tento typ komunikace bývá označován také jako komunikace jednosměrná nebo jednostranná. Lineární komunikace nepostihuje další důležité aspekty komunikačního procesu, jako jsou např. vzájemné přizpůsobování se nebo rušivé elementy.

„Komuniké *(obsah) je soubor zakódovaných informací, které jsou vysílány a přijímány v rámci procesu komunikace mezi komunikátorem a komunikantem.“*[2]

Komuniké může mít buďto formu verbálního sdělení, nebo neverbálního projevu.

„Komunikační kanál *představuje médium, kterým se pomyslně přenášejí vysílaná sdělení.“*[2]

V obousměrné komunikaci, tedy u modelu, který je tzv. interakční, komunikant adekvátně reaguje na vysílané komuniké. Jde tedy o obousměrnou komunikaci a díky ní dostáváme tzv. **zpětnou vazbu**.

Z výše uvedeného transakčního modelu bylo odvozeno schéma interpersonální komunikace, které v sobě zahrnuje i další důležité prvky ovlivňující komunikační proces.(Obr. 1)

Kódování (převedení určitého smyslu do znakových jednotek) je důležitou činností komunikátora. Odpovídající aktivitou komunikanta, je **dekódování** (zpětná interpretace smyslu

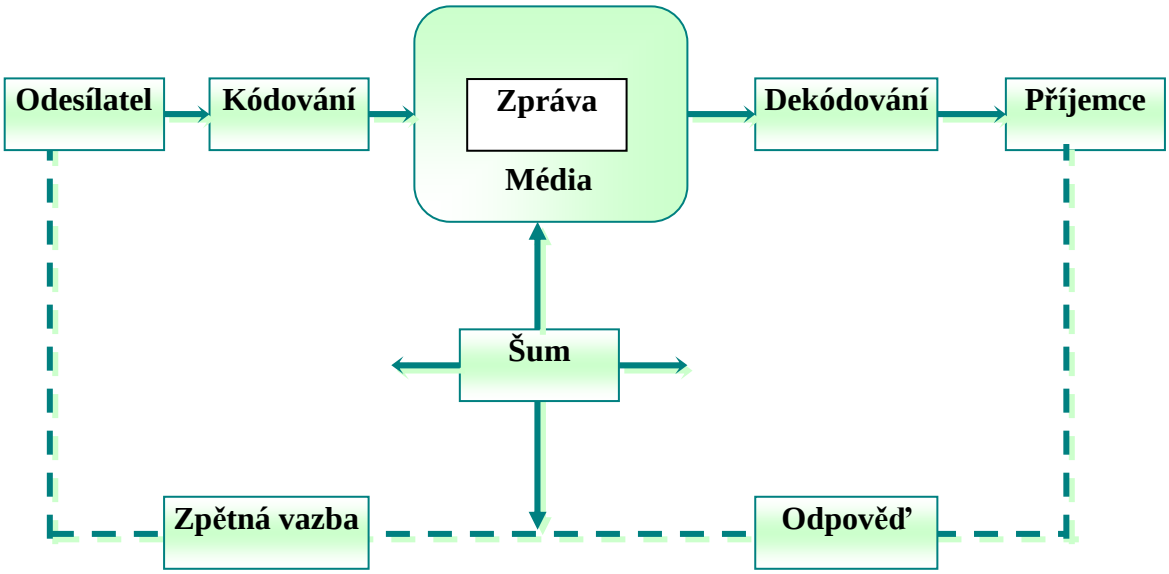
a významu znaků, čili vlastně překlad použitých formálních prostředků komunikace do myšlenek a porozumění sdělení). Kódování a dekódování vyžaduje tedy znalost použitého znakového systému (jazyka) i pravidel jeho používání, je třeba mít komunikační kompetenci. V lidské komunikaci je nejčastěji uplatňovaným znakovým systémem jazyk.[22]

Podstatou přijímání a dekódování sdělení je tedy převádění významu zprávy, tedy nejen jejího obsahu, do mentálních struktur příjemce.

Navazující částí komunikačního procesu je **komunikační šum**. Za ten se v komunikaci považovat vše, co narušuje efektivní předání vysílaných dat, a tím dochází k neúplnosti či zkreslení přijímané informace. Komunikačním šumem mohou být označeny veškeré informace, které jsou přijímány v procesu komunikace, ale jsou pro zúčastněné strany bez užitku.[2]

Nesmíme rovněž zapomenout na **komunikační prostředí**, které ovlivňuje nejen význam, ale i smysl, zřetelnost komunikace a zvolené formy. Takto mohou působit společenské a kulturní okolnosti, ale i fyzikální faktory jako jsou hluk nebo teplota.

Celkový rámec komunikaci dodává její **kontext**, který do značné míry souvisí s komunikačním prostředím. Svou roli zde sehrávají obsahové i věcné souvislosti, vnitřní psychologické i vnější okolnosti (sociální, kulturní a konec konců i přírodní).[22]



Obr. 1 Schéma základního komunikačního modelu

[Zdroj: Rýznar, Ladislav. Společenská diplomacie ve veřejné správě. Praha. MVČR. 2008, upraveno autorem]

1.4 On-line komunikace a její nástroje

On-line komunikace je specifickým typem komunikace, kterým se budeme blíže zabývat, proto ji nyní i teoreticky popisujeme. Umožňuje nám komunikovat elektronickou cestou, tedy prostřednictvím internetu.

Internet sám o sobě je jen prostředek komunikace. K tomu aby interakce mohla vůbec proběhnout, je třeba zvolit jeden z nástrojů on-line komunikace. Známe dva typy, a to nástroje pro synchronní a asynchronní komunikaci.

1.4.1 Synchronní komunikace

Synchronní on-line komunikace je taková, která zajišťuje účastníkům komunikaci ve stejném okamžiku, tedy v reálném čase. Reakce na vyřčenou otázku může být prakticky okamžitá. Nejznámějšími synchronními nástroji on-line komunikace jsou:

- *chat* – nabízí možnost komunikace se skupinou více lidí, většinou probíhá v anonymitě, účastníci používají převážně přezdívky. Povětšinou tedy nevíme, s kým vlastně komunikujeme,
- *Skype* – program, běžně k dispozici všem zájemcům o internetovou telefonii. Základní komunikace mezi vlastníky programu jsou k dispozici v bezplatné verzi. Pomocí Skype lze zasílat i soubory. Bylo zaznamenáno množství hovorů s tématikou sexu, a to v mnoha případech i u nezletilých,
- *ICQ* – základní funkcí programu je zasílání textových zpráv, chatování ve skupině, odesílání SMS zpráv a souborů.

1.4.2 Asynchronní komunikace

Asynchronní komunikace nechá jednoho z účastníků komunikace čekat určitou časovou prodlevu, než se dostaví zpětná reakce. Mezi nástroje tohoto typu on-line komunikace patří:

- *e-mail* – základní a tedy i nejrozšířenější prostředek internetové komunikace. Obsah korespondence mezi komunikujícími je soukromý, a není tedy veřejně dostupný na sociálních sítích. Platí to v tom případě, že žádný z nich obsah nepošle jinému příjemci, nebo nezveřejní na sítích,

- *diskusní fórum* **–** je prostorem na diskusním serveru, na který lze vložit diskusní témata různého typu,
- *webová stránka* **–** dokument, poskytovaný pomocí World Wide Webu.

Jen těžce bychom hledali někoho, kdo by se s on-line komunikací v jakékoli její současné podobě nesetkal. Právě díky ní se časy mezi předáním informace adresátovi zkrátily na minimum. S rychlostí, jakou se zpráva předává, se zároveň předává i její samotný obsah. Vzhledem k povaze celé on-line komunikace již většinou nejsme schopni nijak sledovat další osud námi odesílaných informací.[14]

Důležité je rovněž zmínit, že takto zaslaná zpráva nás téměř po finanční stránce nic nestojí a to bez ohledu, zda ji zasíláme jen na krátkou vzdálenost nebo putuje na jinou stranu zeměkoule.

V dnešní globální době není tedy žádný problém prostřednictvím on-line komunikace komunikovat s kýmkoliv, kdekoliv na světě, zasílat fotografie, dokumenty, sdílet názory, nebo se pomocí webové kamery účastnit soukromého či konferenčního hovoru. A to vše z pohodlí našeho domova.

2 SOCIÁLNÍ SÍTĚ

Ve své publikaci autor Pavlíček tvrdí že *„sociologie definuje sociální síť jako propojenou skupinu lidí, kteří se navzájem ovlivňují, přičemž mohou (ale nemusí) být příbuzní. Sociální síť se tvoří na základě společných zájmů, rodinných vazeb nebo z jiných více pragmatických důvodů, jako je např. ekonomický, politický či kulturní zájem.*“[8] (Obr.2)

Obr. 2 Příklad schématu sociální sítě

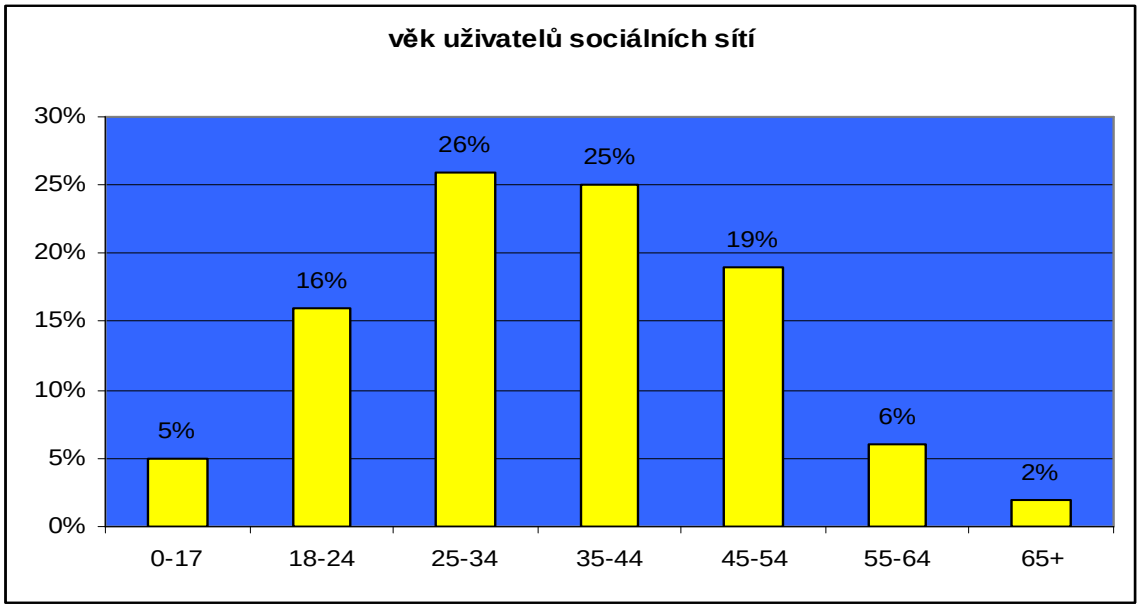
[Zdroj: http://by-the-way.cz/?attachment_id=1892]

V širším slova smyslu je sociální sítí každá skupina lidí, která spolu udržuje komunikaci různými prostředky. Komunikace tedy neprobíhá stejně jako v reálném životě, ale probíhá pod převážně změněnou identitou. A právě tímto vzniká velké riziko zneužití. Útočník si může komunikaci naplánovat a promyslet, může hrubě nejen urážet a ponižovat, ale i vydírat atd.[21]

Pojem sociální síť použil pravděpodobně jako první profesor univerzity v Londýně J. A. Barnes už v roce 1954, když zkoumal sociální vztahy mezi rybáři v Norsku. Z jeho závěrů výzkumu vyplynulo, že taková skupina se dá přirovnat k množině bodů, z nichž některé jsou propojeny linkami, tedy vztah-vazba. Tato myšlenka byla postupem času sociology poupravena do dnešní podoby, tedy že sociální síť je zájmově, přátelsky, rodinně, rasově, nábožensky propojená skupina lidí, kteří se navzájem ovlivňují.[21]

Dá se tedy říci, že každý z nás je součástí nějaké, nejméně jedné sociální sítě.

Na první pohled by se mohlo zdát, že nejrozšířenější věková hranice uživatelů sociálních sítí je do 20 let, tedy převážně teenagerů. Skutečnost však naznačuje něco zcela jiného. Nejpočetnější skupinou na sociálních sítích jsou lidé ve věku 25-34 let. Těsně za nimi je věková skupina 35-44 let, což jsou ti, kterým bylo v době nástupu těchto sítí mezi dvaceti až třiceti lety věku. Průměrný věk uživatele sociální sítě je přibližně 37 let. Nejstaršími uživateli jsou uživatelé sítě LinkedIn a Classmates ve věku 44 a 45 let. Nejmladšími naopak uživatelé ve věku 17 let na síti Bebo.[19] (Obr. 3)



Obr. 3 Průměrný věk uživatelů sociálních sítí dle webu výzkumy.cz v roce 2012

[Zdroj: http://www.vyzkumy.cz/clanky/459-demografie-v-socialnich-sitich-2012, upraveno autorem]

Mezi nejznámější sociální sítě v České Republice patří např. Libimseti.cz, Lide.cz, Spolužáci.cz, Google+, Twitter, MySpace. V našem výčtu nesmíme ovšem zapomenout na čistě firemní síť Yammer, profesní síť LinkedIn a hlavně musíme zmínit nejrozšířenější a potenciálně nejrizikovější síť Facebook a multimediální prostor YouTube.

První moderní sociální sítí na světě, jak ji známe dnes, byla Sixdegrees, která byla spuštěna v roce 1997, ukončena byla v roce 2000 z finančních důvodů a o rok později odpojena. Tato síť měla kolem 3 500 000 uživatelů a obsluhovalo ji okolo stovky zaměstnanců. Doména této stránky však stále existuje, je však dostupná jen pozvaným členům. Filozofie této sítě nebyla nikdy naplněna, neboť na konci devadesátých let nebyl internet zdaleka tak masivně rozšířený jak je tomu v současnosti.[23]

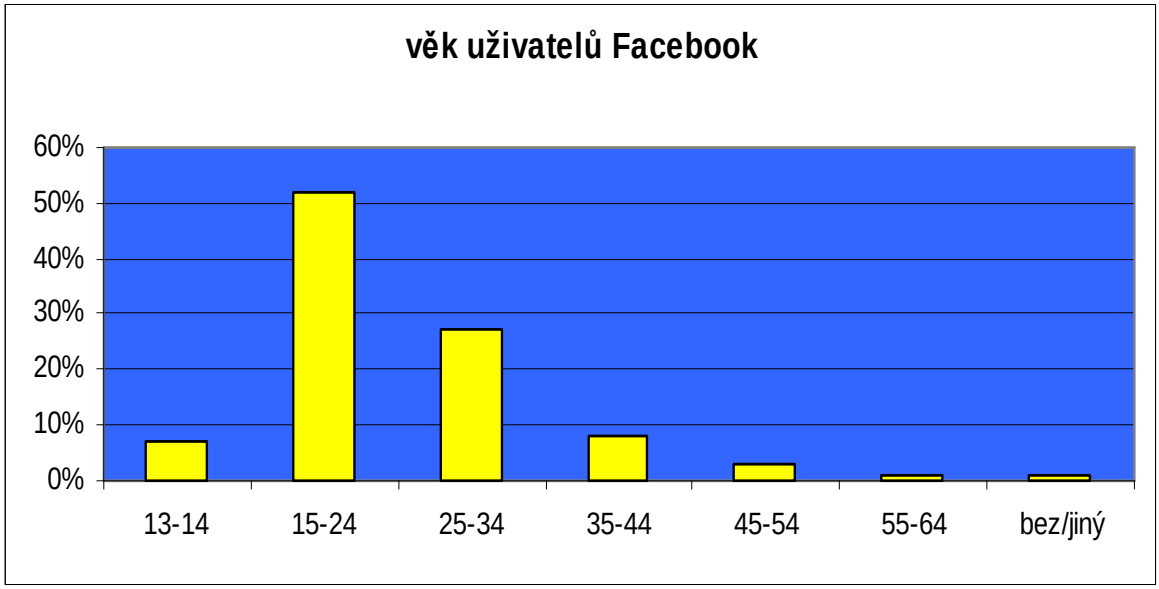
2.1 Facebook

Je nejvíce diskutovaným fenoménem dnešní doby. Jeho vznik je datován rokem 2004 bývalým studentem Harvardské univerzity. Systém měl sloužit jen a pouze pro posluchače na Harvardu, pod názvem Thefacebook.com. Postupně se však připojovaly další univerzity. Od roku 2006 se postupně začaly připojovat soukromé nadnárodní obchodní společnosti a zároveň všichni, kdo měli zájem se zaregistrovat, nesměli být ovšem mladší třinácti let.

V roce 2007 byl Facebook s 57 miliony uživatelů největším studentským webem. V září roku 2012 počet uživatelů překonal magickou hranici a přiblížil se 1,1 miliardě aktivních uživatelů, a to nejen studentů. Věková hranice uživatelů Facebook v ČR je uvedena na obr. 4.[17]

Nebezpečí tohoto serveru spočívá ve vysoké kumulaci citlivých osobních údajů, dat a aplikací, které vedou k jejich shromažďování a využívání. Vzhledem k obrovskému počtu jeho uživatelů se tím zvýšilo i riziko setkání uživatele sítě s různými formami sociálně patologických jevů, včetně kyberšikany a všech jejich druhů.

Společnost čelila v Kanadě obvinění z porušení zákona o shromažďování údajů, které byly uživatelem při odhlášení ze sítě vymazány, ale společností uloženy a zřejmě i nadále využívány.



Obr. 4 Věkové složení uživatelů FB v ČR v roce 2010 dle internetového časopisu Lupa

[Zdroj: http://www.lupa.cz/clanky/cesko-v-socialnich-sitich/, upraveno autorem]

2.2 YouTube

Tento server umožní prakticky komukoli nahrát, veřejně reprodukovat a sdílet videa s jakoukoli tématikou, včetně škodlivého nebo společensky nebezpečného obsahu. Ten se dá sdílet i na webových stránkách, nebo sociálních sítích. Dennodenně je shlédnuto více jak dvě miliardy videosouborů a stovky tisíc je jich tam uloženo.[16]

Každý měsíc ji navštíví až 82 % uživatelů, to znamená každý desátý uživatel, který se pohybuje v internetovém prostředí na něj chodí denně. V současné době jde o největší internetový server na sdílení videosouborů.[24]

S množstvím videosouborů přibývá porušování autorských práv a příliš velká svoboda slova. Dalším problémem je rozmáhání videí s tematikou sexu, zobrazování násilných scén, rasismu, pomlouvačného obsahu, videí s problematikou kybernetické šikany různých forem atd.

3 ZÁKLADNÍ POJMY PROBLEMATIKY ANALÝZI RIZIK

Pojmy nebezpečí a riziko je v reálném prostředí zaměňováno, nebo je mu dáván stejný význam. Proto je třeba, abychom si obě definice krátce popsali a vysvětlili jejich postavení v našem případě.

Cílem analýzy rizika je vytvořit podklady manažerům rizik tak, aby byli schopni je dále ovládat a zároveň dát podklady rozhodovali pro rozhodování o riziku.[10]

V našem případě se namísto manažera bude jednat o metodiky prevence na různých typech škol, odborníky přes kybernetickou šikanu, ředitele škol, psychology, rodiče, a další veřejnost, kterou tato problematika zajímá.

3.1 Riziko

Tento pojem je vždy spojován s určitou pravděpodobností vzniku nebezpečné situace a s možností škody. Dá se tedy říci, že je důsledek aktivace určitého nebezpečí, u kterého se projeví negativní následek. Tímto následkem je vzniklá škola, a to jak finanční tak například ztrátou na lidských životech atd.[10,11]

„Riziko je tedy pravděpodobná újma způsobená dotčené osobě (nositeli rizika), vyjádřená buď penězi nebo jinými jednotkami (počtem dnů pracovní neschopnosti, počtem lidských obětí).“[10]

Riziko se tedy chápe jako očekávání něčeho nepříznivého. Jeho újma může být předem známa, nebo může mít náhodný charakter.

V oblasti kyberšikany a sociálních sítí můžeme riziko chápat např. jako:

- *nebezpečí psychické nebo ekonomické újmy,*
- *nejistotu vznikající v souvislosti s možným výskytem události,*
- *osoba vystavená újmě,*
- *nebezpečí vzniku nějaké újmy,*
- *pravděpodobnost vzniku příslušné újmy*.[11]

Riziko je vztahováno na nějakou vymezenou dobu a k nějakému prostoru. V našem případě prostoru virtuálním.

3.2 Nebezpečí

Můžeme jej definovat jako reálnou hrozbu poškození vyšetřovaného objektu nebo procesu.

A právě identifikace nebezpečí je výchozí úlohou analýzy rizika.[10]

Nebezpečí může , ale taky nemusí být realizováno. Realizace nebezpečí se může projevit i více než jedním způsobem. Každý jednotlivý způsob realizace nebezpečí, vyznačující se výskytem určitých skutečností, označujeme jako **scénář nebezpečí,** který se mění v závislosti na čase.

Scénář nebezpečí je souhrnem:

- *okolností, v nichž se nebezpečí realizuje,*
- *skutečností, jež realizaci provázejí nebo po ní následují*.[11]

Nebezpečí je tedy chápáno jako zdroj ohrožení a riziko jeho míra.

3.3 Vybrané metody analýzy rizik

Metod k posouzení rizika a jeho hodnocení je celá řada. Může se jednat o základní a jednoduché deterministické metody až po počítačové modelování pomocí softwarových nástrojů. Jednotlivé metody se různí dle zkoumaných problémů a jejich kritérií.

V našem výčtu si krátce charakterizujeme jen následující vybrané:

Check list – seznam kontrolních otázek který je založený na postupné kontrole plnění předem stanovených podmínek a opatření.

What If – skupinové řešení problémů, při kterém osoby dobře obeznámeny se zkoumanou problematikou hledají řešení na očekávané události, které se mohou v procesu vyskytnout.

Účelem je odhalit nebezpečné situace, identifikovat zdroje rizika nebo události, které mohou zapříčinit nehodu s nežádoucími následky.

Hazop – je postup, který je založený na pravděpodobnosti hodnocení ohrožení a z nich plynoucích rizik. Je definován pro přesně danou problematiku v jednotlivém podniku. Účelem je důkladně prozkoumat proces nebo činnost a následně zjistit, zda odchylky od normálu mohou způsobit nežádoucí následek.[10]

PNH – touto jednoduchou bodovou polo-kvantitativní metodou se vyhodnocuje riziko ve třech jeho složkách:

- odhad pravděpodobnosti vzniku (**P**) – je zde na stupnici 1 – 5 zahrnuta míra, úroveň a kritéria jednotlivých nebezpečí a ohrožení,
- pravděpodobnost následků – závažnost (**Z**) – rovněž stupnice od 1 do 5,
- názor hodnotitelů (**H**) – v této části jsou zohledněny mimo jiné počty ohrožených osob, čas ohrožení, dynamika rizika, psychosociální rizikové faktory a další vlivy. Stejně jako v předchozích případech i zde je hodnocení na škále 1 – 5.

Celkové hodnocení rizika, ukazatel míry rizika (**R**), se dostane součinem **R = P x Z x H**

Na základě výsledku nám bodového rozpětí vyjádří naléhavost přijetí opatření ke snížení rizika(Tab.1).

Tab. 1 Přijatelnost rizika [10]

Rizikový stupeň	**Hodnota rizika**	**Míra rizika**
I.	> 100	Nepřijatelné
II.	51 – 100	Nežádoucí
III.	11 – 50	Mírné
IV.	3 – 10	Akceptovatelné
V.	< 3	Bezvýznamné

4 CÍL PRÁCE A JEJÍ METODIKA

Tato kapitola nám objasní cíle a metody, které byly zvoleny pro jejich naplnění.

4.1 Definice cílů práce

Cílem této bakalářské práce je seznámit se s vybranými riziky kybernetické šikany, které mají úzkou souvislost se sociálními sítěmi i dalšími prostředky komunikace, např. mobilními telefony.

Dále si klademe za cíl zjistit povědomí u vybrané referenční skupiny o různých formách, dopadech a znalosti prevence kybernetické šikany.

V neposlední řadě budou navrženy opatření ke zlepšení preventivních opatření, ke snížení vzniku rizika nebo jeho dopadu na vybranou referenční skupinu i další účastníky komunikace na sociálních sítích.

4.2 Metodika práce

Primární metodou teoretické a části praktické práce bude obsahová analýza literárních rešerší a internetových zdrojů a jejich následná fragmentace.

Jako další metoda sběru dat bude použita kvantitativní metoda dotazníkového šetření. Tato forma nabízí dostatek času k vyplnění písemného dotazníku, je časově i finančně méně náročná, umožňuje statistickou analýzu dat a zároveň zaručuje alespoň částečnou anonymitu respondentům.

Jako nevýhodu tohoto typu šetření vidíme v nižší návratnosti řádně vyplněných dotazníků a působení vnějších rušivých vlivů při jejich vyplňování.

Výsledky tohoto šetření budou podrobeny zkoumání na základě kterého bude vypracována samotná analýza rizik jednoduchou bodovou polo-kvantitativní metodou PNH u vybraných rizikových faktorů.

II. PRAKTICKÁ ČÁST

5 ANALÝZA STAVU KYBERENTICKÉ ŠIKANY

V následující části práce se zaměříme na samotnou analýzu této formy šikany, jejich specifik a projevů, profilů obětí, pachatelů a dopadů tohoto nežádoucího jevu.

Převážně sociální sítě jsou nejpoužívanějším médiem virtuální komunikace, vzniká zde vyšší míra pravděpodobnosti negativního, společensky nežádoucího chování. Pokud pomineme rizika zasílání spamu, poplašných zpráv, pokusů o získání přihlašovacích údajů do např. bankovních služeb, hoaxů (podvodná zpráva) apod., zjistíme že je kyberšikana velkým sociálně patologickým problémem.

Tento typ šikany má svůj původ v šikaně klasické. Ta ale není jen problémem žáků základních či středních škol, jak by se na první pohled mohlo zdát, je to problém generační a celospolečenský. Různé formy šikany zažívali vojáci základní služby za totalitního režimu ze strany déle sloužících vojáků či dokonce poddůstojníků. Následně i dnes, v pracovním prostředí, se s ní mnoho zaměstnanců mělo, a má možnost setkat formou tzv. mobbingu (špatné zacházení na pracovišti), bossingu (šikana ze strany nadřízeného) nebo chairingu (boj o vedoucí postavení, o „křeslo“). Své zkušenosti s ní mají i např. bývalí partneři, z nichž jeden rozchod mentálně nezvládne a pokouší se pomocí internetu mstít. V mnoha případech jsou následně zveřejněna choulostivá videa či fotografie své bývalé partnerky nebo partnera, s plným uvedením jména, adresy nebo telefonního čísla. Není rovněž výjimkou, umístění těchto diskriminujících záběrů na pornografické stránky.

Vyskytnout se může nejen ve školních zařízeních, ale i v místech pro volnočasové aktivity, jak dětí, mládeže tak dospělých a dokonce i v rodině.

5.1 Kyberšikana

Kopecký definuje tento pojem takto: *„Termínem kyberšikana (z anglického cyberbullying), označujeme nebezpečné komunikační jevy realizované prostřednictvím informačních a komunikačních technologií (např. pomocí mobilních telefonů nebo služeb v rámci internetu), jež mají za následek ublížení nebo jiné poškození oběti*.“ Kyberšikana je druhem psychické šikany.[3]

V naprosté většině případů je jednání útočníka zcela záměrné. Jsou známy i případy, kdy dojde ke komunikačnímu šumu mezi útočníkem a obětí, tedy k běžnému nedorozumění. Rovněž svoji úlohu může sehrát nedomyšlené jednání ze strany pachatele, nebo jen prostý

vtip útočníka velmi špatně pochopený druhou stranou. Oběť je poškozována opakovaně, ať už původním útočníkem, osobami které se do kyberšikany zapojí později anebo i pozorovateli. Je tedy třeba zmínit velmi důležitou úlohu těchto diváků kyberšikany, tzv. sekundárních útočníků, kterou si popíšeme v další části.[3]

Existuje několik rozdílů mezi šikanou klasickou a šikanou, objevující se na internetu. Klasická šikana, která může mít fyzickou i psychickou podobu, jasně definuje útočníka nebo útočníky, taky má své místo a čas, v němž k ní může dojít.

Kybernetická, nebo chcete-li počítačová šikana, je jen modifikovaná verze klasické šikany. Dá se tedy říci, že může i zesilovat účinek šikany klasické. Internetová pavučina dává některým lidem podnět k takovému druhu chování, kterého by se v běžném životě nikdy neodvážili. V síti internetu se nedá rozpoznat rozdíl ve fyzické síle pachatele, jeho společenské postavení, nikdo nepozná jeho skutečný věk, identitu, pohlaví. Rovněž délka trvání klasické šikany je jen omezená, kdežto kyberšikana může být dlouhodobá záležitost, neboť informace, které se na webových stránkách zobrazí, na nich můžou být i desítky let.[3]

Avšak základní rozdíl mezi šikanou klasickou a virtuální je v tom, že tento druh šikany se může objevit kdykoliv a kdekoliv, nelze ji předpovědět či odhadnout.

V základě rozeznáváme dva typy útoků kybernetické šikany:

- *přímé* – realizuje samotný útočník směrem k oběti. On sám vymýšlí strategii útoku, provádí útok samotný a má tedy nad svojí činností kontrolu. Mezi ním a obětí nestojí v cestě nikdo třetí,
- *nepřímé* – v zastoupení jiné osoby nebo osob. Touto třetí osobou může být např. administrátor příslušné sociální sítě, jemuž dá potřebné nepravdivé indicie samotný pachatel. Ten v případě zjištění porušení provozu dané webové stránky zajistí její odstranění. Ne vždy se mu však podaří zjistit oprávněnost. Může tím tedy oběť nevědomě poškodit. Tento typ považujeme za výrazně nebezpečnější.

5.1.1 Specifika kyberšikany

Kyberšikana má své základní specifické znaky, kterými jsou:

Anonymita – virtuální realita umožňuje pachatelům i či útočníkům kyberšikany být registrován pod různými pseudonymy. Používají tedy falešné profily, falešná jména, nebo falešné internetové stránky. To samé platí i pro používání emailových schránek a telefonních

čísel. Většina útočníků rovněž své profily mění a s tím tedy i svou identitu. Snaží se tak lépe kamuflovat svoji činnost a znesnadnit své odhalení čí dokonce dopadení. Díky těmto činnostem se tak cítí bezpečněji a tím může zároveň stoupat jeho agresivita vůči oběti či obětem.[3]

Změna chování útočníků i obětí – v převážně většině jsou původci kyberšikany chlapci nebo muži a jsou zároveň původci i tradiční formy šikany. Mezi nimi bývá rovněž velké množství těch, kteří byli dříve šikanováni klasickou formou. Tímto způsobem si tak můžou vybíjet svoji frustraci na někom cizím a nebo se mstít svému dřívějšímu nebo současnému šikanovateli. Bývají různého společenského postavení ale převládají lidé s vyšším sociálním postavením, kteří zároveň tráví více času na internetových sítích. Jejich oběti jsou ve většině případů lidé závislí na sociálních sítích, bývají méně obeznámeni s riziky pohybu na nich a nemají moc přátel, působí uzavřenějším dojmem až introverzí. Více tedy riskují s nakládáním se svými osobními údaji, nebo fotografiemi. Zároveň pro ně platí, že se někdy stávají sami pachateli kyberšikany nebo alespoň jejími pozorovateli a případně šiřiteli.[3]

Při komunikaci na sociálních sítích se chováme méně opatrně než v realitě. Jsme odvážnější, mluvíme bez zábran o citlivých tématech, udáváme jiný věk nebo status, děláme a zkoušíme co bychom v běžném životě neudělali. Útočníci mohou tedy atakovat jiné osoby vyhrožováním, pomlouváním nebo i vydíráním s vědomím, že je malá šance na jejich odhalení. Oběti mohou být vybrány zcela náhodně, ale může to být i cílený útok na konkrétní osobu, se kterou může mít útočník v reálném životě nějaký spor.

Místo a čas napadení – jsme-li připojeni on-line k nějaké počítačové síti, můžeme se stát terčem kyberšikany. Může to být ve dne, nebo v noci, stejně jako na počítači nebo mobilním zařízení připojeném k internetu. To je rovněž jeden z rozdílů mezi šikanou klasickou a internetovou. Prostor pro klasickou šikanu je dán reálným prostředím a časem, kdežto útok po síti nás může nachytat prakticky kdykoliv, kdy na síti jsme. Může se tedy stát, že oběť bude šikanována i mimo domov nebo republiku, např. v průběhu dovolené. I místo, které bylo doposud pro oběť bezpečné, se může stát pastí. Nezřídka útočník mění i místo odkud napadení provádí. O to problematičtější je pak zjištění a identifikace pachatele.[3]

Pozorovatelé (publikum) – přestože útočník povětšinou „pracuje“ beze svědků, existuje i skupina, která přihlíží dané kyberšikaně. Pozorovatelé, nebo také sekundární útočníci,

mohou například pomocí odkazů na příslušné internetové stránky informovat na uvedený problém další uživatele internetu. Tento jev se pak nekontrolovatelně šíří internetovým prostředím, kde si většinou najde velké množství svých koncových „zákazníků." Tím se může počet pozorovatelů pohybovat i v řádech milionů. Zároveň záznamy vědomě rozešlou dalším svým známým a spustí se tak dominový efekt. I oni tedy poškozují oběť, na kterou tato činnost může mít ještě větší dopad než útok samotný, ať vědomě či nevědomě. Nepřímo tak podporují pachatele, někdy i více než samotný původce útoku.[3]

Manipulace – aktivita komunikace probíhá převážně jedním směrem. Dalo by se přirovnat ke hře „kočky s myší". Útočník je v komunikaci aktivnější a může během ní měnit strategii. Pachatel nevnímá důsledky dopadu svého počínání, nemusí mít tedy k oběti žádnou empatii.

5.1.2 Projevy kyberšikany

Existuje několik způsobů a rovněž tak několik nástrojů, kterými se může kybernetická šikana projevovat. Útočníci ve většině případů používají více rozličných prostředků zároveň, počínaje prozváněním a konče např. zastrašováním, vyhrožováním únosem nebo i smrtí.

Nejběžnější projevy kyberšikany:

Publikování ponižujících videozáznamů, fotografií nebo informací – nezřídka si např. děti na základní škole nahrávají vzájemné a ze začátku nevinné škádlení, které může přerůst z klasické šikany, přes šikanu kybernetickou až po trestný čin. V mnoha případech se jedná dokonce i o pornografické snímky či videa s jasně definovanými tvářemi aktérů. Toto je především doménou mužů, z nichž někteří po rozchodu s partnerkou sáhnou po tomto druhu msty. Záznamy mohou být autentické, a nebo je pachatel může digitálně upravit pro svoji aktuální potřebu. Míst pro uložení takových materiálů je rovněž velké množství, ať se jedná o zasílání fotografií či videosekvencí elektronickou poštou svým známým, nebo známým oběti, uložením na webových stránkách či umístěním na YouTube nebo jiné sociální síti včetně sítě Facebook.

Pachatel k tomuto účelu může založit i vlastní blog, na němž bude informace ponižujícího nebo pomlouvačného charakteru prezentovat širokému okolí posluchačů a čtenářů. Oběti tak může způsobit nejen psychickou újmu, ale zároveň i újmu materiální, a to v tom případě, kdy se oběť bude ucházet o zaměstnání. Zaměstnavatelé si často své nové zaměstnance

prověřují i přes internetové stránky a pokouší se informovat o jejich profesním i soukromém životě. Toto rovněž platí pro výše zmíněné publikování ponižujících videozáznamů či fotografií.

Krádež identity a její zneužití – je velmi častý jev, který nemusí sloužit jen k zisku osobních údajů pro proniknutí do např. internetového bankovního účtu oběti, ale i ke kybernetické šikaně. Pachatel, po zisku potřebných údajů, se tímto způsobem může prezentovat jako oprávněný uživatel daného účtu na sociální síti a svoji oběť sledovat, ponižovat apod. Zároveň může touto cestou získávat informace z e-mailové adresy oběti, mazat její kontakty, nebo rozesílat zprávy s různým obsahem a přílohami v podobě videí a fotografií jménem oběti. V těch nejčernějších případech může prolomit heslo uživatelského bankovního účtu a přivést tak vědomě oběť až do krajních potíží. Vytvoření profilu oběti na sociální síti není pro pachatele žádný velký problém. Je to jen další způsob, jak oběti úmyslně škodit.[3]

Napadání účastníků v on-line komunikaci – internetové diskuze, sociální sítě, veřejné chaty a blogy jsou nejčastějším místem pro tento druh jevu. Povětšinou bývá cílem pachatele vyprovokovat přítomné účastníky k reakci stejné agrese, jakou útočník používá, při diskuzi na různá témata jak náboženského či politického charakteru a nebo i v oblasti sportu apod.[3]

Dalším projevem kyberšikany může být i forma elektronické ankety. Pachatelé ve specifikované, útočně zaměřené a uzavřené otázce očekávají odpověď, týkající se oběti, kterou posléze zveřejní např. na sociální síti.

5.1.3 Pachatelé kyberšikany

Množina možných motivací útočníků nebude ani zdaleka kompletní, ale poskytne nám alespoň dobrý přehled o častých případech, které byly reálně zaznamenány.

Pachatel může být v jakémkoliv věku, jeho schopnost útočit přes sociální síť je limitována pouze jeho schopností ovládat počítač a orientovat se v kybernetickém prostoru, což v dnešní době zvládají na jedné straně stále menší děti, na straně druhé i lidé stále starší. Existuje však určitá věková skupina, která bude z hlediska podílu všech útoků nejvíce zastoupena. Jedná se o tzv. teenagery - tedy skupinu s velkou pravděpodobností nejčastější také u klasické šikany. Specifické pro ně je, že se s virtuálním světem počítačů obvykle

seznámili už ve velmi nízkém, dětském věku. Technické prostředky pro útok proto ovládají dokonale. O co jsou jako útočníci vyspělejší na poli uživatelském, o to méně vyspělí a více nebezpeční pak mohou být svým chováním, často postrádajícím „brzdné mechanismy“. Nacházejí se totiž ve věku, kdy málokterý člověk již dovede domýšlet důsledky svého chování. Problémem je také snížená schopnost oddělovat skutečnou realitu od té virtuální. Zastánci počítačových her mohou namítat, kterak počítačové hry rozvíjejí schopnosti dětí, postřeh, nebo motorické reakce, oni si však neuvědomují, že hraní těchto her může u dítěte snadno vést k záměně virtuální reality za skutečnost. I tento fakt zvýšené síle budoucího útoku nahrává. Podobně jako ve hře útočník nebude mít se svou obětí, kterou z mnohdy sám sobě neznámých důvodů považuje za protivníka, žádné slitování. Už z tohoto plyne, že nejde vždy o fyzicky silnějšího jedince než je jeho oběť, právě naopak. V mnoha případech je útočník sám obětí klasického šikanování svých spolužáků a tímto způsobem se svým trýznitelům může mstít. Ve většině případů bývají útočníci semknutí ve skupině oproti jednotlivci. Z toho vyplívá nebezpečí častějších, organizovanějších a promyšlenějších útoků na oběť.

Nicméně ani pachatele jednotlivce nelze podcenit. Nemusí však být vždy motivován touhou po pomstě. Vzhledem k mentální nedozrálosti můžou být jeho pohnutky čistě osobního charakteru. Může se jednat o člověka, který bude hledat v této formě zdroj své zábavy, může demonstrovat svoji sílu, snažit se posílit pocit sounáležitosti, může se cítit znuděný, toužit po uznání apod.

Mezi nejčastější typy pachatele kyberšikany patří tzv.:

„Pomstychtivý andílek“ – typické pro něj je, že se jako agresor nevnímá. Vnímá sám sebe jako toho, co napravuje zlo, žije v představě, že chrání sebe i ostatní před pravým agresorem, který díky jeho intervenci trpí. Často sám kyberšikanu zažil, proto ji chce nyní druhým oplatit. Myslí si, že se touto formou pomstí a dá oběti lekci. Kyberagresor tohoto typu se zaplétá do hry, ve které se snaží ochránit svého šikanovaného kamaráda. Tito pomstychtivci pracují ve většině případů sami, ale není výjimkou že své aktivity a motivy sdílí se svými nejbližšími nebo těmi, které vnímají jako oběti nyní kyberšikanovaného agresora.[27]

„Bažící po moci“ – pachatelé tohoto typu chtějí jasně dávat najevo svoji autoritu, ukázat, že jsou skutečně silní na to, aby dokázali svoji oběť zmanipulovat prostřednictvím strachu.

Obvykle potřebují publikum, složené z jejich přátel, protože kyberšikana o které by nikdo nevěděl, by k pocitu moci nestačila. Rád se svými činy chlubí, ale pokud se mu nedostává patřičného uznání, přejde ke stupňování útoků. Pachatel je často obětí klasické šikany offline. V kybernetickém prostoru je posílen svojí anonymitou i tím, že svoji oběť nepotká tváří v tvář. Tento typ agresora je jedním z nejnebezpečnějších typů i proto, že oplývá technickými dovednostmi, málokdy si uvědomuje závažnost svých činů a někdy využívá kyberšikanu v zastoupení.[27]

„Sprosté holky“ – v tomto případě jsou typickými agresory děvčata, která tímto způsobem šikanují své kamarádky a nezřídka i kamarády chlapce. Rovněž ony žádají své publikum, chtějí aby ostatní věděli, kdo jsou zač a že právě ony mají sílu šikanovat ostatní. Tímto způsobem touží po tom být obdivovány ve své partě nebo sociální skupině.[27]

„Neúmyslný kyberagresor“ – tento typ agresora vůbec nenapadne, že by jím právě on mohl být. V chatovacích místnostech se většinou vydávají za někoho jiného nebo odpovídají bez přemýšlení o následcích svého chování na nenávistné či provokativní zprávy. Mají tendenci odpovídat ve vzteku nebo dokonce frustraci. Mohou se cítit i zranění nebo naštvaní buďto kvůli zprávám, které jsou jim zaslány ostatními nebo třeba kvůli tomu, co viděli v on-line videích. Motivem bývají dva hlavní důvody: **Můžu** a **Je to legrace**. Neúmyslný agresor se v záplavě vtipkování takto může chovat i k některému ze svých přátel, který ovšem nemusí vždy poznat, od koho mu zpráva přišla a jakou má vážnost.[27]

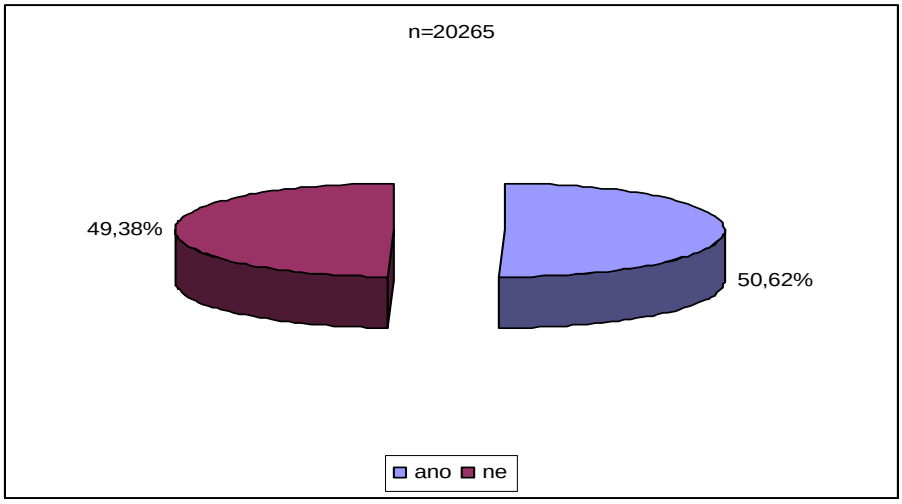
5.1.4 Oběť kyberšikany

Čím méně technicky a mentálně vybavený jedinec, tím větší je riziko, že se z něj stane oběť kybernetické šikany. V mnoha případech je oběť závislá na internetu a sociálních sítích. Ve virtuálním světě si hledá skupinu svých přátel, kterých se mu v reálném světě nedostává, nebojí se riskovat, vytváří si vazby a důvěřuje jim. Oběť svého šikanovatele ani nemusí znát, a převážně taky nezná. Ponížení a výhružky, které jsou směrem k oběti vysílány, jsou v tomto případě s mnohem horším dopadem než u klasické šikany, kde je útočník nebo útočníci známi. Útoky můžou být vedeny jak dlouhodobě, tak krátkodobě, s různou mírou nízké či vysoké intenzity a s použitím různých nástrojů.

Oběti tohoto druhu šikany se stydí přiznat sobě i okolí, že jsou terčem šikany, uzavřou se do sebe a většinou se dostávají do psychických problémů, bojí se chodit do školy, bývají pravidelně nemocní. Jsou samotářští, mají strach, nekomunikují s okolím a nechtějí se

s problémem svěřit. Vyhýbají se kolektivu, aktivitám jak ve škole tak mimo ni. Trpí ztrátou sebejistoty a sebedůvěry. Takové reakce mohou vyústit až v to, že oběť situaci psychicky nezvládne. Následkem může být sebevražedný pokus nebo pokusy, které jsou v mnoha případech dokonané.

V následujícím grafu jsou uvedeny údaje z výzkumu Univerzity Palackého Olomouc, který byl zveřejněn v roce 2012. V něm bylo zjištěno že z celkového počtu 20265 vzorků studentů základních a středních škol, se setkalo s kybernetickou šikanou 50,62 % dotazovaných. V tabulce pod grafem jsou uvedeny nejčastější formy kyberšikany, které se vztahují k výše jmenovanému výzkumu.



Graf 1 Oběti kyberšikany [9]

Tab. 2 Nejčastější formy kyberšikany [9]

Verbální útoky (urážení,ztrapňování, nadávání, ponižování)	33,44 %
Snaha o prolomení elektronického účtu	32,58 %
Obtěžování prozváněním	24,08 %
Vyhrožování, zastrašování	17,38 %
Krádež identity	10,09 %
Vydírání	7,33 %
Ponižování, ztrapňování pomocí fotografie	10,85 %
Ponižování, ztrapňování pomocí videa	5,58 %

5.1.5 Dopad kyberšikany

Na rozdíl od šikany klasické se kyberšikana dá hůře rozpoznat. Není na první pohled viditelná. Oběti kyberšikany se dostávají do psychických problémů. Přestože kybernetická šikana nezahrnuje přímý osobní kontakt mezi pachatelem a obětí, zůstává psychologicky a emocionálně velmi škodlivá. Převážně studenti základních a středních škol popírají závažnost škádlení, obtěžování v síti internet a označují je za neškodné aktivity. Realita však naznačuje něco úplně jiného.

Dopad kyberšikany na lidskou psychiku může mít následující charakter:

- *tenze, strach, stres,*
- *pokles sebehodnocení, sebedůvěry,*
- *depresivní a neurotické potíže,*
- *poruchy spánku,*
- *snížení frustrační tolerance,*
- *pocit neřešitelné situace, ztráta životní pohody,*
- *zkratovité jednání, riziko suicidia (sebevraždy)*
- *zvyšující se agrese,*
- *celková psychická nestabilita,*
- *trauma a posttraumatická stresová porucha*.[25]

5.2 Typy kyberšikany

Kybernetická šikana má mnoho druhů projevu. V této části práce popíšeme typy, s kterými se uživatelé sociálních sítí můžou setkat.

5.2.1 Kybergrooming

„Tímto termínem označujeme chování uživatelů internetu, která má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce.“[3]

Specifikem kybergoomerů je vydávají se za jinou osobu. Hlavním cílem jejich jednání je systematické přesvědčování převážně nezletilé oběti za účelem sexuálního obtěžování či pohlavního zneužití.

V tomto případě hovoříme o druhu psychické manipulace a chování, kdy se někdo pomocí internetu či mobilního telefonu vydává za někoho jiného, snaží se získat falešnou důvěru

napadeného a přimět ho k osobní schůzce. Takováto schůzka může vyvrcholit například napadením nebo sexuálním zneužitím oběti, zneužitím k dětské prostituci a nebo k výrobě pornografických materiálů. Hojně jsou využívány i inzertní portály nabízející možnost přivýdělku či možnost oslnivé kariéry (např. modelingu). S oblibou jsou navštěvovány sociální sítě zaměřené cíleně na nezletilé, např. na volnočasové aktivity nebo herní portály. V neposlední řadě rovněž různé typy seznamek, veřejně přístupných chatů, instant messengerů i mikroblogovacích stránek.[4]

Nejohroženější kategorií jsou děti ve věku 11-17 let, a to převážně dívky, tedy ta skupina, která se nejvíce objevuje on line na internetu na různých výše zmíněných typech stránek. Tato věková hranice nemá ještě vytvořen dostatek životních zkušeností a sociálních dovedností a snadno podlehne neznámému dobrodružství. Nejrozšířenějšími typy obětí jsou děti s nedostatkem sebedůvěry, děti v nouzi hledající náhradu za rodiče, děti velmi důvěřivé, naivní a děti v pubertě, které se nebojí mluvit o sexualitě velmi otevřeně. [4]

Dalším důležitým aspektem spojeným s internetovou manipulací je sociální zázemí mladého člověka. Velmi rizikovou skupinou jsou děti z finančně slabých rodin či dětských domovů. Útočník na ně velmi často aplikuje manipulaci, která je spojena s uplácením (tzv. „luring“). Za poskytnutí fotografií, osobních údajů, nebo za slib osobní schůzky je oběti nabídnuto např. značkové oblečení, mobilní telefon případně finanční hotovost. Do skupiny potenciálních obětí můžeme rovněž zařadit děti, které jsou závislé na internetových aplikacích, tedy sociálních sítích, chatech, případně on-line hrách. Za potenciální oběti lze rovněž považovat děti, které jeví známky závislostního chování ve vztahu k internetovým aplikacím, zejména chatu, sociálním sítím a on-line hrám.[26]

S rostoucím časem pohybu takového člověka se zvyšuje pravděpodobnost, že na kybergroomera narazí.

Sítě kybergroomerů v některých případech kooperují při únosech dětí k sexuálním deviacím, fyzickému týrání apod. Rovněž mívají ve zvyku si mezi sebou předávat databáze potenciálních obětí.

Proces kybergroomera prochází těmito etapami: [28]

- *výběr sociální sítě,*
- *příprava kontaktu ,*
- *kontakt,*

- *příprava na osobní schůzku,*
- *osobní schůzka*

5.2.2 Kyberstalking

„Stalking (lov, pronásledování) označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu.“[3]
Kyberstalkeři tedy využívají při pronásledování informačních a komunikačních prostředků. K základním projevům můžeme řadit opakované a dlouhodobé pokusy o kontakt s obětí formou zasílání e-mailů, telefonátů, SMS zpráv (služba dostupná na mobilních telefonech), pozorností a dárků, kontaktování oběti přes ICQ (program k zasílání textových zpráv a souborů), Skype, chatovací místnost apod.[5]

Rozdíl mezi kyberstalkery a kybergroomery je v tom, že se kyberstalkeři při svém pronásledování vyvarují fyzickému násilí. Ale i toto nemusí už být pravidlem, neboť jsou známy případy kdy byly ženy zavražděny svými bývalými manžely, kteří se prezentovali jako stalkeři nebo kyberstalkeři. Nejpočetnější skupinou obětí kyberstalkingu jsou kromě bývalých partnerů rovněž známé osobnosti či celebrity a politici.

Motivací chování stalkera nebo kyberstalkera je touha po pomstě, po moci a narcismus pachatele.
Typickými projevy kyberstalkingu jsou:

- *opakované pokusy o kontakt* – e-maily, telefony, SMS,
- *přímé nebo nepřímé výhružky* – demonstrování moci, který u normální osoby vzbuzují oprávněný strach a obavy,
- *zneužívání osobních údajů* – zveřejnění telefonního kontaktu a adresy oběti na internetu, např. s legendou že chce prodat byt nebo že poskytuje sexuální služby.[15]

Útočník může kontaktovat svoji oběť například formou vyhrožování, vydírání nebo navozením pocitu viny. Text zpráv, které útočník posílá, bývá povětšinou urážející nebo i zastrašující či vyhrožující tak, aby vzbudil obavy a strach. Někdy může text obsahovat i výhružku fyzického napadení či zabití oběti nebo jeho blízkých. Není však výjimkou i text pro oběť zkraje příjemný. Kyberstalker se snaží svoji oběť pomocí sociálních sítí nebo jinými komunikačními kanály pomluvit u jejich přátel, rodiny nebo v zaměstnání, např. informacemi na jím vytvořených webových stránkách, které se nezakládají na pravdě.

V zásadě můžeme říci, že stalkerem a tedy i kyberstalkerem může být:

- *osoba, kterou oběť osobně zná a ví, že ji pronásleduje,*
- *osoba, kterou oběť osobně zná, ale neví, že ji pronásleduje,*
- *osoba, kterou oběť osobně nezná (např. kyberstalkeři hledající své oběti na internetu).*[5]

Kyberstalkerem se rovněž může stát:

- *bývalý partner oběti,*
- *uctívač,*
- *neobratný nápadník,*
- *ublížený pronásledovatel,*
- *sexuální útočník,*
- *poblouzněný milovník.*

Kybernetičtí stalkeři se zpravidla neuchylují k fyzickému napadení. Používají však jako nástroje různé typy spywarových programů. Důležité je mít na paměti, že každý kyberstalker může být stalkerem a opačně.[20]

Druhy reakcí na kyberstalking:

- *psychické* – nervozita, podrážděnost, lekavost, pocity vyčerpanosti, únava, ztráta chuti do života, pocity bezradnosti a bezmoci,
- *finanční* – investice do bezpečnosti, dočasné přestěhování,
- *pracovní* – zhoršení výkonu v zaměstnání, změna pracovního místa nebo ukončení pracovního poměru,
- *sociální* – snížení zájmu o dříve důležité vztahy a aktivity, izolace, strach z neznámých lidí.[15]

5.2.3 Kybersexting

Jedna z forem kybernetického šikanování se projevuje zasíláním fotografií, nebo video sekvencí s tematikou sexu. Sexting (složenina slov sex a textování) může mít mnoho podob, od těch nevinných mezi dospělými, až po ty nejvážnější případy, jako je například dětská pornografie. Jedná se o vysoce rizikové chování, neboť útočník může mít k dispozici velmi citlivý materiál, který se velmi často zneužívá na sociálních sítích, kde může dlouhou dobu kolovat, popř. být použit až za dlouhé období od jeho vzniku. Je opravdu velmi

těžké tyto materiály ze sociálních sítí a jiných portálů odstranit, nebo zastavit jejich šíření. Mnohdy se tyto prostředky stávají zdrojem vydírání. První případy sextingu byly v České Republice zachyceny v roce 2005. Sexting může jako takový podporovat šíření dětské pornografie.

I zde jsou potenciálními oběťmi mimo dospělých, převážně děti a dospívající mládež. Pořizování vyzývavých a intimních fotografií se stalo součástí virtuální intimity mladých lidí.

5.2.4 Happy Slapping

Jeho účelem je nečekaně fyzicky napadnout buď mladistvého, dospělého nebo i starého člověka. Spolupachatel agresora celý čin nahrává na mobilní telefon nebo kameru. Takto pořízené video poté umístí na internet nejčastěji na YouTube. Video je určeno k tomu, aby své diváky pobavilo. Obětí se může stát prakticky kdokoliv, někdo, kdo se jen tak projíždí v parku na kolečkových bruslích nebo běhá, někdo kdo pospíchá na autobus, atd. Oběť je tak traumatizována několikanásobně, jak samotným útokem, tak i následným ponižujícím zveřejněním videa. Ve Velké Británii, kde se termín Happy Slapping používá nejčastěji, je slovo spojováno s anglickými pojmy jako je "chav“ (urážlivé pojmenování určité skupiny dospívajících v Anglii) nebo "ned“ (obdoba „hooligans“).[18]

Známý je případ ubití bezdomovce partou tří výrostků v Británii. Na sociálních sítích kolovalo nějakou dobu jimi natočené video, kde po útoku natáčeli jeho bezvládné a zkrvavené tělo. Ani v České republice není o tyto případy nouze.

5.2.5 Outing

S tímto pojmem se běžně nesetkáme, ale s jeho projevem rozhodně ano. Jedná se především o natáčení na videokameru nebo mobilní telefon v choulostivých nebo až trapných situacích a zveřejnění těchto dokumentů na sociálních sítích. Stačí se jen podívat na síť YouTube a jistě mezi videi najdeme důkazy tohoto jevu. Tímto způsobem je rovněž možno oběti vyhrožovat nebo ji dokonce vydírat.

5.2.6 Syndrom FOMO

Tento pojem pochází z anglického Fear of missing out, což se dá volně přeložit jako obava nebo strach z toho, že něco zmeškáme či prošvihneme.

Do této kategorie řadíme lidi ve věkovém rozpětí 18 až 30 let, což je doba kdy si každý jedinec utváří svou vlastní identitu, navazuje nové známosti a snaží se společensky co nejlépe uplatnit. Díky sociálním sítím zveřejňujeme, aktualizujeme a chlubíme se svými zážitky z dovolených, rodinných událostí, pracovních úspěchů nebo tím, že jsme si něco nového pořídili. O neúspěšných pokusech nebo událostech které nedopadli zrovna nejlépe se ovšem na svém profilu raději nezmiňujeme. Vytváříme tak kolem sebe tedy iluzi, snahu být v očích ostatních lidí lepší než ve skutečnosti vlastně jsme.[12]

Pokud je jedinec dostatečně sebevědomý a ví, kde je hranice virtuální komunikace, nemusí to být až takový problém si uvědomit, že profily a údaje na nich u našich známých můžou být i smyšlené nebo přinejlepším přehnané. Nemá tedy potřebu se tím trápit a srovnávat se s ostatními.[12]

Jinak to může ovšem být u jedince, který je nejistý, přecitlivělý nebo trpí depresemi. Taková osoba už může mít předpoklady i vrozené, které se do situace můžou promítnout. Například po zhlédnutí fotografií z oslavy, na kterou nebyl dotyčný pozván, se sebevědomí může rovnat bodu mrazu nebo se dokonce dostaví stavy úzkosti.[12]

Reakce můžou být různého charakteru. Jedinec se může snažit dostat na úroveň ostatních, může situaci řešit i rezignací, snaží se aktivněji zapojit do zjišťování informací o dalších společenských akcích, investuje čas, peníze i energii do cestování nebo investuje značné finanční částky do značkové módy. Vše si samozřejmě pečlivě dokumentuje a prezentuje prostřednictvím sociálních sítí. Výsledkem tohoto snažení bývá vyčerpání, únava a stres, že vše nestihne, neuvidí, že mu něco pod rukou uteče, že něco nezvládne.[12]

6 DOTAZNÍKOVÉ ŠETŘENÍ

V rámci daného průzkumu byl vytvořen na stránkách Survio.cz formulář s 15 otázkami, z nichž 3 byly otevřené, 8 uzavřených a 4 s více možnostmi odpovědí. Otázky byly vytvořeny tak, aby reflektovaly stanovené cíle.

Výsledky dotazníkového šetření budou zpracovány do grafické podoby, která by měla sloužit k lepší orientaci. Ke grafům, kromě jednoho kde byla odpověď stoprocentní a dalších dvou které byly součástí statistické tabulky, budou uvedeny popisy a vysvětlení.

6.1 Stanovení cílů

Cílem našeho šetření je zjistit u dané skupiny dotazovaných jejich povědomí o problematice spojené s kyberšikanou, o jejích specifikách, dopadech, o informacích, které nejčastěji uvádějí na sociálních sítích, o druzích kyberšikany. V neposlední řadě zjistíme, zda je tato referenční skupina připravena a schopna se jí bránit, a jaká forma prevence by podle jejich názoru byla nejvhodnější.

6.2 Metodika dotazníkového šetření

Jako referenční skupinu, která je předmětem dotazníkového šetření jsme vybrali tzv. teenagery, tedy adolescentní jedince ve věku 15–20 let. V převážné většině se jedná o studenty různých typů středních škol a učilišť.

Volba právě na tuto skupinu padla ze dvou důvodů:

- jsou dobře obeznámeni s pohybem na sociálních sítích, kde je výskyt kyberšikany největší,
- je zde větší míra pravděpodobnosti, že se s kybernetickou šikanou již v minulosti setkali,

Oslovili jsme namátkově 50 teenagerů v centru města Zlín, jak mužského tak ženského pohlaví. Dotazníková metoda probíhala co nejvíce anonymně, vždy byl dotazován jen jeden respondent. Každý z respondentů měl dostatek času k jeho vyplnění. Po ukončení byl vypsaný dotazník respondentem zalepen do přiložené obálky a odevzdán. Celkové vyhodnocení výsledků bylo počítáno ze 48 ks řádně vyplněných dotazníků. Dva tiskopisy museli být skartovány z důvodu jejich jen částečného vyplnění.

Dotazníkové šetření proběhlo v období 23.7. – 26.7. 2014. V první polovině měsíce srpna byli obálky s dotazníky rozlepeny a zpracovány do stávající podoby.

Složení a počet respondentů, kteří se zúčastnili dotazníkového šetření, nám představují následující tabulky.

Tab. 3 Věková struktura respondentů [*vlastní zpracování*]

Věk respondentů	Počet respondentů	Procentuální zastoupení
15	6	12,5 %
16	11	22,9 %
17	15	31,3 %
18	10	20,8 %
19	4	8,3 %
20	2	4,2 %

Tab. 4 Základní statistické údaje dotazníkového šetření [*vlastní zpracování*]

Základní statistické údaje	
Věkový průměr	17,5
Věkové rozpětí	15–20
Počet žen	25
Počet mužů	23
Celkový počet respondentů	48

6.3 Výstupy dotazníkového šetření

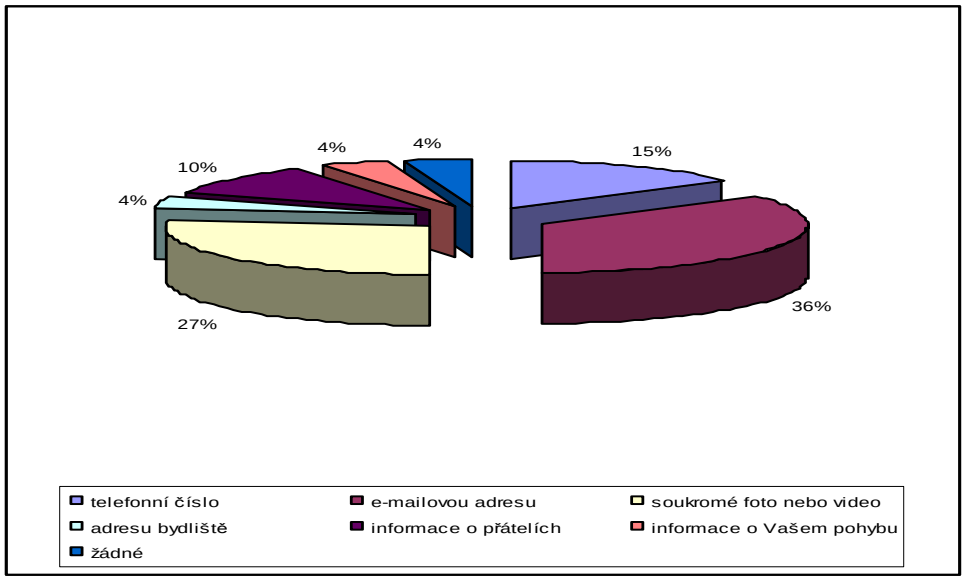
Otázka č. 1 „Jaký je Váš věk?“ a **otázka č. 2** „Vaše pohlaví?“ jsou součástí statistických údajů v tab. 3 a tab.4, tudíž nemají podobu grafu.

Otázka č. 3 – Používáte ke komunikaci některou ze sociálních sítí?

V této otázce nešlo ani tak zjišťovat o kterou konkrétní sociální síť jde. Cílem bylo se utvrdit v našem přesvědčení, že studenti využívají sociální sítě prakticky stále, proto nás výsledek nepřekvapil. Všech 48 dotazovaných komunikuje prostřednictvím alespoň jedné sociální sítě. Z toho důvodu zde rovněž neuvádíme grafické znázornění.

Otázka č. 4 – Jaké informace osobního charakteru na nich nejčastěji zveřejňujete?

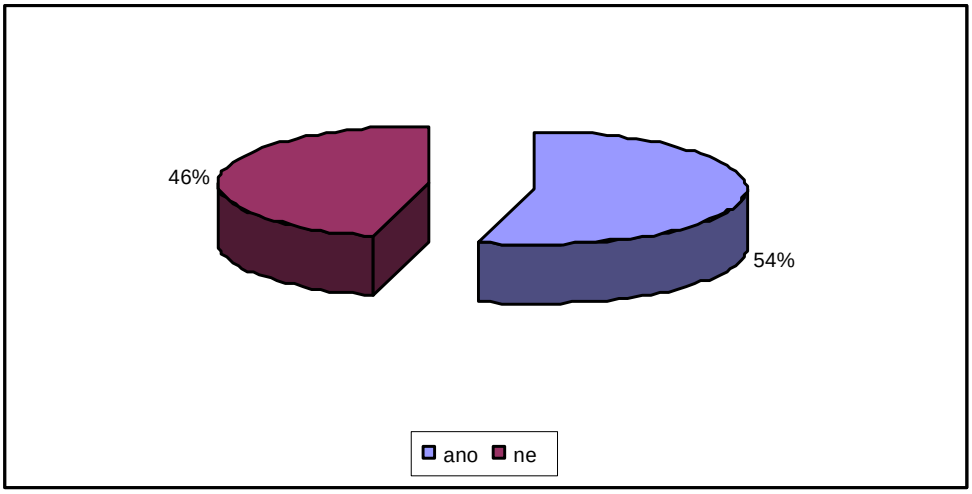
Tady bylo možno zvolit jednu ze sedmi nabízených odpovědí, anebo zvolit svoji vlastní. Poslední možnost nevyužil nikdo. Celkem 17 uživatelů (35 %) poskytuje e-mailovou adresu, 13 uživatelů (27 %) zveřejňuje své osobní fotografie nebo videa. S větším odstupem respondenti zvolili telefonní číslo (15 %) a informace o přátelích (10 %).



Graf 2 Nejčastěji zveřejňované informace [*vlastní zpracování*]

Otázka č. 5 – Setkali jste se na sociální síti Facebook a YouTube s projevy kyberšikany?

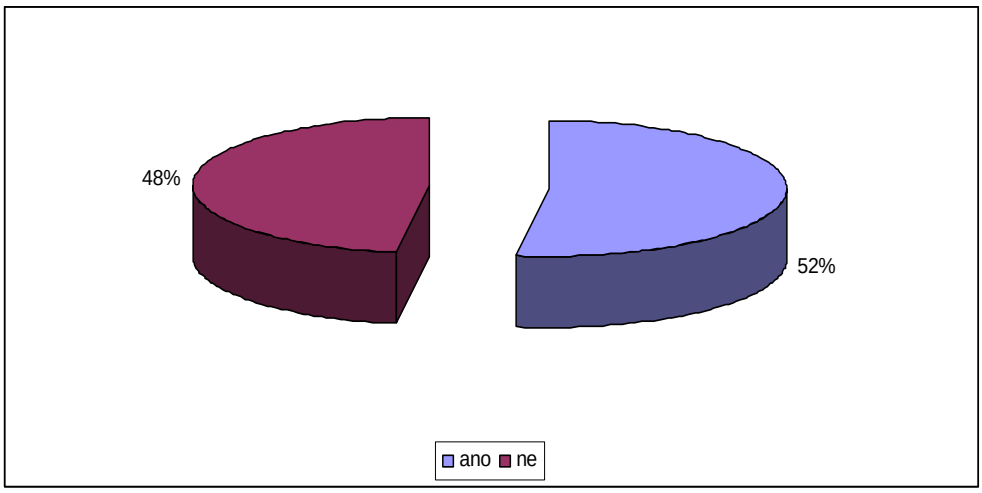
Účelem této otázky bylo zacílit na dvě sociální sítě z teoretické části naší práce. Chtěli jsme se dovědět, zda se respondenti setkali s projevy kyberšikany právě na těchto zmiňovaných sítích. Výsledek je téměř vyrovnaný, 26 respondentů (54 %) se setkalo, zatímco 22 (46 %) nic takového na Facebooku a YouTube nezaregistrovali.



Graf 3 Projevy kyberšikany na Facebook a YouTube [*vlastní zpracování*]

Otázka č. 6 – Stali jste se někdy obětí, pachatelem nebo svědkem kybernetické šikany?

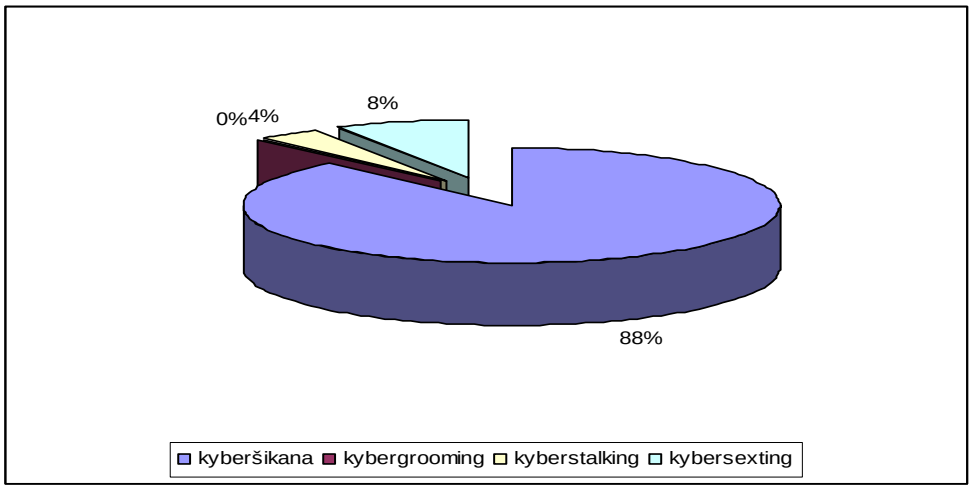
Náš průzkum ukázal že 25 uživatelů (52 %) se s některým typem a různou formou kyberšikany už někdy v minulosti setkali a to buďto jako oběť, pachatel nebo případně svědek události. Tato čísla zapadají do výzkumu projektu E-bezpečí z roku 2012.



Graf 4 Oběť, pachatel nebo svědek kybernetické šikany [*vlastní zpracování*]

Otázka č. 7 – Pokud jste odpověděl(a) v otázce č. 6 ano, tak kterého druhu kyberšikany se to týkalo?

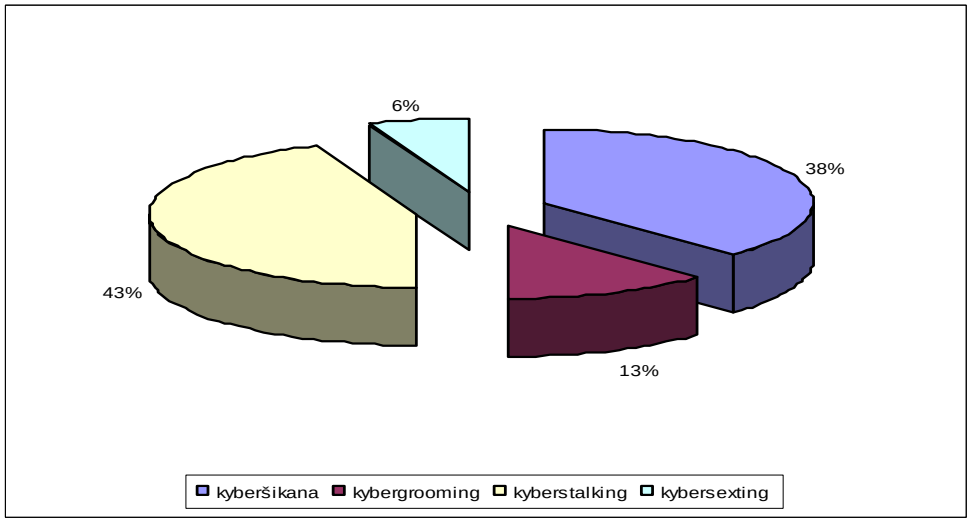
Klasická kyberšikana, tedy např. obtěžování, prozvánění, zastrašování, publikování ponižujících fotografií či videí, zažilo z 25 „kyberšikanovaných“ celkem 22 respondentů. Kyberstalking uvedl jeden respondent (4 %), zkušenosti s kybersextingem mají dva respondenti (8 %) a s kybergroomingem se nesetkal ani jeden z dotazovaných.



Graf 5Kterého druhu kyberšikany se to týkalo [*vlastní zpracování*]

Otázka č. 8 – Který z výše jmenovaných druhů je dle Vás nejnebezpečnější?

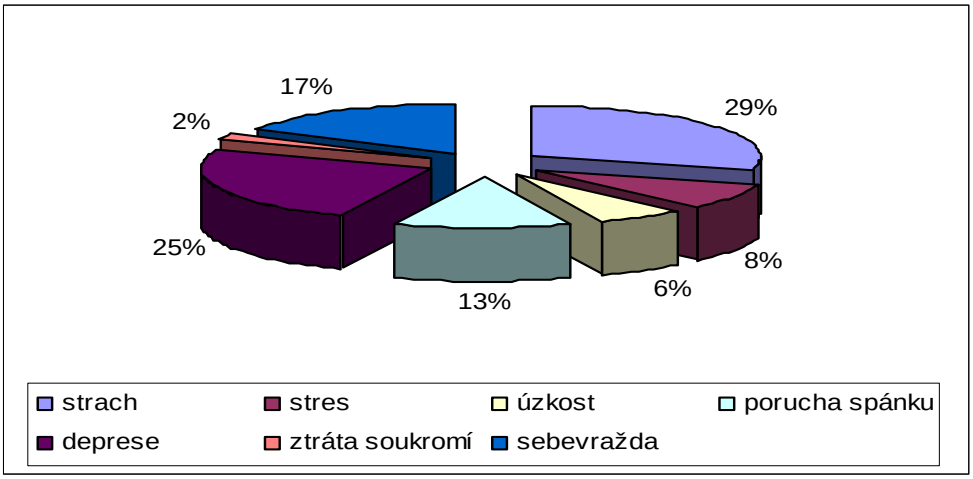
Kyberstalking byla vybrán jako nejnebezpečnější druh. Potvrdilo to 21 respondentů, tedy 43 %. Druhým v pořadí byla kyberšikana, tu vybralo 18 tázaných (38 %), pak kybergrooming 6 lidí (16 %) a kybersexting 3 (6 %).



Graf 6 Nejnebezpečnější druh kyberšikany [*vlastní zpracování*]

Otázka č. 9 – Jaký dopad může mít podle Vás některý z druhů kyberšikany?

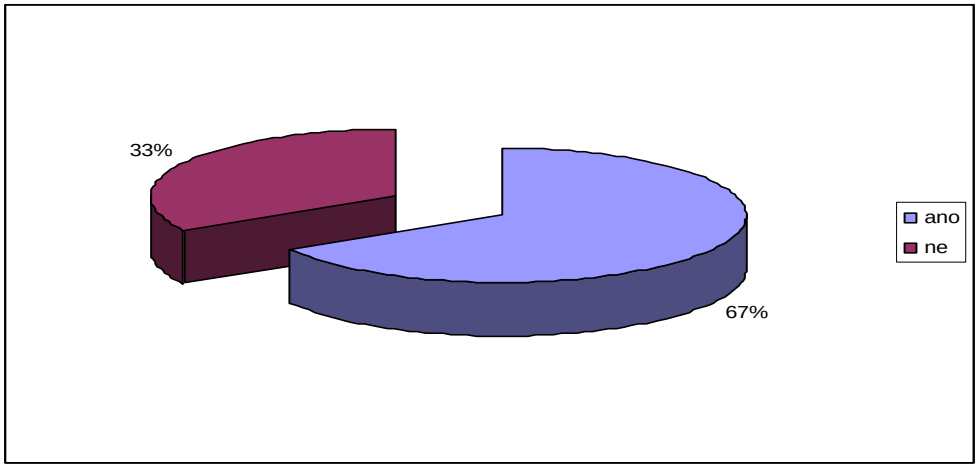
Nejčastěji udávaným dopadem kyberšikany je podle respondentů strach, který označilo 14 (29 %) z nich. Druhý nejčastější dopad byli označeny deprese, ty volilo 12 (25 %) respondentů, následovala sebevražda s 8 odpovědi (17 %), porucha spánku (13 %), stres (8 %), úzkost a ztráta soukromí.



Graf 7 Dopad druhů kyberšikany [*vlastní zpracování*]

Otázka č. 10 – Víte kdo provádí ve Vaší škole prevenci před nebezpečnými jevy (šikana, kyberšikana atd.)?

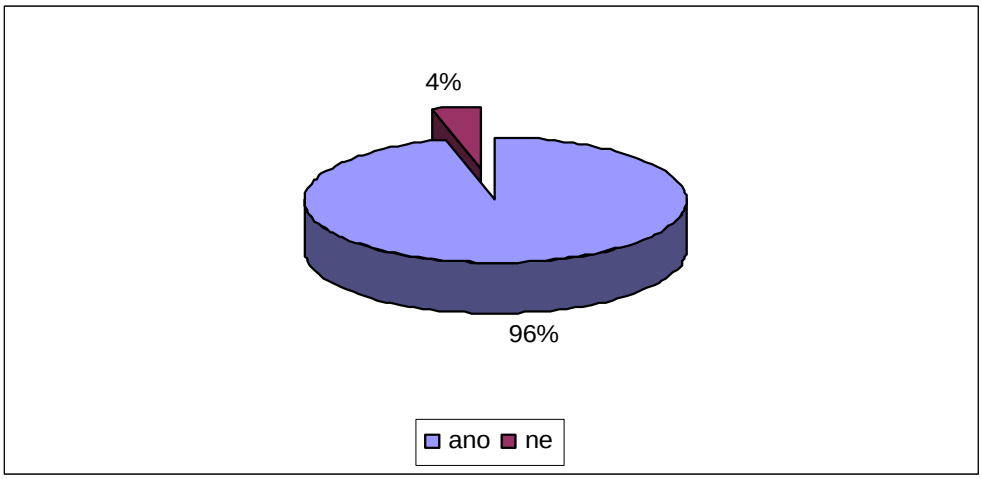
Tyto výsledky byli pro nás velmi překvapivé. Někteří oslovení studenti vůbec netušili, kdo na jejich škole vede metodickou činnost zaměřenou na prevenci nebezpečných nebo sociálně patologických jevů (33 %, 16). Celkem 32 z nich(67 %), znalo konkrétní osobu v podobě metodika prevence nebo psychologa školy.



Graf 8 Kdo provádí prevenci před nebezpečnými jevy [*vlastní zpracování*]

Otázka č. 11 – Oznámili byste událost spojenou s kyberšikanou na Vaší škole?

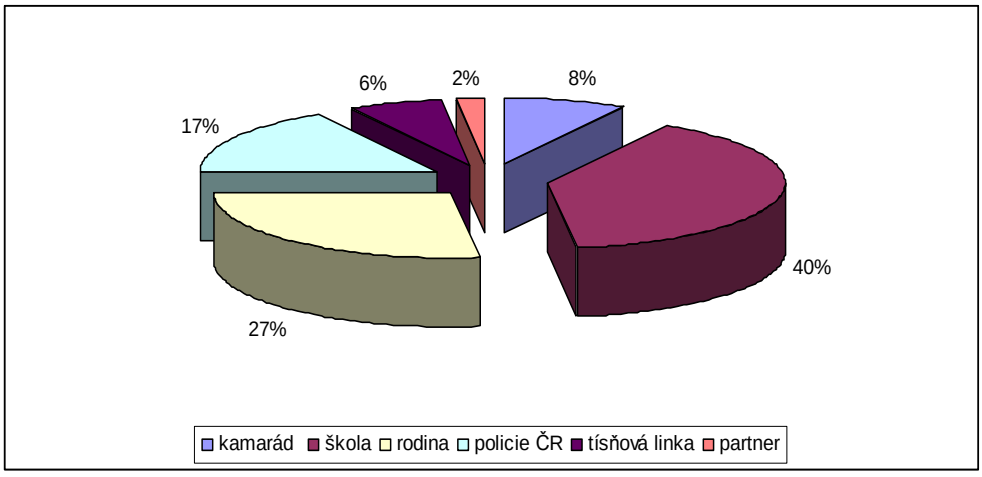
Valná většina (96 %, 46) by našla odvahu a výskyt kyberšikany by nahlásila. Zbývající dva (4 %) zakřížkovali ne. S největší pravděpodobností je k tomu vede strach, že by se stali terčem pozdějšího útoku samotného pachatele nebo pachatelů.



Graf 9 Oznámení události spojené s kyberšikanou [*vlastní zpracování*]

Otázka č. 12 – Na koho byste se s problémem spojeným s kyberšikanou obrátili nejdříve?

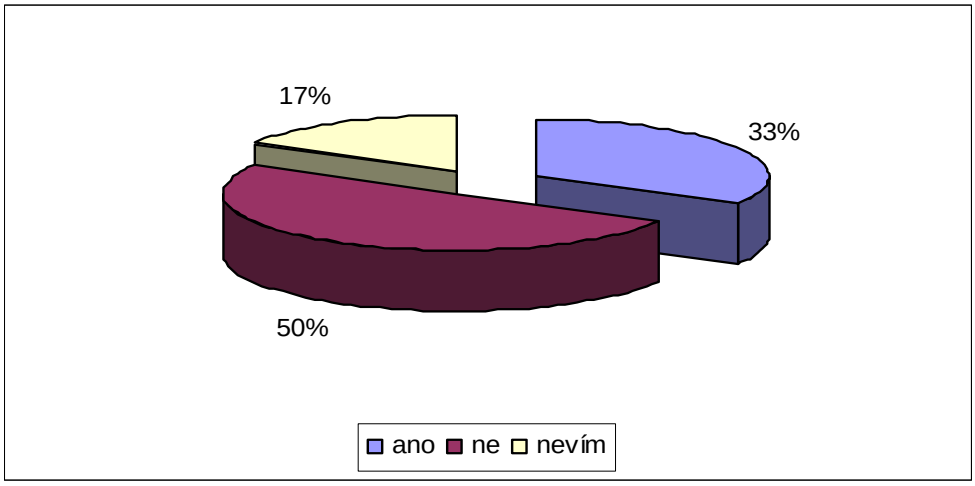
Dotazovaná skupina by se nejdříve obrátila na školu, celých 40 %, tj. 19 z nich. Na druhém místě by 13 oslovilo rodinu (27 %), 8 z nich (17 %) by alarmovalo Policii ČR, 3 (6 %) by volali tísňovou linku, 4 respondenti (8 %) by se svěřili kamarádovi, a jeden (2 %) by uvědomil jako prvního svého partnera.



Graf 10 Na koho se s problémem s kyberšikanou obrátit [*vlastní zpracování*]

Otázka č. 13 – Myslíte si, že se dá vzniku kyberšikany předejít?

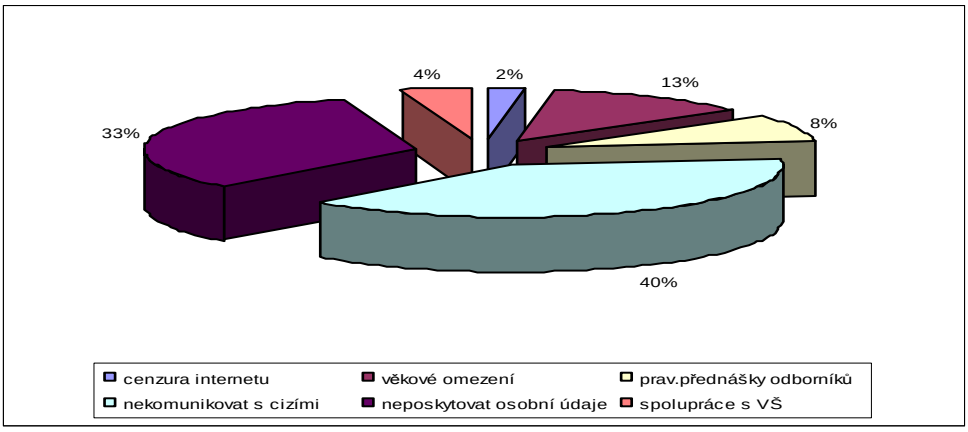
Polovina dotázaných si myslí, že proti fenoménu kybernetické šikany není adekvátní obrany. Na druhé straně 33 % z nich tj. 16 dotazovaných je toho názoru, že je cesta k potlačení tohoto jevu. Osm z celé skupiny (17 %) vyplnilo v dotazníku odpověď nevím.



Graf 11 Dá se vzniku kyberšikany předejít? [*vlastní zpracování*]

Otázka č. 14 – Jaká forma prevence by byla podle Vás nejúčinnější?

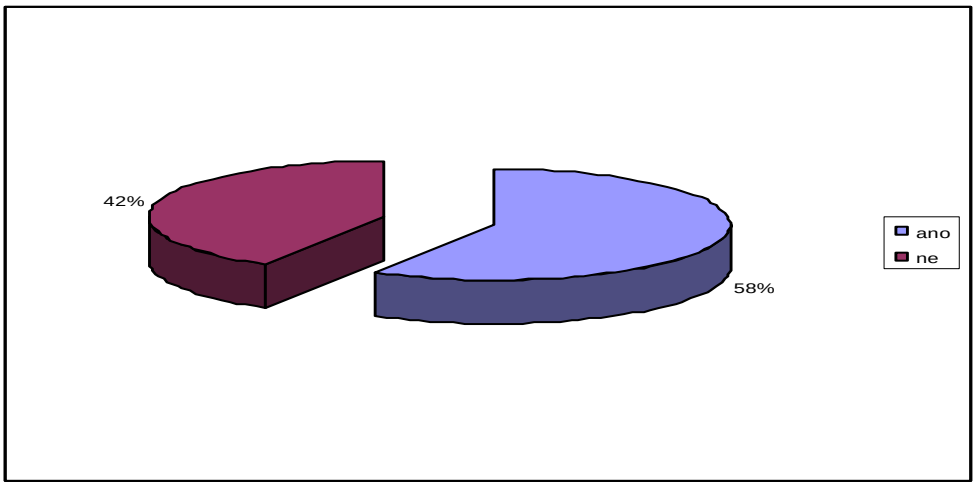
Jako nejúčinnější preventivní opatření se podle 19-ti respondentů (40 %) jeví nekomunikovat s neznámými lidmi a neposkytovat žádné osobní údaje. K tomu se přiklonilo 16 (33 %) dotázaných. Dále 6 (13 %) respondentů hlasovalo pro věkové omezení vstupu na sociální sítě, 4 (8 %) pro pravidelné přednášky na dané téma, 2 (4 %) navrhli spolupracovat s vysokými školami zaměřenými na tuto problematiku a jeden respondent (2 %) by navrhl internetovou cenzuru.



Graf 12 Nejúčinnější forma prevence [*vlastní zpracování*]

Otázka č. 15 – Znáte nějakou organizaci, která se zabývá kyberšikanou a její prevencí?

Celkem 28 tázaných (58 %) má povědomí o některé z organizací, které se kybernetické šikaně a prevencí před jejím výskytem zabývá. Oproti tomu 20 respondentů (42 %) o těchto institucích nic neví.



Graf 13 Znalost organizací, které se zabývají kyberšikanou [*vlastní zpracování*]

6.3.1 Shrnutí výstupů dotazníkového šetření

Formou dotazníkového šetření jsme zkoumali u skupiny tzv. teenagerů, jejich zkušenosti s kybernetickou šikanou. Zajímalo nás, zda se tato věková skupina někdy setkala s různými projevy a typy kyberšikany, jaký typ kyberšikany je podle jejich názoru nejrizikovější, jaké informace na sociálních sítích poskytují, zda ví na koho se s případnými problémy mají obrátit, jako formu prevence by navrhovali.

Z průzkumu vyplynulo že všichni z oslovené skupiny mají vytvořený nejméně jeden účet na sociálních sítích a tudíž ji aktivně používají ke komunikaci. Nejčastější údaj, který zveřejňují na svých profilech, je e-mailová adresa, což je mimo jiné i jedna z podmínek zřízení jakéhokoliv účtu na sociálních sítích, a osobní (soukromé) fotografie nebo videa. právě jejich sdílení je v současné době touto věkovou skupinou velmi preferované.

Těsná většina dotázaných se přiznala, že se s kyberšikanou v různých formách a typech již setkala, ať už v minulosti tak v současné době. Jako nejrizikovější typ uvedli kyberstalking. Důvod by mohl být ve větší medializaci a četnosti výskytu případů, které se v posledních letech dostali do povědomí veřejnosti. Kybegrooming, který je v odborných kruzích brán jako nejrizikovější neboť může mít nejzávažnější dopad ze všech typů, označilo jen velmi málo respondentů.

V případě nutnosti, by se většina respondentů obrátila na školu, a nebo na rodinu, což hodnotíme jako velmi dobře zvolenou strategii. Jen málo dotázaných by se obrátilo přímo na Policii ČR a nebo na jednu z tísňových linek.

Vcelku úspěšně si tazatelé vedli v otázce zda by výskyt kyberšikany nahlásili. Téměř všichni se přiklonili k odpovědi ano, zároveň by však chtěli zůstat v anonymitě. Otázkou zůstává, zda by věděli na koho konkrétního se ve škole, pokud se kyberšikana bude odehrávat tam obrátit, protože část z nich nemá tušení, kdo na jejich školách provádí prevenci před nebezpečnými jevy, včetně kyberšikany.

Jako nejčastější dopad byl v dotazníku uveden strach, který vzniká jako reakce na hrozící nebezpečí. Dalším dopadem v pořadí byla zvolena deprese. Sebevražda, tedy nejhorší dopad kyberšikany na jedince, byla uvedena v osmi případech.

Polovina všech dotazovaných je toho názoru, že proti kyberšikaně není účinná obrana. Jednou z možností jak jí předejít je podle názorů respondentů vyhnout se komunikaci s cizími lidmi, kteří pro nás mohou představovat riziko, a zároveň pečlivě zvažovat komu a jaké osobní údaje poskytneme.

7 VYHODNOCENÍ VYBRANÝCH RIZIK KYBERNETICKÉ ŠIKANY METODOU PNH

Problematika kybernetické šikany je z pohledu krizového řízení a tvorby analýzy rizik prozatím neprobádanou oblastí. V této části budou vyhodnocena daná vybraná rizika metodou PNH, která se jeví pro tuto problematiku nejvhodnější. Všechna níže zmíněná rizika velmi úzce souvisí s problematikou kybernetické šikany. Některá z nich byla popsána v části 5 této práce a byla i jednou ze součástí dotazníkového šetření.

V teoretické části jsme si danou metodu krátce specifikovali a v následující části bude použita pro naše konkrétní případy.

Tab. 5 Specifikace rizik [*vlastní zpracování, 10*]

Pravděpodobnost (P)	**Následky (N)**	**Názor hodnotitelů (H)**
Nahodilá	Téměř žádná újma	Zanedbatelný vliv na míru nebezpečí a ohrožení
Nepravděpodobná	Malá újma	Malý vliv na míru nebezpečí
Pravděpodobná	Větší újma	Větší, nezanedbatelný vliv
Velmi pravděpodobná	Vážná újma	Velký a významný vliv na míru ohrožení
Trvalá	Velmi vážná újma	Více významných a nepříznivých vlivů

Tab. 6 Metoda PNH vybraných rizik [*vlastní zpracování*]

Zdroj rizika (faktory)	**Identifikace**	**P**	**N**	**H**	**R**
Technický	Pokus o prolomení elektronického účtu	4	1	3	12
Technický	Prolomení elektronického účtu	3	4	5	60
Technický	Vytvoření falešného účtu na sociální síti	3	5	4	60
Technický	Zasílání osobních údajů (rodné číslo, bydliště, jméno a příjmení)	3	2	2	12

Technický	Zasílání soukromých fotografií a videosouborů	2	2	3	12
Technický	Zasílání materiálů o oběti s pornografickou tématikou	3	4	5	60
Technický	Napadání účastníků on-line komunikace	2	3	3	18
Psychický	Vydírání pomocí sociálních sítí	2	3	5	30
Technický	Pronásledování pomocí sociálních sítí	3	4	4	48
Psychický	Urážení, ponižování, ztrapňování na sociálních sítích	3	3	3	27
Psychický	Nabádání k sebepoškození	3	4	4	48

Z výsledků zjištěných pomocí metody PNH je patrné, že největším nebezpečím spojeným s kybernetickou šikanou a tedy rizikem, které patří do kategorie NEŽÁDOUCÍ jsou prolomení elektronického účtu, vytvoření falešného účtu oběti a šíření dětské pornografie.

U prvního případu může hrozit finanční ztráta, která může vyústit až k exekuci na majitele napadeného účtu. To platí pro případ, že se jedná o účet např. internetového bankovnictví.

V případě vytvoření falešného účtu na sociální síti může být oběť dlouhodobě vystavena pomlouvání, ztrapňování, šíření osobních fotografií nebo video souborů (často i se sexuální tematikou) apod. Následkem může být nehmotná újma jako např. psychické potíže. V závažnějších případech se oběť může pokusit o sebevraždu.

Zasílání převážně nevyžádaných pornografických materiálů po sociálních sítích je dalším problémem a potenciálním rizikem pro případnou oběť nebo oběti.

Na hranici rizika NEŽÁDOUCÍ je rovněž pronásledování prostřednictvím sociálních sítí a nabádání účastníků komunikace k sebepoškození.

8 NÁVRH ZLEPŠENÍ PREVENCE RIZIKA KYBERNETICKÉ ŠIKANY

V následující části se zaměříme na možnost snížení rizika kybernetické šikany a navrhneme možnosti zlepšení prevence před tímto jevem.

Navrhneme patřičná opatření pro naši sledovanou cílovou skupinu, která se dají aplikovat i pro ostatní uživatele sociálních sítí. Využijeme souhrn výsledků dotazníkového šetření a zároveň poznatků, které jsme získali analýzou samotného jevu kybernetické šikany a vlastní logickou úvahou, která pramení ze studia jednotlivých rizik z dostupných literárních a internetových zdrojů.

Za základní kámen pro omezení rizik považujeme nikoliv zkoumání technických prostředků a případných možností jejich omezování, pomocí kterých je kyberšikana realizována, ale jako cestu k eliminaci těchto problémů vidíme psychologické zkoumání chování člověka a to nejen v prostředí sociálních sítí, ale i v reálném životě. Dodržováním určitých pravidel bezpečnosti vycházejících ze znalostí těchto člověku přirozených zákonitostí chování, můžeme konkrétním projevům kyberšikany i předcházet.

Pro člověka je spíše přirozená důvěřivost, než její protipól a právě zde jsou většinou otevřena pomyslná vrátka pro kyberšikanu – velká část obětí se chovala v tomto prostředí důvěřivě. Pokud je nám důvěřivost přirozená, pokusme se být každý den alespoň trochu více obezřetnými a nedůvěřivými. Svět sociálních sítí na první pohled vypadá tak trochu jako jiný svět. Jeví se přátelsky, všichni jsou tam zdánliví přátelé („mám je v přátelích, mají mě v přátelích“). Co může ale pro tento reálný svět znamenat – kolik „přátel“ kdo na sociální síti má? Neměli bychom místo kvantitě virtuálních přátel, dát přednost spíše kvalitě těch reálných? Na druhou stranu to neznamená, že bychom prostředí sociálních sítí měli zcela zavrhnout. Přináší nám to i kladné stránky. A pak, „zdravě nedůvěřivý“ bude spíše ten, kdo prostředí zná a pohybuje se v něm, než ten, který od něj byl izolován a bude si chtít vše nové důvěřivě vyzkoušet.

K eliminaci rizik spojených s kybernetickou šikanou navrhujeme tři oblasti působení.

8.1 Primární prevence

Za primární oblast působení vůči rizikům, kterými se zabývá tato práce, považujeme rodinu. Z hlediska prevence je důležité především s dětmi a mládeží jakožto nejohroženější skupinou, otevřeně komunikovat nejen o těchto problémech, ale v prostředí rodiny s dětmi vůbec často mluvit, a to o různých tématech. Hlavním problémem dnešního uspěchaného světa je nedostatek času. Pochopitelně rovněž vysoká rozvodovost a z ní plynoucí stav, kdy se o dítě následně stará pouze jeden rodič, zlepšení situace nenapomáhá, právě naopak. Dítě se cítí odstrčeno, posunuto na druhou kolej, a tak se z reálného, pro něj toho horšího světa, obrací k tomu virtuálnímu. Je proto nutné udělat si čas na úkor jiných aktivit a věnovat jej ke společně strávenému volnu. Při komunikaci volit takovou strategii, aby se dítě rozpovídalo o svých problémech ve škole nebo ve svém okolí. Důležité je, aby si tedy případné problémy nenechávalo dítě pro sebe. Děti by se měli naučit mluvit o tom, co na internetu hledají, co je tam zajímá, kterou sociální síť používají. Měla by fungovat interakce ze strany rodičů. Jejich počínání na internetu a sociálních sítích by mělo být dítěti rovněž známo.

I když je to při dnešním nedostatku času těžké, lze tímto způsobem odhalit mnohé vznikající potíže již v samotném zárodku a tím jim předcházet. S dětmi a mládeží je nezbytné mluvit především o tom, jaké informace při komunikaci na síti nesmím ostatním uživatelům nikdy zasílat (osobní údaje a fotografie). Musí se naučit být všímavé nejen v užším slova smyslu, ale také ve vztahu k širšímu okolí, protože obětí může být i jeho kamarád nebo spolužák.

Za klíčové považujeme rozvrh volnočasových aktivit. Je čistě jen na dohodě rodiny a jejich potomků, jakým aktivitám (sportům, kulturním, výtvarným činnostem apod.) se ve volném čase děti chtějí a budou věnovat. Ze strany rodičů by měla následovat důkladná kontrola vykonávání této činnosti a nápomoc při řešení problémů s těmito aktivitami.

8.2 Sekundární prevence

Za neméně důležitou, ale ve vztahu k oblasti primární až následnou, považuji účast institutu školy na prevenci a řešení této problematiky.

Ze školského zákonu vyplývá povinnost školy co se týká bezpečnosti a ochrany zdraví jednotlivých žáků ve školských zařízeních. Samotné školy vypracovávají školní řády a vnitřní

řády školy, kterými upravují mimo jiné i problematiku ochrany před sociálně patologickými jevy. Metodik prevence předkládá údaje o preventivních opatřeních na příslušný školní rok.

Mezi nejčastější aktivity v rámci prevence patří např.:

- *adaptační kurzy,*
- *teamové aktivity,*
- *školní vzdělávací programy,*
- *zájmové vzdělávací programy,*
- *peer programy.*

V praxi však neexistuje jednotná metodika či systém výuky. Dosavadní stav, kdy si školy vytvářejí sami své vzdělávací programy určované rámcem vzdělávacího programu, na nárůst problémů reagovat nestačí. Tady je třeba reagovat pružněji.

Průběžně vzděláváni – učitelé všech typů škol by měli být vzděláváni v oblasti používání prostředků moderních komunikačních technologií, aby mohli kvalifikovaně své žáky a studenty o problematice informovat jak v oblasti prevence, tak v odhalování případů již započaté kyberšikany. Domníváme se, že metodicky by problematika měla být řešena centrálně tak, aby byl kladen důraz na kvalitní proškolování učitelů. Na každé škole by měl být kompetentní a důkladně proškolený poradce zabývající se touto problematikou, koordinující na škole činnost ostatních pedagogů v problematické oblasti. Tato osoba v podobě metodika prevence nebo psychologa v zařízeních sice je, ale omezený počet školení a stejně tak školení se zaměřením na větší množství jevů a rizik, je dle nás nedostačující v poměru s pokrokem v oblasti technologií i neustálého vzrůstajícího problému kybernetické šikany. Výuka by měla reflektovat pokrok moderních technologií a učitelé využívat možností nové techniky tak, aby svým působením na žáky a studenty, usměrňovali používání těchto prostředků pro žádoucí účely. Tento pracovník nebo pracovníci, či osoby určené k tomuto účelu, by měli být nadále vzdělávány nejen ve výše zmíněných technologiích, ale i v kooperaci se sdruženími zabývající se prevencí kybernetické šikany, k jejímu odhalování a postupům, které zaujmout v případě odhalení tohoto jevu.

Krizový scénář – každé školské zařízení by jej mělo mít vytvořený. Ten by měl detailně řešit dané postupy v případě odhalení a následném řešení problematiky.

Povědomí – hraje u studentů i jiných účastníků procesu kyberšikany velkou roli. V osnovách školy by měla být metodika, jak tomu napomáhat. Ze strany pedagogů by mělo být přistupováno k tomuto jevu se vší vážností. Pedagog by měl být svých chováním a jednáním vzorem.

Preventivní informační skupiny – povědomí by se dalo zvýšit založením preventivních a informačních skupin, které by v úzké spolupráci s vedením školy a odborníky na prevenci kyberšikany, šířili osvětu formou přednášek, letákovými akcemi i např. dny prevence, jak pro studenty, tak pro rodiče.

Šíření tištěných publikací – která by detailně popisovaly jednotlivá rizika v kybernetickém prostoru a byly by samozřejmě k dispozici všem v areálu školy, a to včetně návštěv a rodičů.

Návštěvy externích odborníků – kteří by se žáky obou stupňů povinných přednášek a následných diskuzí, řešily s účastníky jejich dotazy nejen veřejně, ale i individuálně a anonymně.

Výzkum – v podobě ankety nebo dotazníku. To je další způsob jak pružně reagovat na případný problém kyberšikany. Správně položené otevřené i uzavřené otázky mohou po analýze výsledků psychologem i odborníkem na kyberšikanu nastínit případnou problematiku.

Studenti vysokých škol – studující humanitní obory, nebo obory zaměřené na vyhledáváním rizik a prevencí před nimi. Pomocí peer programů by se tímto více a pružněji reagovalo na dané problémy. Tento systém by mohl být přínosem pro obě strany.

Schránky důvěry – sloužící k anonymnímu oznámení problémů s kyberšikanou. Tyto schránky by měli být umístěny tak, aby se skutečně zachovala anonymita oběti kybernetické nebo i klasické šikany. S údaji v těchto schránkách by mělo být zacházeno jako s interními, velmi citlivými materiály, které by se měli dále pomocí pedagogů a hlavně odborníků (nikoliv jen školních metodiků, ředitele, psychologa) rozklíčovat a následně zvolit správnou strategii k jejich řešení.

8.3 Terciární prevence

Zatímco dvě předešle navrhované oblasti se zejména týkaly prevence, terciární oblast by kromě preventivní funkce, měla svou působností z větší části pokrývat řešení již propuknuté kyberšikany. Měla by být tvořena institucemi a projekty specializujícími se na danou problematiku. Samozřejmostí je nezbytná účast Policie České republiky na všech těchto projektech.

Z exitujících projektů a institucí, které jsou veřejně prezentovány jmenujeme:

- *projekt E-Bezpečí,*
- *projekt E-Nebezpečí pro učitele,*
- *projekt Safeinternet,*
- *projekt Červené tlačítko,*
- *Centrum prevence rizikové virtuální komunikace Přírodovědecké fakulty univerzity Palackého v Olomouci ,*
- *Internet Helpline – (pomoc online – linka bezpečí online),*
- *Bílý kruh bezpečí,*
- *Národní centrum bezpečnějšího internetu a další.*

Problematiku by měli legislativně centrálně zastřešovat naši zákonodárci. Parlament České republiky by měl předkládat a schvalovat zákony v takovém znění, které bude nejen usnadňovat Policii České republiky práci při řešení závažných případů, v nichž je ohrožen lidský život, ale především pružně reagující na nové hrozby.

Pouze dobrou spoluprací všech tří výše zmíněných složek, lze dosáhnout uspokojivých výsledků na poli prevence i potírání společensky nebezpečných dopadů kyberšikany.

A konečně – spolupráce by neměla být ohraničena pouze hranicemi České republiky. Jestliže je internet globální sítí bez hranic, tyto problémy mají jednoznačně ráz globálního charakteru a překračují legislativu jednotlivých států. Jen neustálým dialogem mezi státy lze o problematice shromažďovat nové poznatky napříč zeměmi a získávat tak nové zkušenosti z mnoha konkrétních případů, které se staly v různých koutech světa.

ZÁVĚR

Jak jsme už v úvodu předeslali, tato práce zdaleka neobsáhla všechna rizika kybernetické šikany. Nebyl to ale cíl práce. Rizika kyberšikany na sociálních sítích jsou skutečně velkou množinou pro pravděpodobnost vzniku patologických jevů.

Cílem naší práce bylo obeznámit se s kybernetickou šikanou jako s nejčastějším jevem na sociálních sítích, které jsou v neustálém rozmachu. K naplnění tohoto cíle jsme použili dostupné literární i internetové zdroje.

Stejně tak jsme si dali za cíl zjistit u námi vybrané skupiny respondentů povědomí o tomto riziku, o jejich druzích a znalostech preventivních opatření. K dosažení tohoto cíle bylo využito dotazníkové šetření.

Z tohoto šetření byly zjištěny i nedostatky ve znalosti dotazované skupiny v oblasti prevence. Proto považujeme informovanost a povědomí o problému za klíčový prvek.

Na základě zjištěných skutečností i formou úvahy bylo navrženo řešení ke zlepšení prevence jak pro naši referenční skupinu, která byla předmětem dotazníkového šetření, tak pro další účastníky z řad uživatelů sociálních sítí, převážně z kategorie dětí a mládeže.

Navrhnuli jsme řešení tohoto problému jak v prostoru domova, tedy v rodině, tak zároveň zavedení a zintenzivnění prevence kybernetické šikany na všech stupních škol. Výstupy této práce by mohli sloužit kromě dotazované skupiny také ostatním studentům, ředitelům, metodikům prevence na základních a středních školách a v neposlední řadě široké veřejnosti, která by se chtěla o této problematice něco dovědět. Práce by jim měla pomoci se zorientovat v dané problematice.

Přestože jsou školy a hlavně většina studentů v nich dobře obeznámeni s problematikou kybernetické šikany, není dle našeho názoru tomuto problému ve školních vzdělávacích programech věnována taková pozornost, jakou by si zasloužila.

Primárně navrhujeme zaměřit se více na odborníky, kteří s tímto problémem pracují denně a jsou tedy vysoce specializovaní v daném oboru, mají možnost sledovat nové „trendy“ a zároveň analyzují probíhající případy útoků v praxi.

Zjištěním a posouzením aktuálního stavu kybernetické šikany můžeme konstatovat, že ještě stále vidíme možnosti a cesty, jak s touto problematikou obeznámit co nejširší veřejnost a s její aktivní pomocí se pokusit zabránit jejímu neustálému rozšiřování.

SOUHRN BAKALÁŘSKÉ PRÁCE

Tato bakalářská práce se věnuje problematice kybernetické šikany a rizik s ní spojených.

V teoretické části jsme se v malé míře věnovali komunikaci, která úzce souvisí s pohybem na sociálních sítích, chatech, diskuzích apod. Součástí kapitoly je i on-line komunikace a její prostředky. Dále jsme si stručně popsali dvě z několika sociálních sítí. První z nich byl Facebook, tedy v současné době nejpoužívanější sociální síť pro věkovou skupinu (obr.4), jejichž část je součástí našeho dotazníkového šetření. Druhou sítí je multimediální YouTube, kde se kumulují mimo jiné videa či fotografie s tématikou této práce. Poslední kapitolou bylo seznámení se základními pojmy analýzy rizik, cílem práce a její metodikou.

Praktická část se již zabývá samotnou problematikou kybernetické šikany. Popisujeme v ní její specifika, druhy, projevy, pachatele, oběti, dopady a stav k roku 2012, kdy byly prezentovány poslední výsledky výzkumu Univerzity Palackého v Olomouci.

V další části jsme krátce popsali druhy kyberšikany jako jsou kybergrorming, kybersexting, happy slapping, outing a zmínili se i o syndromu FOMO, tedy závislosti na sociálních sítích.

Důležitou částí práce je dotazníkové šetření, které mapovalo problematiku spojenou s kyberšikanou u tzv. teenagerů, tedy ve věkovém rozpětí 15–20 let. Zajímalo nás zda se s ní setkali, v jaké formě, zda vědí kam se obrátit v případě, kdy se stanou obětí, pachateli nebo pozorovateli. Zároveň nás zajímalo jakou formu prevence by zvolili. Nedílnou součásti je i popis a vyhodnocení dotazníku.

Jako metodu analýzy rizik jsme použili metodu PNH. Pomocí této metody jsme určili míru rizika u vybraných nebezpečí spojených s kyberšikanou. Do tabulkového zpracování a výpočtů jsem zahrnuli jak vybraná rizika z páté kapitoly, tak i některá další která mohou vážně ohrozit uživatele sociálních sítí.

Poslední částí práce bylo navržení zlepšení preventivních opatření nejen pro námi sledovanou skupinu, ale prakticky i pro ostatní účastníky komunikace na sociálních sítích a zájemce o prevenci před tímto nebezpečím.

SEZNAM POUŽITÉ LITERATURY

[1] DEVITO, Joseph A. *Základy mezilidské komunikace*. Praha: Grada Publishing, 2001. 420 s. ISBN 80-7169-988-8

[2] KONEČNÁ, Zdeňka. *Základy komunikace*. Brno: Nakladatelství CERM, 2009. 151 s. ISBN 97880-214-3891-0

[3] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace, příručka pro učitele a rodiče*. Olomouc: NET University, 2010. 34 s. ISBN 978-80-254-7866-0

[4] KOPECKÝ, Kamil. *Kybergrooming, nebezpečí kyberprostoru*. Olomouc: NET University, 2010. 16 s. ISBN 978-80-254-7573-7

[5] KOPECKÝ, Kamil. *Stalking a kyberstalking, nebezpečné pronásledování*. Olomouc: NET University, 2010. 14 s. ISBN 978-80-254-7737-3

[6] MIKULÁŠTÍK, Milan. *Komunikační dovednosti v praxi*. 2., dopl. a přeprac. vyd. Praha: Grada Publishing. 2010. 325 s. ISBN 978-80-2339-6

[7] MIKULÁŠTÍK, Milan. *Komunikační dovednosti v praxi*. Praha: Grada Publishing, 2003. 361 s. ISBN 80-247-0650-4

[8] PAVLÍČEK, Antonín. *Nová média a sociální sítě*. Praha: Oeconomica, 2010. 181 s. ISBN 978-80-245-1742-1

[9] SZOTKOWSKI, René, Kamil KOPECKÝ a Veronika KREJČÍ. *Nebezpečí internetové komunikace IV*. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2013. 177 s. ISBN 978-80-244-3911-2

[10] ŠEFČÍK, Vladimír. *Analýza rizik*. 1. vyd. Zlín: Univerzita Tomáše Bati, 2009. 98 s. ISBN 978-80-7318-696-8.

[11] TICHÝ, Milík. *Ovládání rizika, analýza a management*. 1.vyd. Praha: C.H.Beck, 2006. 396 s. ISBN 80-7179-415-5

SEZNAM INTERNETOVÝCH ZDROJŮ

[12] BARVÍNKOVÁ, Marie. *Proč mě nikdo nemá rád? Deprese ze sociálních sítí mají svůj název*. In: Idnes.cz [online] ©1999-2014, 11.9.2013 [cit.2014-01-20] Dostupný z: <http://ona.idnes.cz/socialni-site-zpusobuji-syndrom-fomo-d8l-/vztahy-sex.aspx?c=A130910_143608_vztahy-sex_brv>

[13] BENEŠOVÁ, Jana. *Stalking: dejte si pozor*. In: BKB.CZ [online] časopis LOOK, srpen 2008 ©Bílý kruh bezpečí, o.s. [cit. 2014-02-01] Dostupný z: <http://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/>

[14] BEZPEČNÝ INTERNET. *On-line komunikace*. [online] ©2000-2010 [cit. 2013-09-06] Dostupný z: <http://www.bezpecnyinternet.cz/zacatecnik/on-line-komunikace/default.aspx>

[15] BKB. *Nebezpečné pronásledování*. [online] ©Bílý kruh bezpečí, o.s. [cit. 2014-02-01] Dostupný z: <http://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/>

[16] CENTRUM. *Youtube*. Aktuálně.cz [online] ©199902014 [cit. 2013-10-06] Dostupný z: <http://wiki.aktualne.centrum.cz/youtube/>

[17] ČESKÁ TELEVIZE. *Počet aktivních uživatelů Facebook překonal miliardu*. [online] ©1996-2014, 4.10.2012 [cit. 2013-09-06] Dostupný z: <http://www.ceskatelevize.cz/ct24/media-it/198374-pocet-aktivnich-uzivatelu facebooku-prekonal-miliardu/>

[18] E – BEZPEČÍ. *Happy slapping*. [online] ©2010 [cit. 2014-02-01] Dostupný z: <http://cms.e-bezpeci.cz/content/view/71/39/lang,czech>

[19] MAREK, Tomáš. *Studie: věk uživatelů sociální sítě.* In: Inflow.cz [online] ©2007-2013, 22.2.2010 [cit. 2014-02-01] Dostupné z: <http://www.inflow.cz/studie-vek-uzivatelu-socialnich-siti>

[20] MULLEN, E. Paul a kol. *The management of stalkers*. Advanced in Psychiatric Treatment, 2001. [online] ©2014 [cit. 2014-02-01] DOI: 10.1192/apt.7.5.335. Dostupný z: <http://apt.rcpsych.org/content/7/5/335.full>

[21] OBJEVIT. *Sociální sítě – pohled do historie*. [online] ©2010-2013, 5.3.2013 [cit. 2014-01-20] Dostupné z: <http://objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280>

[22] PAULÍK, Karel. *Psychologické základy lidské komunikace*. elektronický učební text ,Ostrava: Fakulta strojní VŠB – TU Ostrava. 2007. 95 s. Fakulta strojní VŠB. [online] Dostupný z: <http://projekty.fs.vsb.cz/415/psychologicke-zaklady-lidske-komunikace.pdf>

[23] PLATKO, Ondřej. *Sociální sítě 1. díl.* In: Owebu.cz [online] ©2014, 29.6.2009 [cit. 2014-02-01] Dostupný z: <http://owebu.bloger.cz/Internet/Socialni-site-1-dil>

[24] PRO VÁŠ BYZNYS. Youtube. [online] [cit. 2014-02-01] Dostupné z: <http://www.provasbyznys.cz/youtube>

[25] PSYCHICKÉ OBTĚŽOVÁNÍ. *Kyberšikana.* [online] ©2010-2013 [cit. 2014-02-01] Dostupné z: <http://psychickeobtezovani.webnode.cz/news/kybersikana/>

[26] RVP, metodický portál: *Kybergrooming.* [online]. [cit. 2014-01-19]. Dostupné z: <http://wiki.rvp.cz/Knihovna/1.Pedagogick%C3%BD_lexikon/K/Kybergrooming>

[27] STOP cyberbullying: *Types of cyberbullies.* [online]. [cit. 2014-01-20]. Dostupné z: <http://stopcyberbullying.org/parents/howdoyouhandleacyberbully.html>

[28] WEBER, M. Gregory, *Grooming children for sexual molestation.* In: Vachss.com. [online] ©1996-2014, [cit. 2014-01-19] Dostupné z: <http://www.vachss.com/guest_dispatches/grooming.html>

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Analýza rizika kybernetické šikany

Dobrý den,

studuji třetím rokem Fakultu logistiky a krizového řízení v Uherském Hradišti. Věnujte prosím několik minut svého času vyplnění následujícího dotazníku, pro praktickou část mé bakalářské práce na téma Analýza rizika kybernetické šikany. Prosím o vyplnění dotazníku skupinou respondentů ve věkovém rozmezí 15-20 let.

Dotazník bude použit jen pro výše zmíněný účel, proto prosím o co nejobjektivnější a pravdivá data.

Děkuji

Radek Slovák

1. Váš věk?

2. Vaše pohlaví?

○ muž ○ žena

3. Používáte ke komunikaci některou ze sociálních sítí?

○ ano ○ ne

4. Jaké informace osobního charakteru na nich nejčastěji zveřejňujete?

○ rodné číslo ○ telefonní číslo ○ e-mailovou adresu ○ soukromé foto nebo video ○ adresu bydliště

○ informace o přátelích ○ informace o Vašem pohybu ○ žádné

○ Jiná

5. Setkali jste se na sociálních sítích (Facebook, YouTube) s projevy kyberšikany?

○ ano ○ ne

PŘÍLOHA P I: DOTAZNÍK

6. Stali jste se někdy obětí, pachatelem nebo svědkem kybernetické šikany?

○ ano ○ ne

7. Pokud jste odpověděl(a) v otázce č.5 ano, tak kterého druhu kyberšikany se to týkalo?

○ kyberšikana (obtěžování, ponižování, verbální útoky, zesměšnění atd.)
○ kybergrooming (manipulace k osobní schůzce, zneužití)
○ kybersexting (rozesílání foto, video se sexuální tematikou oběti na sociální.síti)
○ kyberstalking (pronásledování pomocí internetu nebo mobilu)

8. Který z výše jmenovaných druhů, je dle Vás nejnebezpečnější?

[ ]

9. Jaký dopad může mít podle Vás některý z druhů kyberšikany

○ strach ○ stres ○ úzkost ○ porucha spánku ○ deprese ○ ztráta soukromí
○ sebevražda ○ žádné
○ Jiná [ ]

10. Víte, kdo provádí na Vaší škole prevenci před nebezpečnými jevy (šikana, kyberšikana, atd.)?

○ ano
○ ne

11. Oznámili byste událost spojenou s kyberšikanou na Vaší škole?

○ ano ○ ne

12. Na koho byste se s problémem spojeným s kyberšikanou obrátili nejdříve?

[ ]

13. Myslíte si, že se dá vzniku kyberšikany předejít?

○ ano ○ ne ○ nevím

PŘÍLOHA P I: DOTAZNÍK

14. Jaká forma prevence by podle Vás byla nejúčinnější?

- ○ cenzura internetu
- ○ věkové omezení zakládání profilu na sociálních sítích
- ○ pravidelné přednášky odborníků
- ○ spolupráce se studenty VŠ zaměřených na tuto problematiku
- ○ nekomunikovat s neznámými lidmi
- ○ neposkytovat osobní údaje
- ○ Jiná [ ]

15. Znáte nějakou organizaci, která se zabývá kyberšikanou a její prevencí?

○ ano ○ ne