Internetová bezpečnost

Alice Nezhybová

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Alice Nezhybová**
Osobní číslo:	**L18461**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Internetová bezpečnost**

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k dané problematice s důrazem na monografie a analytické materiály.
2. Seznamte se s jednotlivými typy kyberšikany.
3. Proveďte dotazníkový průzkum v oblasti kyberšikany.
4. Zpracujte výukový materiál podporující internetovou bezpečnost v oblasti kyberšikany.

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

Seznam doporučené literatury:

1. CLAYPOOLE, Ted a Theresa PAYTON. *Protecting your internet identity: are you naked online?*. Updated edition. Lanham: Rowman & Littlefield, [2017], ix, 277 s. ISBN 9781442265394.
2. KOVÁŘOVÁ, Pavla. *Informační bezpečnost žáků základních škol: lekce v knihovnách*. Brno: Filozofická fakulta, Masarykova univerzita, 2019, 261 s. Opera Facultatis philosophicae Universitatis Masarykianae. ISBN 9788021092709.
3. ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014, 183 s. Psyché. ISBN 9788021075276. Dostupné také z: http://www.grada.cz/deti-a-dospivajici-online_7905/kniha/katalog/.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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 právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- 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);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 27.7.2021

Jméno a příjmení studenta: Alice Nezhybová

…….
podpis studenta

ABSTRAKT

Bakalářská práce na téma Internetová bezpečnost se dělí na dvě části, teoretickou a praktickou. Začátek teoretické části je věnován sociálním sítím. Jedná se především o vysvětlení, jakým způsobem se vyvíjely sociální sítě v historii, dále co znamená mít profil na těchto sítích a jaké typy uživatelů zde můžeme najít. Další kapitola se věnuje druhům sociálních sítí. V poslední kapitole teoretické části lze najít informace o kyberšikaně. Jedná se především o vysvětlení historického kontextu, určení druhů kyberšikany a definice druhů kyberšikany. V praktické části se práce věnuje analýze vztahu dětí k problematice kyberšikany, a to prostřednictvím dotazníkového šetření. Dále je v práci provedeno multikriteriální hodnocení pro výběr nejnebezpečnějšího prostředku komunikace z hlediska zneužití kyberšikany. Po vyhodnocení je v poslední kapitole navrženo opatření a vytvořen elektronický výukový materiál.

Klíčová slova: agresor, bezpečnost, kyberšikana, oběť, sociální síť

ABSTRACT

The bachelor thesis has the topic Internet security is divided into two parts, theoretical and practical. The beginning of the theoretical part is devoted to social networks. It is mainly an explanation of how social networks have evolved in history, then means of having a profile on these networks and what types of users can be found here. The next chapter deals with the types of social networks. In the third and last part of the theoretical part you can find information about cyberbullying. It is mainly an explanation of the historical context, the identification of types of cyberbullying and the definition of types of cyberbullying. In the practical part, the work deals with the analysis of the relationship of children to the issue of cyberbullying, through a questionnaire survey. Furthermore, a multicriteria evaluation is performed for the selection of the most dangerous means of communication in terms of abuse of cyberbullying. After the evaluation, an electronic teaching material is designed and created in the last chapter.

Keywords: aggressor, cyberbullying, security, social network, victim

Děkuji Ing. Petru Svobodovi Ph.D. za pomoc při vedení bakalářské práce. Mé poděkování patří též těm, kteří v rámci dotazníkového šetření odpověděli na otázky. V neposlední řadě děkuji rodině a všem svým přátelům, kteří mě podporovali po celou dobu studia.

„Osud nám nemůže vzít nic z toho, co by nám dříve nedal.“

Seneca

OBSAH

ÚVOD

Kyberšikana je v dnešní době především v kruhu mladých lidí velice zmiňovaným pojmem. Většina dětí je na tento způsob agrese upozorněna již v mladém věku, například ve škole, od rodičů, či se o něm dozví přímo z internetu. Naštěstí v dnešní době existuje už mnoho filmů, seriálů a knih zabývajících se touto problematikou, a tak díky nim děti mohou zjistit základní informace o tom, jak se jí bránit. I přesto se často dnešní děti pohybující se ve světě sociálních sítí mohou dostat pod kontrolu agresora, využívajícího k dosažení svého cíle právě zmíněnou kyberšikanu. Takovýto agresor tedy využívá počítače, informační a komunikační technologie k ublížení druhému. Může se jednat například o vydírání, ztrapňování, ubližování, ohrožování, zastrašování a podobně.

Setká-li se někdo s kyberšikanou, je možné, že se ocitne v různých rolích. Mezi tyto role patří agresor, přihlížející a oběť. Každá role potřebuje svým způsobem pomoc. Agresorům by bylo potřeba vysvětlit, jaké následky může mít jejich chování. Obětem by bylo potřeba pomoci především v boji proti agresorům, a hlavně s následným vyrovnáním se s danou situací. Přihlížející by zase potřebovali především dostat motivaci a odvahu pro nahlášení a řešení případu kyberšikany, které byli svědky. Zvýšení povědomí o této problematice je tedy velice nutné, už jen kvůli skutečnosti, jaké následky může mít působení kyberšikany na oběti. O to více je potřeba tuto problematiku řešit, jelikož jsou obětmi často děti, které jsou na své soukromí velice citlivé a jeho narušení by mohlo v jejich budoucím životě způsobit velké psychické problémy.

I. TEORETICKÁ ČÁST

1 SOCIÁLNÍ SÍTĚ

Nejoblíbenějším prostředkem komunikace 21. století jsou právě sociální sítě na internetu. Tyto sítě mnohdy sdružují jednotlivce, kteří poté vytvářejí nestejnorodé specifické skupiny. Ačkoliv takovéto skupiny mají možnost vytvářet se na různých místech, např. ve školách či na univerzitách, poslední dobou se jejich nejoblíbenějším místem vzniku stal internet.

Objasnění této popularity může být takové, že na rozdíl od většiny obyčejných míst, kde počínají sociální sítě, internet poskytuje neomezené sdružování milionů jednotlivců z celého světa. Ti se touží poznávat, setkávat, navazovat přátelství či intimní vztahy, profesionální spojenectví, hromadit a sdílet informace, vyměňovat si znalosti týkající se například filmů, seriálů, hudby, sportu a podobně. Témata a zájmy těchto sítí jsou tak hojné a rozmanité, jak jen si to naše mysl dokáže představit.

V on-line prostředí využívají sociální sítě pro svoje potřeby možnosti webových stránek. Takové webové stránky pak označujeme jako sociální weby. Ty fungují především jako určité on-line komunity uživatelů internetu. Komunity mají možnost uživatele se společnými zájmy, náboženstvím nebo třeba politickými názory sdružovat.

Prezentování jednotlivců, vytváření svých vlastních sociálních sítí a udržování kontaktu s ostatními uživateli umožňují sociální sítě, jako je Facebook, Instagram, MySpace nebo Twitter. Velice časté jsou v dnešní době sítě, díky kterým mohou uživatelé těchto sítí nalézt nové partnery, ale zároveň mohou mít i pracovní povahu, kdy dochází ke shromažďování lidí ze stejného pracovního prostředí (Bednář, 2011; Hulanová, 2012).

1.1 Historie sociálních sítí

V roce 1954 byl poprvé použit termín „Sociální síť“. Přesně jej definoval sociolog a profesor londýnské ekonomické univerzity Jameson Barnes, který se zabýval zkoumáním sociálních vztahů mezi norskými rybáři. Svým výzkumem dospěl k takovému závěru, že veškerá společnost tvoří jakousi síť vztahů, které jsou vzájemně propojeny, tzv. sociální síť. S polovinou 90. let je spojován vznik sociálních sítí nebo spíše jeho náznak, kdy převládal velký rozmach univerzitních studentů, kteří se pustili do vytváření programů sloužících pro komunikaci v okruhu školy, ale i s rodinou. Jednalo se o neveliké a neznámé sociální sítě, jež fungovali v omezeném okruhu skupiny lidí. V roce 1997 vnikla první a zároveň průlomová sociální síť, kterou byla aplikace SixDegrees.com. Umožňovala svým uživatelům vytvořit si profilový účet, pomocí kterého komunikovali s ostatními uživateli

a prohlíželi si ostatní profily. I když tato aplikace zaujala spoustu lidí, tak se později stala finančně prodělečná a v roce 2001 byla zrušena. Následující sociální sítí byla seznamka Friendster.com, kterou založil v roce 2002 inženýr, podnikatel a investor Jonathan Abrams. Z počátku si seznamka vedla dobře, avšak později začala upadat a v roce 2009 ji odkoupila asijská firma Mol Global za 26,5 miliónů dolarů. Nyní už nefunguje jako seznamka, ale jako skupina, ve které se potkávají hráči počítačových her a komunikují mezi sebou navzájem. Další průlomové sociální sítě jsou blíže uvedeny v následující kapitole (Sociální sítě a jejich vývoj – pohled do historie, 2013).

1.2 Profil na sociálních sítích

Sociální sítě dávají možnost zformovat vlastní profil, který ve většině případů bývá spojován s off-line identitou uživatele. Toto propojení může být více či méně zřetelné:

a) konkrétně patrné díky zveřejnění jména, fotografie a dalších identifikačních údajů,

b) spíše nepřímé, je-li uživatel ztotožněn dle osobitých publikovatelných materiálů (např. zájmy, zkušenosti) či na základě viditelných okruhů přátel.

Profil je vytvářen neustálou aktivitou uživatelů, kteří mají do značné míry kontrolu nad jeho podobou. Jedinci na něj vkládají většinu materiálů a informací, které vidí ostatní uživatelé internetu. Mohou rovněž používat více možných funkcí aplikace, např. dávat takzvané „lajky“, přidávat komentáře, sdílet příspěvky nebo měnit statusy. Profil znázorňuje dobrou možnost pro kontrolovanou sebeprezentaci neboli proces, kterým subjekt usiluje o kontrolování dojmu, jaký si o něm vytvářejí jiní. Přesto je v anonymních on-line prostředích kontrola vyšší než tato, například jako je anonymní chat, a proto zde nemáme velkou šanci rozpoznat, jak se uživatel projevuje v jiných prostředích. U adolescentů je často vyšší tendence k experimentům s on-line identitou, napříč tomu je u nich sebereprezentace na sociálních sítích poměrně realistická. Na sociálních sítích většinou nezveřejňují falešné fotografie, neuvádějí zde klamné historky či zkušenosti a nepředstírají, že jsou kupříkladu jiného pohlaví. Nicméně se uživatelé na sociálních sítí snaží vylepšit. Nejedná se o výrazné změny, ale o úsilí vypadat dobře, avšak stále autenticky. Uživatelé například raději publikují více pozitivních informací než těch negativních. V tomto procesu se dospívající často snaží řídit dle reakcí druhých, především významných a slavných osobností (Ševčíková et al., 2014).

1.3 Typy uživatelů sociálních sítí

Vyskytuje se řada typologií pro označení typů uživatelů na sociálních sítích. Jako hlavní byla vybrána typologie dle Vojtěcha Bednáře, která jako jediná dělí uživatele podrobněji do dvou skupin. Uživatele člení na aktivní a pasivní, na základě druhu činnosti, kterou praktikují na sociálních sítí. Současně skupinu aktivních uživatelů rozčlenil na aktivní tvůrce a poskytovatele obsahu a na aktivní hodnotiče a distributory obsahu. Rovněž tak rozvrhnul pasivní uživatele na hodnotitele obsahu, pozorující autoritu a pozorovatele. Podstatnou informací je, že právě uživatelé tvoří veškerý obsah na sociálních sítích jakoukoliv svojí činností, ať už aktivní nebo pasivní (Kovářová, 2019).

Následující popsané typologie byly vybrány dle dalších kritérií. Pojednává o typologiích, které vytvořili odborníci zabývající se danou problematikou, nebo o typologie známých výzkumných agentur (Bednář, 2011).

1.3.1 Typologie podle Vojtěcha Bednáře

Aktivní typologie

- aktivní uživatel – tvůrce a poskytovatel obsahu

Tito uživatelé tvoří celkový základ všech sociálních sítí. Publikovaným obsahem vzbudí zájem u ostatních uživatelů, pro které má daný obsah určitý smysl či hodnotu a bývá šířen dál. Ačkoli je jejich počet nízký, tvoří velice důležitou skupinu uživatelů pro existenci sociálních sítí.

- aktivní uživatel – hodnotič a distributor

Díky této skupině dochází k šíření obsahu. S radostí projevují svůj zájem o diskuse a hodnocení obsahu na sociálních sítích, zároveň se z nich mohou stát i tvůrci, jelikož se při sdílení cizích příspěvků do jisté míry realizují.

Pasivní typologie

- pasivní uživatel – hodnotič obsahu

Je velmi komplikované rozpoznat takové uživatele a zároveň obtížné je něčím zaujmout. Netvoří žádný obsah na sociálních sítích a nezapojují se do diskusí. Jediným typickým

příkladem pro tuto pasivní skupinu je tlačítko „Like“, kterým projeví, že se jim příspěvek líbí, čímž současně přispívají k šíření informací.

- pasivní uživatel – pozorující autorita

S těmito uživateli se tak často na sociálních sítích nepotkáváme. I když jsou pasivní, tak mají velký vliv, ale pouze když sdílí a hodnotí. Jedná se o tzv. sběratele virtuálních kontaktů, mají mnoho přátel, ale i přesto poněkud málo komunikují, diskutují a hodnotí. Jestliže si získáme tyto uživatele, mohou pro nás znamenat cenný zdroj informací a také nám pomohou je šířit.

- pasivní uživatel – pozorovatel

Takové pozorovatele můžeme nazvat i jako prohlížeče či čtenáře. Nezapojují se do komunikace, nechtějí sdílet ani komentovat, a když už se zapojí do virtuální diskuse, tak většinou negativně. Na apely k aktivitě vůbec nereagují. Pro tuto skupinu jsou sociální sítě nutností, nikoliv zábavou, a především je využívají ke své práci (Bednář, 2011).

1.3.2 Typologie podle americké výzkumné agentury Forrester Research

Nejdříve tato typologie byla použita na knižní sociální sítě. Většinu těchto uživatelů nelze řadit do jedné skupiny, protože mezi nimi často přecházejí. Charakteristický předpoklad pro jejich aktivitu je obvykle přečtení určitého počtu knih, ke kterým mají možnost se vyjadřovat, komentovat a hodnotit je.

Tvůrci (creators) – aktivně tvoří a zveřejňují blogy, webové stránky, hudbu i videa, píší a publikují články často i na webech jiných lidí.

Kritici (critics) – vyjadřují se k příspěvkům ostatních, editují články, zveřejňují recenze a hodnocení produktu či služeb a přispívají do on-line fór.

Vypravěči (converstationalists) – nejméně jednou týdně zveřejňují a pečují o své statusy na sociálních sítích.

Sběratelé (collectors) – obvykle využívají RSS (Rich Site Summary), označují jimi fotografie nebo webové stránky, případně se účastní hlasování o popularitu stránek.

Účastníci (joiners) – pravidelně navštěvují a udržují si své profily a blogy.

Diváci (spectators) – hodnotí pomocí bodového systému, poslouchají podcasty, pročítají blogy a dívají se na videa.

Neaktivní (inactives) – nevyužívají a nezajímají je sociální sítě, nebo o nich vůbec nic nevědí (Global social media adoption in 2011, 2012; Dočekal, 2012).

1.3.3 Typologie společnosti TNS Digital Life

Tato jedna z největších celosvětových výzkumných agentur zkoumá chování uživatelů na sociálních sítích a následně je dělí do šesti skupin.

Ovlivňovatelé (influencers) – jsou na internetu neustále, připojují se kdekoliv a kdykoliv, nejčastěji přes mobilní telefon. Díky své intenzivní aktivitě na síti mají velký vliv.

Komunikátoři (communicators) – nevyjadřují se pouze za sebe, ale také často vstupují do diskusí vyvolaných jinými uživateli. Řadí se mezi nejaktivnější účastníky diskusních skupin.

Hledači znalostí (knowledge-seekers) – jejich prioritou je hledání a získávání informací pro vlastní užití. Nikde se nepřihlašují ani neregistrují, používají pouze základní funkce stránek. I když mají rádi nové věci, sociální sítě je nezaujaly.

Síťovači (networkers) – s ostatními komunikují přes internet, což jim nahrazuje klasické mezilidské vztahy. Rádi vstupují do interakcí s ostatním, ale neradi prezentují své vlastní názory.

Uchazeči (aspirers) – nováčci v užívání internetu a sociálních sítí, kteří se v průběhu mohou stát i jiným typem uživatele.

Praktici (functionals) – tvrdí, že je sociální sítě vůbec nezajímají, mají strach o bezpečnost svých dat a raději používají emaily. Často mluvíme o starších uživatelích, kteří jsou především čtenáři a sledují zpravodajství. Na sítích se nevyjadřují (Tůmová, 2012).

2 DRUHY SOCIÁLNÍCH SÍTÍ

Vytváří se stále více a více internetových stránek, přes které se scházejí lidé z celého světa, proto jsou sociální sítě opravdovým fenoménem dnešní doby. Společně tak sdílejí své zážitky, posílají videa, vyměňují si kontakty a hrají spolu hry. Seznam těchto možných aktivit je opravdu velmi rozsáhlý (Teenageři a komunikace na internetu, 2020).

2.1 Osobní sociální sítě

Slouží především ke komunikaci, udržení kontaktu a sdílení významných momentů s přáteli. Nejpodstatnější je zde uživatel a vše kolem něj. Tyto sítě zdůrazňují aktuálnost (Dobosiová, 2015).

Facebook – nejpoužívanější sociální síť na světě založena Markem Zuckerbergem v roce 2004. Uživatelé na svém profilu sdílí fotky, příspěvky či videa. Jednou ze zajímavostí je, že zde uživatelé nahrají v průměru 200 miliónů fotek za den (Přehled sociálních sítí 2019, 2019).

Instagram – jedna z nejoblíbenějších sociálních sítí, která nabízí zveřejňování fotografií a videosekvencí. Uživatelé svůj obsah označují „hashtagy“, které ostatním usnadňují vyhledávání obdobných témat (Kožíšek a Písecký, 2016).

Snapchat – aplikace, kde si lidé mezi sebou posílají fotky a sdílejí videa, která automaticky nebo po určitém čase zmizí po zhlédnutí (Sociální sítě, 2020).

Foursquare – síť, která sdílí polohy prostřednictvím chytrých telefonů, kde pomocí této aplikace označí uživatelé svou polohu na určitém místě. Dále mají možnost toto označení komentovat, přidat poznámku či fotografii (Sociální sítě, 2013).

Myspace – umožňuje vytvořit si vlastní internetový profil, na kterém si uživatelé ukládají a sdílejí multimédia (MySpace, 2021; Hulanová, 2012).

2.2 Sítě zaměřené na sdílení obsahu

Tato kategorie zahrnuje kombinaci osobního, uměleckého a profesního obsahu. Hlavní roli zde hraje pouze obsah na sociálních sítích (Dobosiová, 2015).

Twitter – poskytuje uživatelům možnost psát krátké zprávy, tzv. tweety o maximální délce 140 znaků. Objevují se zde čerstvé informace, neboť tuto síť používá spousta médií, odborníků a známých osobností (Kožíšek a Písecký, 2016).

Pinterest – platforma, která má schopnost rychle najít inspirace a informace z různých kategorií (Přehled sociálních sítí 2019, 2019).

YouTube – největší videoslužba na světě, která má denně přes dvě miliardy přístupů. Umožňuje nahrání a přehrávání videí, komentování nebo vytváření playlistů (Kožíšek a Písecký, 2016).

Tik Tok – poměrně mladá sociální síť, na které uživatelé tvoří krátká videa, které pak kdokoli sdílí na další sociální sítě, komentují a „lajkují" (Přehled sociálních sítí 2019, 2019).

Tumblr – služba, kde uživatelé píšou krátké články a zveřejňují multimédia (Sociální sítě, 2020).

2.3 Komunity se stejnými zájmy

Obsah těchto sociálních sítí se soustředí především na specifické zájmy. Díky tomu, že se zde potkávají lidé se stejnými zájmy, vzniká spousta nových virtuálních přátelství a vztahů, které dále mohou vést k osobnímu setkání a případně i přátelství v reálném životě (Dobosiová, 2015).

Last.fm – aplikace zaměřená na hudbu, která nám nabízí playlisty s různými žánry nebo od uživateli vybraných interpretů (Last.fm, 2021).

Flickr – komunitní web zaměřený na sdílení fotografií (Flickr, 2021).

LinkedIn – profesní síť, kde mají uživatelé svůj profil, který je podobný životopisu. Oblíbená je především u personalistů, kteří přes ni hledají vhodné kandidáty na volné pozice (Přehled sociálních sítí 2019, 2019; Kožíšek a Písecký, 2016).

Tinder – aplikace umožňující navazování kontaktu mezi lidmi. Využívá geografické polohy, aby našla lidi v blízkém okolí. Potom uživatelé rozhodují přetažením prstu doprava nebo doleva na fotografii, jestli se jim osoba líbí či nelíbí (Tinder, 2021).

Clubhouse – nová sociální síť, která funguje na principu sdílení mluveného slova v rámci konkrétních místností. Uživatelé se připojují a komunikují v místnosti s tématikou, která je zajímá. Poté jsou všichni v místnosti rozděleni do dvou kategorií – jedná se o publikum a „řečníky". Do aplikace se dostanete tehdy, pokud obdržíte pozvánku od uživatele (Jelič, 2021).

3 KYBERŠIKANA

Kyberšikana (Cyberbullying) je jakékoliv chování, jehož úmyslem je ublížit, zastrašit, vyvést z rovnováhy nebo jinak ohrozit oběť prostřednictvím moderních informačních technologií – zvláště internetu nebo mobilního telefonu.

O kyberšikaně se hovoří, pokud oběť byla napadána cíleně a opakovaně skupinou či jedincem. V některých případech je propojena s klasickou šikanou, která obsahuje například slovní nadávky, pomluvy, ponižování nebo fyzické útoky. Kyberšikana zahrnuje mnoho podob útoku, jimiž mohou být verbální útoky, vyhrožování a zastrašování, ztrapňování šířením fotografií, videí či zvukových nahrávek, krádež identity, průnik na účet s cílem ponížit oběť, vydírání nebo i obtěžování vyzváněním (Kovářová, 2019).

Mezi některými dětmi a mladými lidmi se vyskytuje krutost. On-line anonymita má schopnost vyvolávat v jedinci násilné sklony, poněvadž mu dodává pocit moci nad obětí. Veřejný profil internetu dovoluje posměškům a vyhrožováním opustit teritorium školy a pronásledovat jejich oběť, pokaždé když je on-line. Obtěžování může nadále pokračovat, i když oběť změní školu nebo se přestěhuje (Hulanová, 2012; Kožíšek a Písecký, 2016).

3.1 Historický kontext

Do počátku 90. let 20. století sahá historie informačních a komunikačních technologií a s ní i kyberšikana. Nicméně její předchůdce můžeme najít již v pravěku. Jistě se nejedná o kyberšikanu jako takovou, ale o jeskynní kresby. Podle vědců šlo o psychické a sociální pochody, jejichž cílem bylo zesměšnit nebo poškodit někoho před širším publikem. Autor kreseb zůstává neznámý. Takové chování vychází ze shodných psychických a sociálních faktorů jako nynější kyberšikana (Claypoole, 2017).

Do celého světa se začaly šířit informační a komunikační technologie na konci 20. století. Společně s technologií se začala vyvíjet i kyberšikana. Mezi lety 2001-2003 založil Bill Belsey webové stránky týkající se kyberšikany (www.cyberbullying.org). Tyto webové stránky fungují doposud. Jeden z prvních článků o kyberšikaně vyšel v roce 2003 v časopise Journal of the American Academy of Child and Adolescent Psychiatri. Článek upozorňoval na nedostatek akademických odkazů vztahující se k tomuto problému. (Claypoole, 2017).

Po roce 2006 začali zahraniční autoři vydávat knihy zabývající se tímto problémem. Většina autorů vycházela z teorií a poznatků Billa Belseyho a Nancy Willarda. V České republice byly první výzkumy týkající se kyberšikany prováděny v letech 2009-2010 v rámci projektů

Minimalizace šikany a E-Bezpečí. Ukázalo se, že většina dětí pojmu kyberšikana nerozumí. Výzkumem se také zjistilo, že děti byly nejčastěji šikanovány pomocí e-mailů a mobilních telefonů. Výsledky projektů se nedají porovnávat, jelikož byly oba prováděny s odlišnými respondenty a rozdílnou metodou (Vašutová, 2010; Rogers, 2011).

3.2 Právní rámec

Zákon č. 40/2009 Sb., trestní zákoník.

Trestné činy proti svobodě

- § 175 Vydírání
- § 176 Omezování svobody vyznání

Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství

- § 182 Porušení tajemství dopravovaných zpráv
- § 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 184 Pomluva

Trestné činy proti lidské důstojnosti v sexuální oblasti (ad sexting)

- § 191 Šíření pornografie
- § 192 Výroba a jiné nakládání s dětskou pornografií
- § 193 Zneužití dítěte k výrobě pornografie

Trestné činy proti rodině a dětem

- § 202 Svádění k pohlavnímu styku

Trestné činy proti majetku

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Trestné činy obecně ohrožující

- § 287 Šíření toxikomanie

Trestné činy narušující soužití lidí

- § 352 Násilí proti skupině obyvatelů a proti jednotlivci
- § 353 Nebezpečné vyhrožování
- § 354 Nebezpečné pronásledování (tzv. kyberstalking)
- § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

Jiná rušení veřejného pořádku

- § 357 Šíření poplašné zprávy

Některé další formy trestné součinnosti

- § 364 Podněcování k trestnému činu
- § 365 Schvalování trestného činu (Zákon č. 40/2009 Sb.)

3.3 Vymezení rozdílů klasické šikany a kyberšikany

Šikana	Kyberšikana
- fyzický útok	- psychický útok
- konkrétní útočníci	- anonymní útočník
- úmyslná	- může být neúmyslná
- fyzická síla	- počítačové znalosti
- menší publikum	- větší publikum
- snadněji rozpoznatelná	- velmi obtížně rozpoznatelná

(Hollá, 2013)

3.4 Typy kyberšikany

Kyberšikana má spoustu podob, prostřednictvím kterých jde agresorovi vždy o zesměšnění, ublížení, stresování a poškození oběti. Nejčastěji se setkáváme s následujícími typy kyberšikany:

Kyberstalking

Znamená opětované zasílání zpráv, které obsahují výhružky, útočná a zastrašující sdělení, součástí může být také vydírání. Může vyvrcholit k fyzickému ohrožení. Patří sem i krádeže identity.

Kybergrooming

Jedná se o chování uživatelů na internetu, jehož záměrem je prostřednictvím internetových komunikačních prostředků vzbudit v jedinci pocity důvěry a pomocí falešné identity ho zneužít nebo vylákat na schůzku.

Kyberharašení

Značí opakované zprávy zasílané agresorem, které oběť vnímá jako nepříjemné. V této situaci je typické, že agresor posílá oběti nespočet zpráv vždy, když se oběť připojí nebo ji zahlcuje neúmyslnými SMS či MMS. Většinou jde o jednosměrnou komunikaci, kterou se oběť snaží ukončit.

Flaming

Označuje prudkou hádku, která se uskuteční mezi dvěma nebo více uživateli ve virtuálním komunikačním prostředí. Jedná se o plamennou výměnu názorů, jelikož flame znamená plamen. Převážně se setkáváme s urážkami, nadávkami, útočnou rétorikou nebo nám může agresor i vyhrožovat. Flame war značí hádku, která trvá delší dobu.

Sexting

Znamená zasílání fotografií, videí nebo textových zpráv se sexuálním obsahem. Provozování této činnosti má dvě varianty. Zprávy si můžeme vyměňovat s vlastním partnerem nebo s cizími osobami. Rizikové mohou být obě varianty, obzvláště v druhém případě. Objevují se i případy, kdy partner po rozchodu zveřejní tyto materiály.

Happy slapping

Prvotní forma happy slappingu vypadala tak, že byl napaden a zfackován neznámý kolemjdoucí jedincem či skupinou dospívajících. Současně tak celou situaci někdo natáčí na mobilní telefon, aby mohl následně video zveřejnit na internetu. Fyzické napadení již nemusí zahrnovat pouze fackování, ale může se v závažnosti stupňovat za hranici zákona.

Impersonation

Situace, kdy se agresor v on-line prostředí vydává za oběť. Například si může vytvořit falešný profil oběti a používat její údaje a fotografie. Vystupuje tak pod identitou oběti, a to zpravidla ubližujícím a nevhodným způsobem.

Denigration

Označuje sdělování klamných informací o druhém, které má za cíl druh sociálního poškození. Je tedy mířeno obzvláště na přihlížející.

Outing

Jedná se o fotografování a natáčení oběti v trapných a intimních situacích, které se následně zveřejňují na internetu. Pachatelé se někdy snaží oběť vydírat a přimět ji, aby citlivé informace o sobě publikovala sama.

Exclusion

Forma kyberagrese, kdy je oběť vyloučena z on-line skupiny, do které by měla nebo chtěla patřit (Černá et al., 2013; Kyberšikana, 2019).

3.5 Specifika kyberšikany

Charakteristikou klasické šikany je agresivní chování, nerovnost sil agresora a oběti. Pokud se jedná o kyberšikanu, tak se tyto charakteristiky mnohdy nemusí vůbec vyskytovat, jelikož se kyberšikana může objevovat kdykoliv a kdekoliv. Je schopná se šířit velmi rychle a může dosáhnout až nepředvídatelných rozměrů. Díky internetu se tak agresorům dostalo dalších prostředků k ubližování oběti. V procesu šikanování se může měnit role agresora a oběti.

Agresor

V klasické šikaně bývá agresorem silný jedinec, avšak v kyberšikaně to může být prakticky kdokoliv. Nezáleží zde na fyzické nebo sociální zdatnosti agresora, ale na zdatnosti v oblasti informačních technologií.

Oběť

Obětí se může stát naprosto kdokoli, stejně tak jako agresorem. Ten si vybírá svou oběť v kyberprostoru zcela náhodně. Neustále však převládají útoky na jedince se sníženou schopností se bránit. Těm, kteří jsou na mobilních telefonech či počítačích závislí, hrozí větší riziko vyhledání a napadení agresorem.

Čas a místo útoků

Čas a místo u klasické šikany lze často předpokládat, neboť se útoky opakují většinou na totožných místech a ve stejnou dobu. Agresoři znají výhody jejich chování v podobně kyberšikany, využívají především anonymitu na internetu k nepřetržitému kyberšikanování oběti mimo školu. Nikdo neví, kdy útok nastane. Již připojením uživatele k internetu může nastat počátek útoku. S tímto nebezpečím se lze prakticky setkat kdekoliv a kdykoliv.

Absence fyzického násilí

Kyberšikana znesnadňuje identifikaci oběti jejím okolím, jelikož se v procesu nevyskytují přímé znaky šikanovaní, jako jsou například roztrhané oblečení, ztráta věcí či peněz, zranění, modřiny a podobně.

Absence úniku

Klasická šikana je založena na osobním setkávání agresora a oběti, které je možno zčásti předvídat a případně se mu i vyhnout. Agresor kyberšikany může neustále narušovat soukromí oběti, pronásledovat ji prakticky kdekoli a nutit ji tak žít pod nesnesitelným tlakem.

Opakování

Stejný účinek jako systematické klasické šikanování může mít jediná nemilá zpráva, e-mail či odkaz na webové stránky, kde jsou zveřejněny urážky určené oběti. Takové zprávy si může oběť pořád dokola pročítat. Zjištění, že existující zprávy není možné na internetu zrušit a stávají se tak trvalé, přidávají oběti pocit beznaděje. Během klasické šikany si oběť nemusí všechny nadávky a urážky pamatovat, ale v případě SMS zpráv, chatu, e-mailu a webových stránek si všechno to, co ji agresoři sdělili, pročítá neustále dokola. V tomto případě mají napsaná slova značně tvrdší dopad než slova mluvená.

Šíře publika

Kyberšikana, která probíhá na webových stránkách, poskytuje přístup v podstatě komukoli, kdo má připojení na internet. Kdokoli na světě se tak může stát divákem kyberšikany. Nemusí se odehrávat opakovaně, stačí jedna publikovaná ponižující fotografie oběti na webu a kdokoli si ji může stáhnout nebo ji šířit ještě předtím, než ji poskytovatel konkrétního serveru dokáže odstranit. Ponížení mohou vidět stovky i tisíce lidí. Následkem může u oběti dojít k psychickému zhroucení (Hulanová, 2012; Šambergerová, 2020).

3.6 Prostředky kyberšikany

Kyberšikana se realizuje pomocí různých informačních a komunikačních technologií. Tyto technologie se velmi rychle vyvíjejí a lidé díky nim čerpají nové způsoby v komunikaci. V současné době se tak stávají nedílnou součástí našeho života. Prostředky kyberšikany vykazují různé formy. Jakýkoli útočník kyberšikany, vlastnící nějakou komunikační technologii, má možnost využít nebo rovnou zneužít spoustu komunikačních prostředků k provedení kyberútoku.

SMS a MMS zprávy

Mezi první prostředek kyberšikany lze zařadit útoky s využitím SMS a MMS zpráv. Tento druh kyberšikany je velice častým a úroveň anonymity útočníka se může dostat na vysokou úroveň, obzvlášť když využije SIM kartu „na jedno použití“. Taková karta není nějak vázáná na jméno, bydliště či jakýkoliv jiný údaj, umožňující dohledání pachatele. Samotný útok vypadá tak, že oběť dostává v krátkém čase množství zpráv. Obsah těchto zpráv může být výhružný, a často i útočného charakteru.

Mobilní telefonáty

Mobilní telefon se stává v dnešní době nejrozšířenějším komunikačním prostředkem. Takovýto prostředek se velice lehce dostane do rukou agresorů, kteří jej využívají k neustálým telefonátům. Tyto hovory mohou být v lepším případě pouze obtěžující, ale lze zažít i telefonáty s útočným podtextem, anebo dokonce hovory výhružného charakteru. Podobným druhem těchto útoků, může být i případ, kdy je osobě ukraden telefon a následně se pachatel vydává za majitele telefonu. Využívá tak cizí identitu při vyhrožování a obtěžování ostatních lidí.

E-mailové zprávy

Tento druh útoku, z hlediska zachování anonymity, je ideálním prostředkem pro využití při kyberšikaně na internetu. Vytvořit si e-mailový účet je otázkou pár minut a agresoři tak mohou velice rychle a snadno ihned rozesílat útočné a výhružné zprávy obětím.

Sociální sítě

Sociální sítě jsou v dnešní době jednoznačně nejrozšířenějším místem, na kterém se odehrává většina lidských komunikací a kontaktů. Komunikaci lze rozdělit na soukromou a veřejnou. Právě zmíněná soukromá komunikace mezi lidmi na sociálních sítích se může lehce stát cílem útočníků, kteří z ní chtějí získat co nejcitlivější informace a ty dále využívat

k vyhrožování, zastrašování a často i k vydírání. Nejčastěji k těmto odcizením citlivých informací dochází při vydávání útočníka za jinou osobu, která se oběti zdá důvěryhodná. Obezřetnost oběti je často na minimální hranici a důsledkem dochází k odcizení a následnému zneužívání získaných citlivých informací.

Internetové stránky

Dalším prostředkem kyberšikany rozšířené především v kruzích známých osobností a politiků jsou útoky, při kterých je o dané osobě vytvořen například falešný blok, anebo osobní stránka. Lze se setkat i s případy, kdy byla o oběti vytvořena anketa, kde se klade mnoho osobních otázek týkajících se soukromého života oběti.

Chatovací místnosti

Prostředek kyberšikany, probíhající především na herních stránkách a ve virtuálních světech, se často vyznačuje účastí především mladých lidí na tomto způsobu komunikace. Dokud nejsou porušena žádná bezpečnostní opatření, jedná se o výborný prostředek sdílení informací. V opačném případě dochází k zneužití těchto komunikačních místností a nastává tak vyhrožování a zastrašování zúčastněných osob.

Instant messaging

V dnešním světě je pro komunikaci mezi lidmi velice často využívaná řada aplikací a programů, jako jsou například Messenger či Skype. Tyto programy se často stávají prostředkem, který využívají útočníci pro obtěžování nebo vyhrožování lidem, kteří jsou účastníky těchto online komunikací.

On-line hry

Především v okruhu mladých lidí se velice často vyskytuje prostředek kyberšikany využívající online hry. Útočníci během hraní napadají slovně ostatní hráče a často dochází až k výhružkám či zastrašování. Dále útočníci mohou nutit oběti k plnění různých úkolů, specifické komunikaci nebo mohou oběť vyloučit z online hry (Rogers, 2011).

II. PRAKTICKÁ ČÁST

4 ANALÝZA VZTAHU DĚTÍ K PROBLEMATICE INTERNETOVÉ BEZPEČNOSTI A KYBERŠIKANY

Jak bylo zmíněno v teoretické části, existuje mnoho typů kyberšikany a lidé se s ní mohou setkat na mnoha místech a různých prostředcích komunikace. Mezi nejzranitelnější skupinu, z hlediska kyberšikany, patří především děti ve školním věku. Základním předpokladem pro úspěšnou obranu proti kyberšikaně je vědomí o této možné hrozbě. Jen když děti ví, jaká hrozba je může potkat, dokáží se jí bezpečně vyhnout. Proto je potřeba zjistit, jak jsou na tom děti ve školním věku s povědomím o problematice internetové bezpečnosti a kyberšikany a na základě toho následně provést další kroky pro zlepšení aktuálního stavu.

4.1 Stanovení výzkumných otázek a hypotéz

Před analýzou vztahu dětí k problematice kyberšikany je potřeba si stanovit hranice zkoumaného problému. Je potřeba si uvědomit, co od dotazníkového šetření očekáváme a jaké jsou předpoklady výsledků. Ke stanovení rozsahu a hranic zkoumaného problému slouží definování výzkumného problému, výzkumných otázek a hypotéz.

Pro přesné vymezení, co chceme zkoumat, je potřeba stanovit výzkumný problém.

Výzkumný problém:

Přítomnost kyberšikany u žáků základních škol

Výzkumné otázky:

- Kolik dětí je seznámeno s problematikou kyberšikany?
- Odkud se děti poprvé dozvídají o kyberšikaně?
- Jaký je názor dětí na kyberšikanu?
- Kolik dětí se již setkalo s kyberšikanou?
- Jaký je početní poměr mezi agresory, obětmi a přihlížejícími kyberšikaně?
- V případě, že by se děti setkaly s kyberšikanou, jak by se zachovaly?

Výzkumnými otázkami dané téma lze lépe popsat a následně z nich vyvodit jisté hypotézy.

Hypotézy:

Hypotézu můžeme označit jako předpoklad současného stavu. Snažíme se ji výzkumem ověřit – tedy zamítnout nebo nezamítnout. Zde byly stanoveny následující hypotézy:

1. Děti využívají sociální sítě hlavně kvůli komunikaci s přáteli.
2. Děti vnímají kyberšikanu stejně nebezpečnou jako klasickou fyzickou šikanu.
3. Děti vědí, že ke kyberšikaně se využívají hlavně sociální sítě.

4.2 Dotazníkové šetření

Součástí praktické části je dotazníkové šetření. Uvedený druh výzkumu byl zvolen zejména proto, že je anonymní a umožnil tak oslovit velký počet respondentů, čímž se podařilo získat značné množství informací. S ohledem na zvolené téma bakalářské práce je anonymita považována za velkou výhodu. Respondent s utajenou totožností snáze odpoví i na otázky, na které by veřejně pod svým jménem pravděpodobně neodpověděl.

Samotný dotazník byl vytvořen přes on-line aplikaci Formuláře Google, kde probíhalo i jeho vyplňování. Otázky obsaženy v dotazníku byly formulovány jednoduše a srozumitelně, aby byly pro respondenty pochopitelné. Dotazník je rozdělen do tří částí. První část zahrnuje úvod a informativní otázky, druhá část tématiku sociálních sítí a třetí se zabývá kyberšikanou. V dotazníku se nachází 20 výzkumných otázek. Lze mezi nimi nalézt otázky polouzavřené a uzavřené (dichotomické, trichotomické i polytomické).

Jako respondenti pro dotazníkové šetření byli zvoleni žáci druhého stupně základních škol. Jedná se o děti ve věku od 10 do 16 let, v období označovaných jako střední školní věk a starší školní věk neboli pubescence až adolescence. Uvedená věková skupina byla zvolena z toho důvodu, že děti v tomto období rády zkouší nové věci a experimentují. Taktéž je pro ně důležitý kontakt s vrstevníky, které často hledají právě na internetu, především na sociálních sítích. Proto bylo zajímavé zjistit, zdali tyto děti mají povědomí o problematice kyberšikany, jak se chovají na internetu, zda jednají bezpečně a nejsou tak ohroženi tímto negativním fenoménem současnosti.

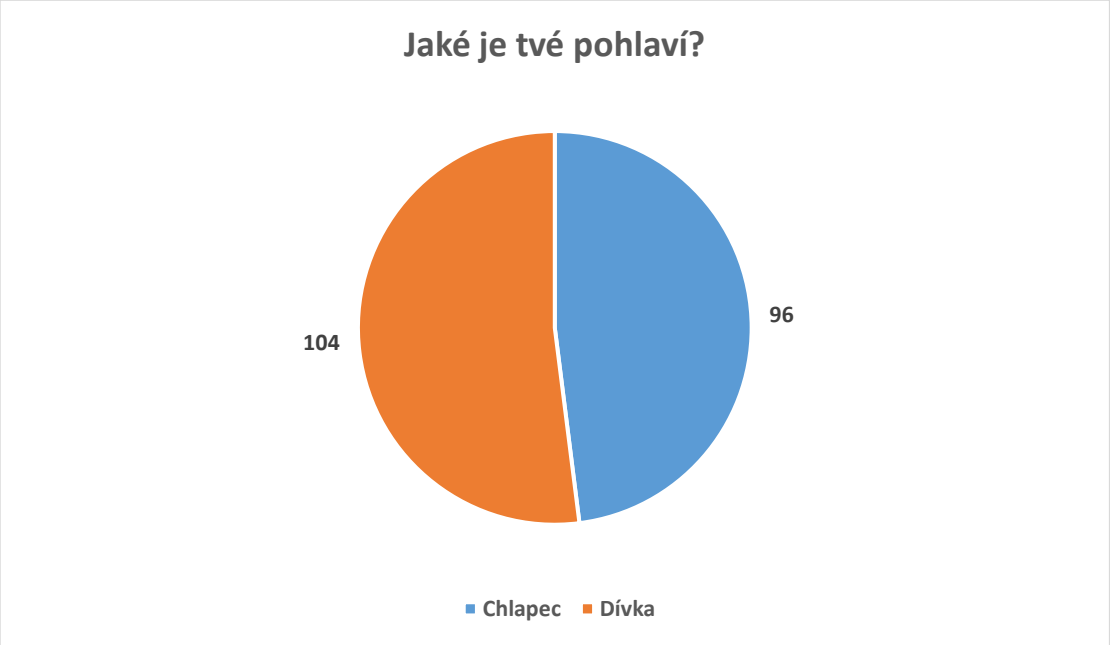
Na tento dotazník odpovídalo 200 respondentů.

4.2.1 Analýza a vyhodnocení výsledků

Následující část je věnována veškerým poznatkům, které byly získány od respondentů. Výsledky dotazníkového šetření jsou uvedeny v grafech. Na začátku dotazníku byly nejdříve zkoumány údaje dotazovaných, které nám přiblíží zkoumaný vzorek. Jedná se o údaje týkající se pohlaví a věku. Dále jsou jednotlivě rozebrány otázky vztahující se k sociálním sítím a kyberšikaně dle odpovědí zúčastněných.

Otázka č. 1: **Jaké je tvé pohlaví?**

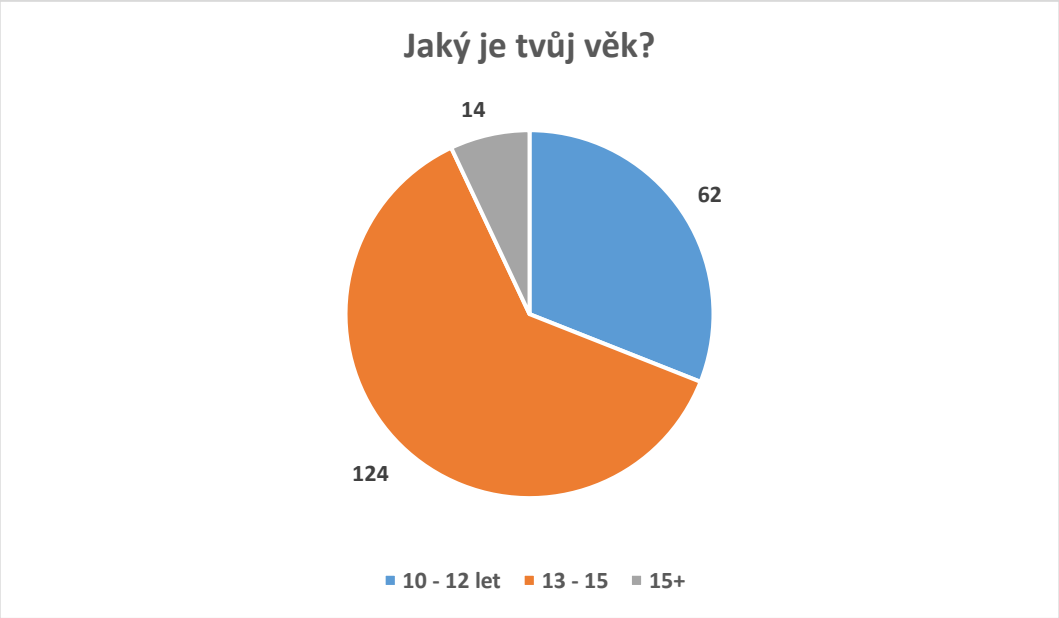
Dotazníkového šetření se zúčastnilo 200 respondentů z druhého stupně základních škol. Podle pohlaví je rozdělení na 104 dívek (52 %) a 96 chlapců (48 %).



Obrázek 1 - Graf odpovědí na otázku č. 1 [vlastní]

Otázka č. 2: **Jaký je tvůj věk?**

Podle věku je nejčetnější skupina ve věku 13–15 let a to 124 respondentů (62 %). Dále je 62 dotazovaných (31 %) ve věku 10-12 let a poslední zkoumanou skupinu tvoří ve věku 15+ let 14 respondentů (7 %).



Obrázek 2 - Graf odpovědí na otázku č. 2 [vlastní]

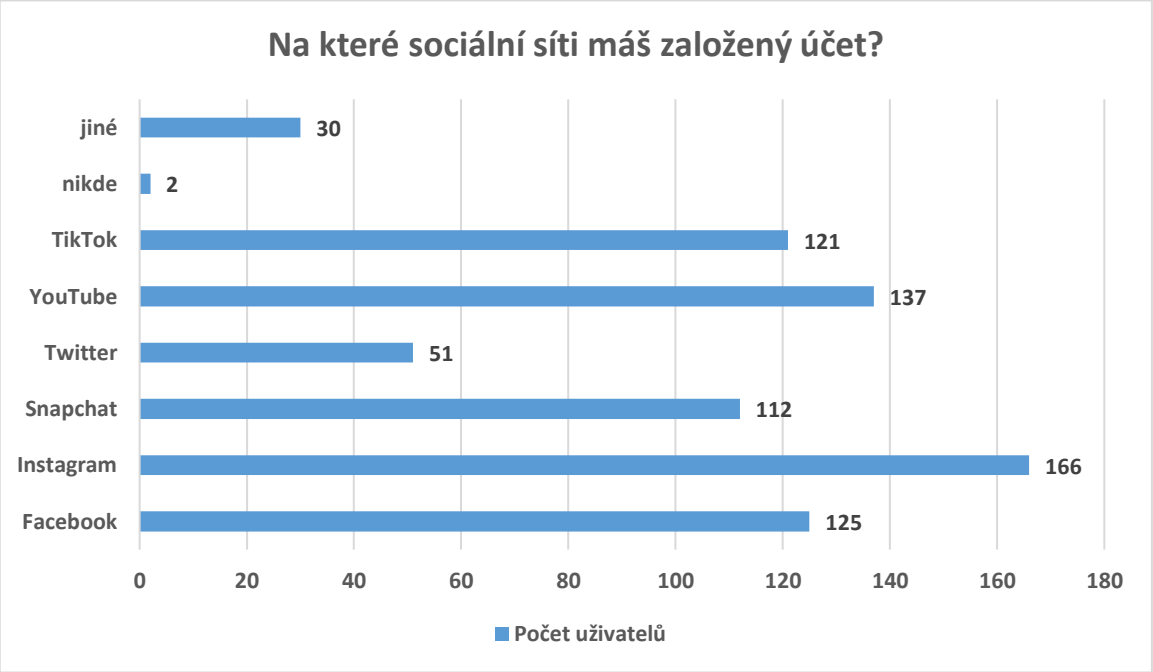
Otázka č. 3: **Máš založený účet na nějaké sociální síti?**

Většina dotázaných, tedy 194 (97 %), odpovědělo, že mají založený účet na nějaké sociální síti. Pouze 6 respondentů (3 %) nemá založený účet na žádné sociální síti.

Obrázek 3 - Graf odpovědí na otázku č. 3 [vlastní]

Otázka č. 4: **Na které sociální síti máš založený účet?**

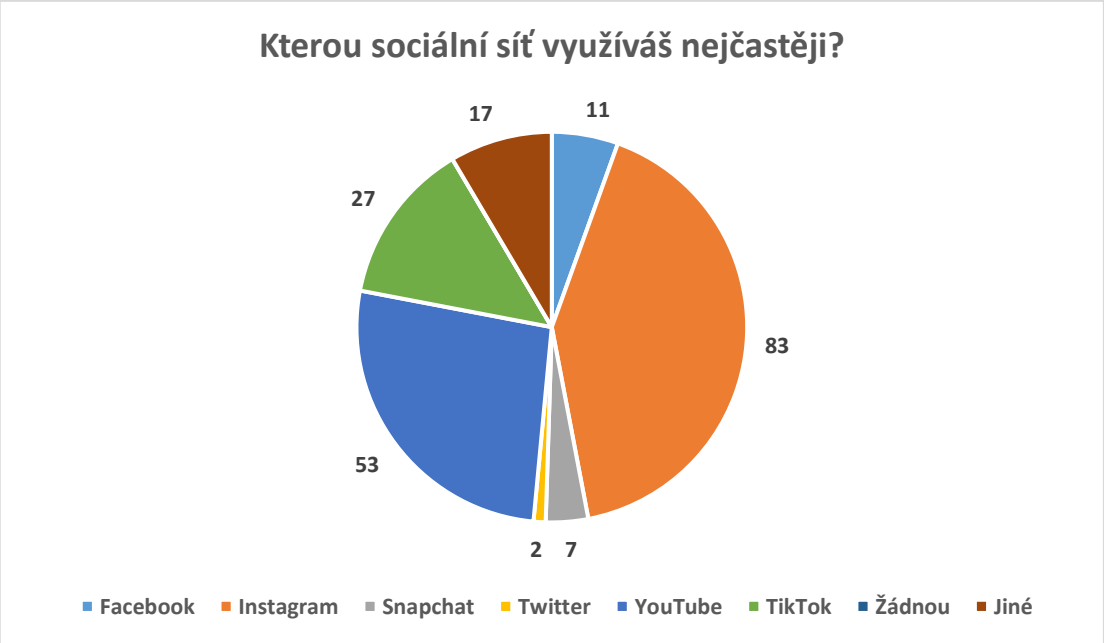
Zde měli respondenti možnost výběru více odpovědí. Na sociální síti Instagram má založený účet naprostá většina, tedy 166 dotazovaných. Mezi další populární sítě patří YouTube se 137 uživateli, Facebook se 125 a TiTok se 121 uživateli. Aplikaci Snapchat používá 112 respondentů. Nejmenší počet 51 uživatelů má Twitter a 30 dotázaných odpovědělo, že má účet na jiných sociálních sítích (Messenger, WhatsApp, Viber, Twitch nebo Discord). Pouze 2 respondenti odpověděli, že nemají nikde založený účet. Většina dotazovaných má založený účet více než na jedné sociální síti.



Obrázek 4 - Graf odpovědí na otázku č. 4 [vlastní]

Otázka č. 5: **Kterou sociální síť využíváš nejčastěji?**

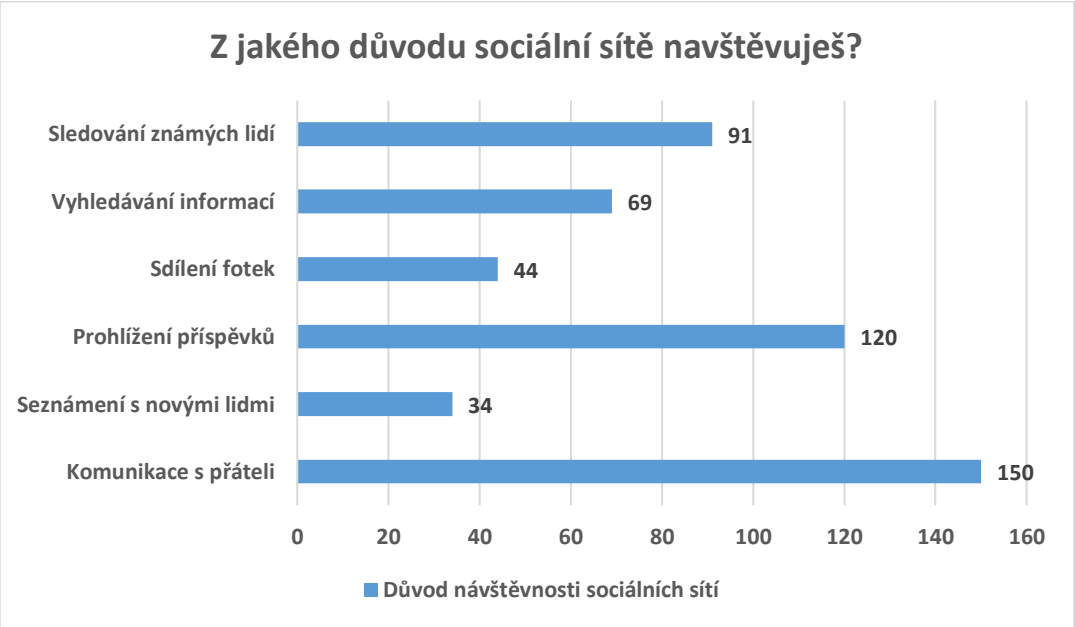
Většina dotazovaných nejčastěji využívá sociální síť Instagram. Odpovědělo tak 83 respondentů (42 %), druhou nejvyužívanější sítí je YouTube, kterou využívá 53 respondentů (27 %). TikTok využívá 27 respondentů (14 %), 17 respondentů (9 %) využívá jiné sociální sítě, než jsou uvedeny v dotazníku (Messenger, WhatsApp, Viber, Twitch nebo Discord). Facebook, jakož to nejrozšířenější sociální síť, využívá pouze 11 dotazovaných (6 %). Jako nejméně využívané sítě vyšly z dotazníku Snapchat s počtem 7 uživatelů (4 %) a Twitter s nejmenším počtem 2 uživatelů (1 %).



Obrázek 5 - Graf odpovědí na otázku č. 5 [vlastní]

Otázka č. 6: **Z jakého důvodu sociální sítě navštěvuješ?**

Zde měli respondenti možnost výběru více odpovědí. 150 dotazovaných uvedlo, že nejčastěji navštěvují sociální sítě z důvodu komunikace s přáteli. Druhý nejvyšší počet 120 respondentů využívá sociální sítě z důvodu prohlížení příspěvků. Dalšími důvody jsou sledování známých lidí (91), vyhledávání informací (69), sdílení fotek (44) a seznámení s novými lidmi (34). Je zřejmé, že respondenti využívají sociální sítě z více důvodů.



Obrázek 6 - Graf odpovědí na otázku č. 6 [vlastní]

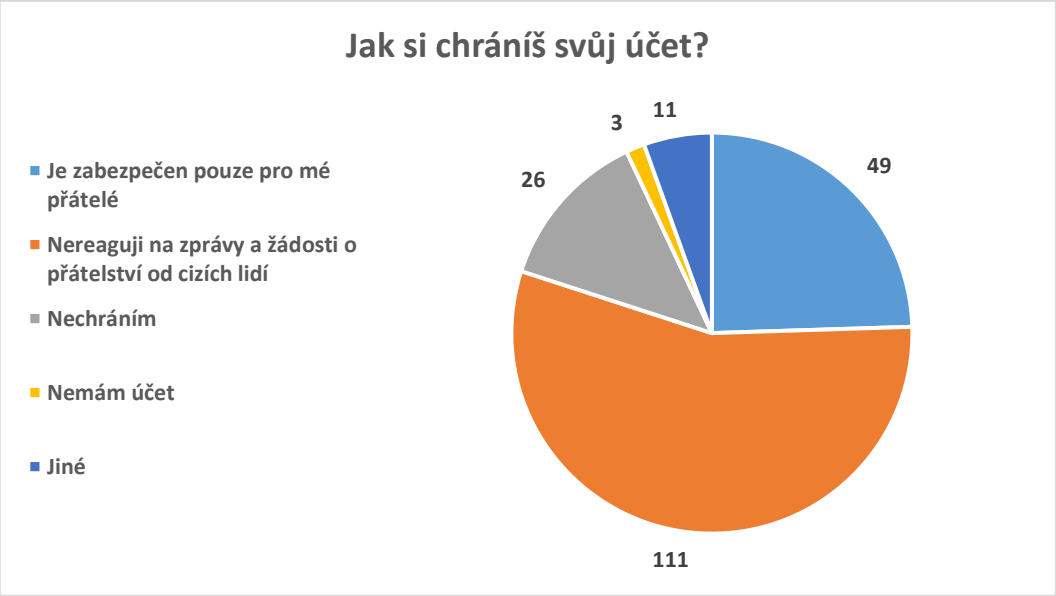
Otázka č. 7: **Kolik času na nich denně trávíš?**

Z odpovědí vyplývá, že 63 respondentů (32 %) stráví na internetu denně 1-2 hodiny. Možnost 2-3 hodiny zvolilo celkem 52 dotázaných (26 %) a možnost 3 a více hodin uvedlo dokonce 46 respondentů (23 %). 25 dotazovaných (13 %) stráví denně na internetu méně než hodinu a zbývajících 14 (7 %) uvádí čas 1 hodinu. Je patrné, že respondenti na internetu tráví poměrně dost času.

Obrázek 7 - Graf odpovědí na otázku č. 7 [vlastní]

Otázka č. 8: **Jak si chráníš svůj účet?**

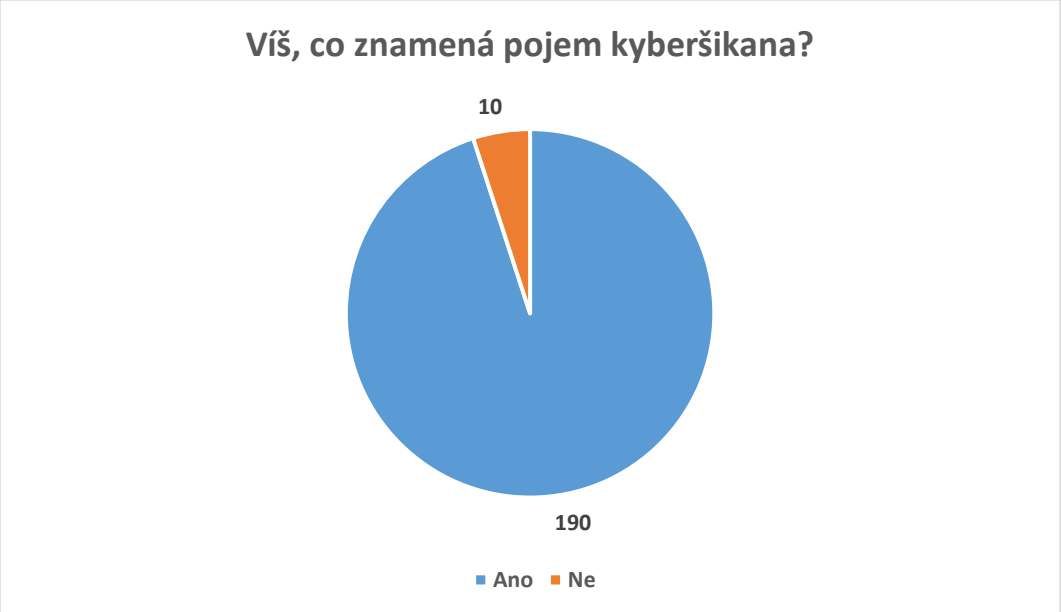
Ze sběru dat týkajícího se chránění svého sociálního účtu vyplývá, že největší počet 111 (56 %) uvedlo, že používají formu ochrany účtu pouze nereagováním na zprávy a žádosti o přátelství od cizích lidí. Dále 49 dotázaných (25 %) má účet zabezpečený tím, že je přístupný pouze pro své přátelé a 26 respondentů (13 %) si svůj účet nechrání žádným způsobem. 11 uživatelů (6 %) si chrání svůj účet jiným způsobem a zbylí 3 (2 %) nemají žádný učet na sociální síti.



Obrázek 8 - Graf odpovědí na otázku č. 8 [vlastní]

Otázka č. 9: **Víš, co znamená pojem kyberšikana?**

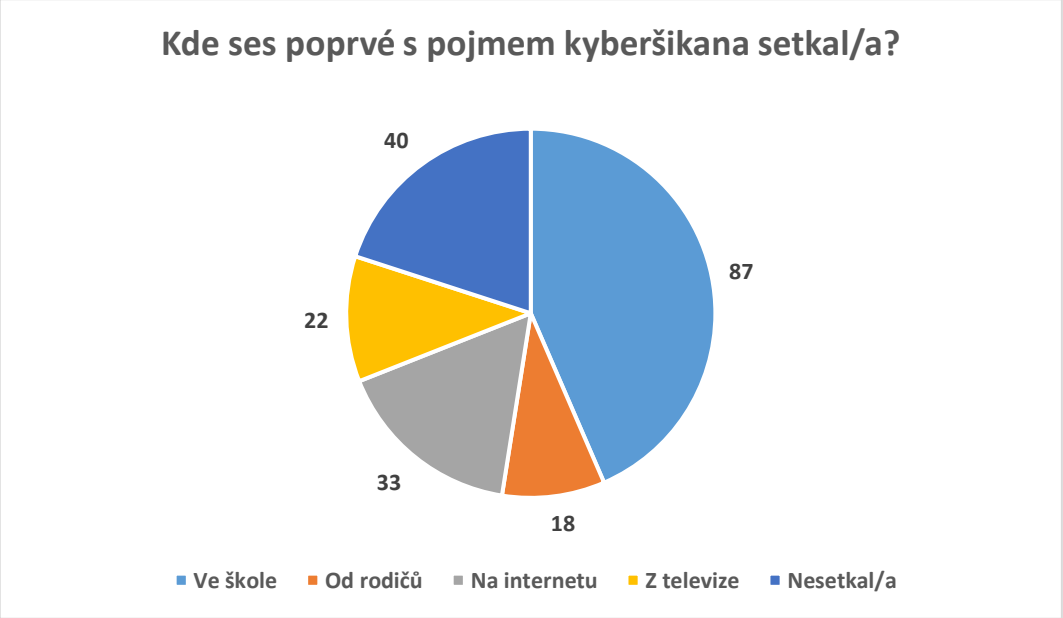
Kyberšikana je velmi závažným problémem v dnešní době. Je nezbytné kyberšikanu včas řešit a nepřehlížet ji. Vychází z tradiční šikany a její zákeřnost spočívá v tom, že prostřednictvím informačních a komunikačních technologií, může prakticky nastat kdekoliv a kdykoliv. Otázka zjišťuje, zda studenti pojem znají. Naprostá většina, tedy 190 respondentů (95 %), ví, co pojem kyberšikana znamená. Bohužel 10 dotázaných (5 %) pojem nezná.



Obrázek 9 - Graf odpovědí na otázku č. 9 [vlastní]

Otázka č. 10: **Kde ses poprvé s pojmem kyberšikana setkal/a?**

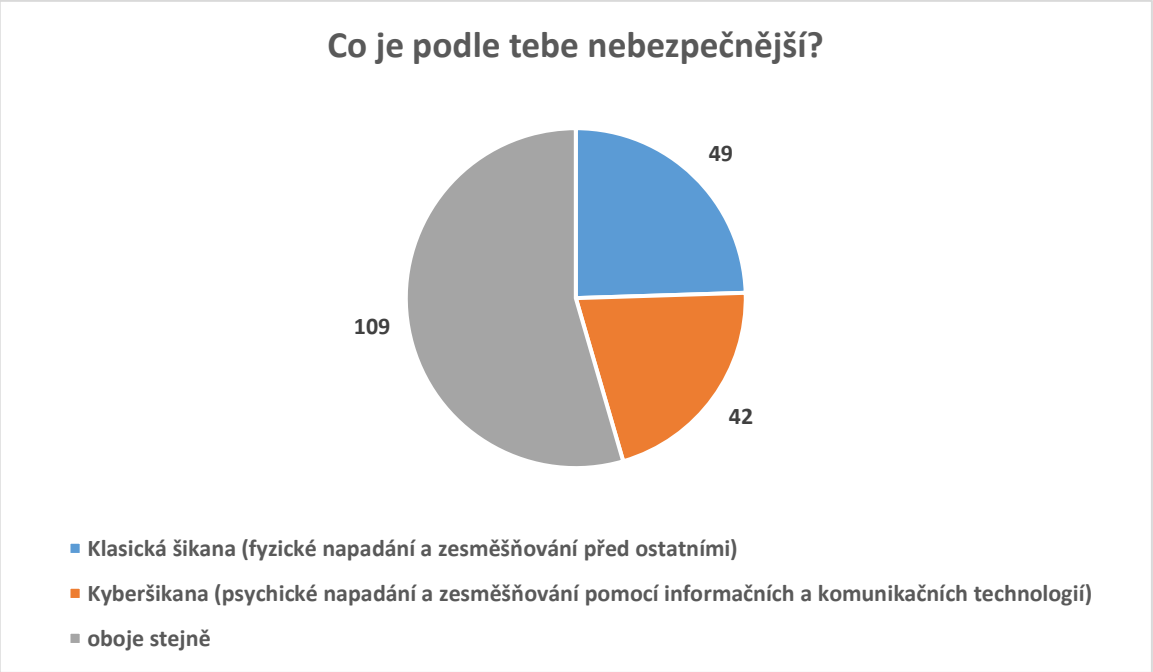
Celkem 87 respondentů (44 %) uvedlo, že se s tímto pojmem poprvé setkalo ve škole. 40 dotázaných (20 %) odpovědělo, že se s termínem kyberšikany nesetkali, tedy na něj poprvé narazili v tomto dotazníku. Další možnou variantou byla odpověď na internetu, kterou zvolilo 33 respondentů (17 %). Možnost z televize zvolilo celkem 22 dotázaných (11 %). Poslední možnou odpovědí byla odpověď od rodičů a tu vybralo pouze 18 respondentů (9 %).



Obrázek 10 - Graf odpovědí na otázku č. 10 [vlastní]

Otázka č. 11: **Co je podle tebe nebezpečnější?**

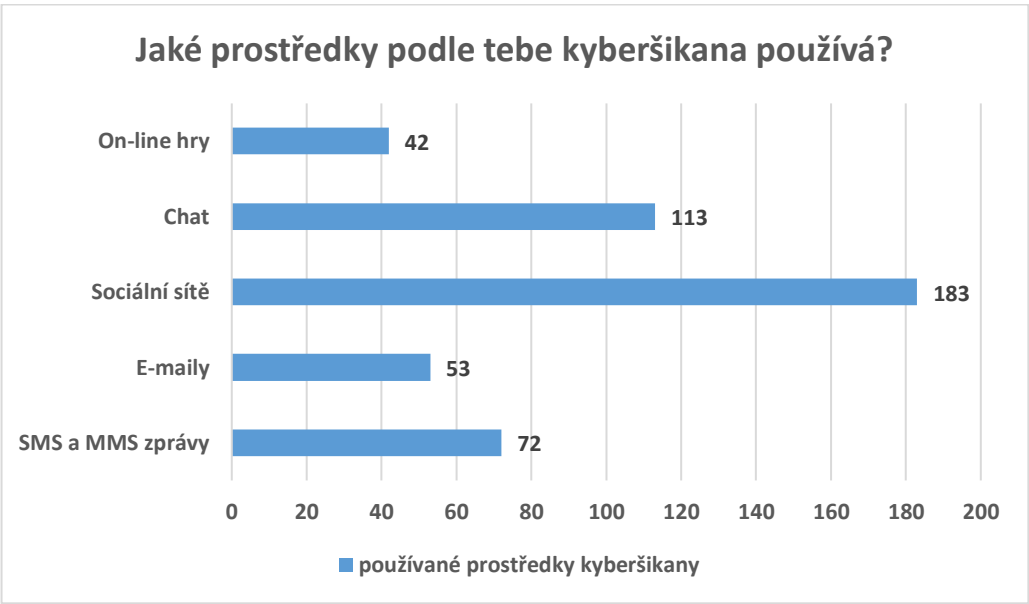
Otázka měla zjistit, jak respondenti vnímají nebezpečnost šikany a kyberšikany. Z odpovědí vyplývá, že 109 dotazovaných (55 %) považuje klasickou šikanu a kyberšikanu za stejně nebezpečné. Možnost, že je klasická šikana nebezpečnější než kyberšikana, uvedlo 49 respondentů (25 %). Kyberšikana je pro 42 dotázaných (21 %) nebezpečnější než klasická šikana.



Obrázek 11 - Graf odpovědí na otázku č. 11 [vlastní]

Otázka č. 12: **Jaké prostředky podle tebe kyberšikana používá?**

Zde měli respondenti možnost výběru více odpovědí. Převážná většina dotazovaných odpověděla, že mezi prostředky kyberšikany patří sociální sítě, celkem 183 respondentů. Další možnou variantou byla odpověď chat, kterou uvedlo 113 dotázaných. Jako nejméně používané prostředky kyberšikany vyšly z dotazníku SMS a MMS zprávy (72), e-maily (53) a on-line hry (42).



Obrázek 12 - Graf odpovědí na otázku č. 12 [vlastní]

Otázka č. 13: **Setkal/a ses někdy s kyberšikanou?**

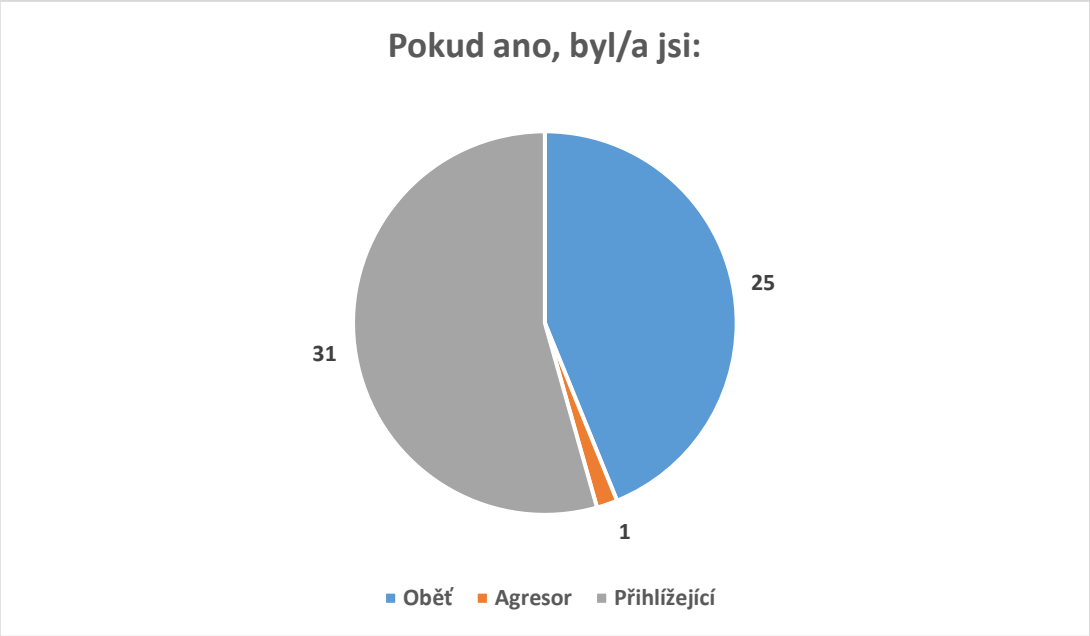
Otázka zjišťuje, zda se samotní studenti někdy setkali s kyberšikanou. Převážná část, tedy 162 dotázaných (81 %), se s kyberšikanou nesetkali. Celkem 38 respondentů (19 %) zvolilo možnost opačnou, tedy odpověď ano, již se s kyberšikanou někdy setkali.

Obrázek 13 - Graf odpovědí na otázku č. 13 [vlastní]

Otázka č. 14: **Pokud ano, byl/a jsi:**

Tato otázka navazuje na předchozí otázku č. 13, kde bylo zjišťováno, jestli se někdo z respondentů někdy setkal s kyberšikanou. Otázka nebyla povinná a účastníci ji mohli v dotazníkovém šetření přeskočit. I přesto na tuto otázku odpovědělo 57 účastníků. Je patrné, že se s kyberšikanou setkalo více dotázaných, než kolik jich odpovědělo ano v předchozí otázce.

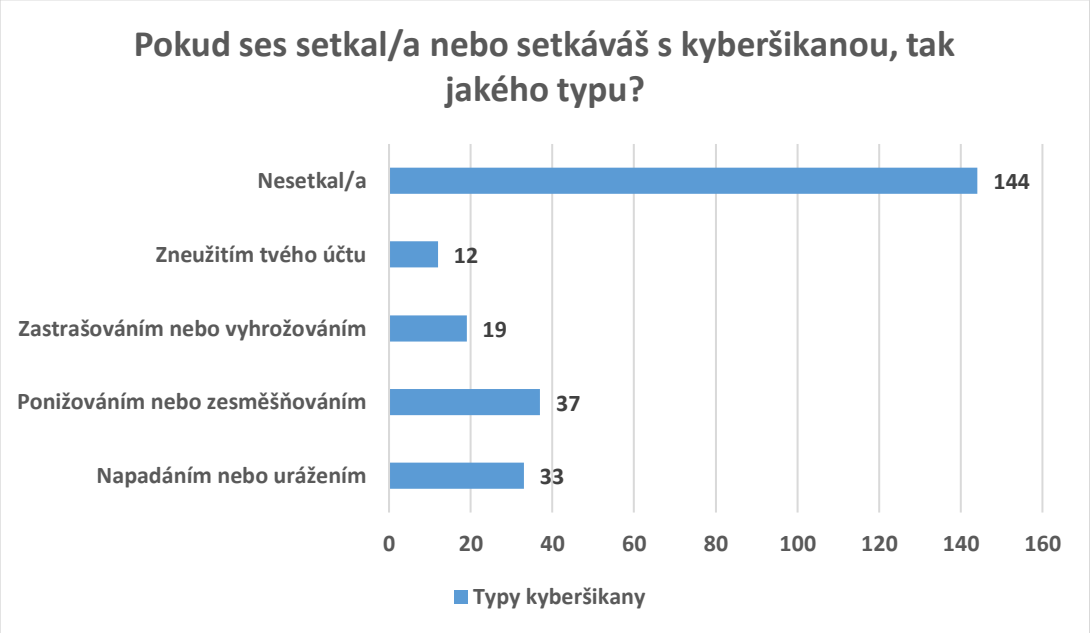
Celkem 31 respondentů (54 %) se někdy setkalo s kyberšikanou jako přihlížející (svědci), kteří mají jistý vliv na vývoj kyberšikany. Tato role je významná hlavě proto, že mohou zabránit jejímu dalšímu pokračování. V mnoha případech přihlížející nic neudělají, čímž dávají tichý souhlas k tomu, co se odehrává. Bohužel 25 respondentů (44 %) bylo obětí kyberšikany. Jedinec, který se stává cílem kyberšikany je kyberoběť, kterému vzniká velké riziko vzniku psychických problémů. Možnost, že se někdo setkal s kyberšikanou jako agresor odpověděl 1 dotázaný (2 %). Kyberagresor je osoba, která šikanu rozpoutá a aktivně se na ní podílí.



Obrázek 14 - Graf odpovědí na otázku č. 14 [vlastní]

Otázka č. 15: **Pokud ses setkal/a nebo setkáváš s kyberšikanou, tak jakého typu?**

Zde měli respondenti možnost výběru více odpovědí. Nejvyšší počet 144 dotazovaných uvedlo, že se s kyberšikanou nesetkali. Dalších 37 respondentů uvedlo setkání s kyberšikanou typu ponižování a zesměšňování, 33 respondentů typu napadání nebo urážení a 19 dotázaných se setkalo se zastrašováním nebo vyhrožováním. Na možnost kyberšikany typu zneužitím tvého účtu zareagovalo 12 respondentů.

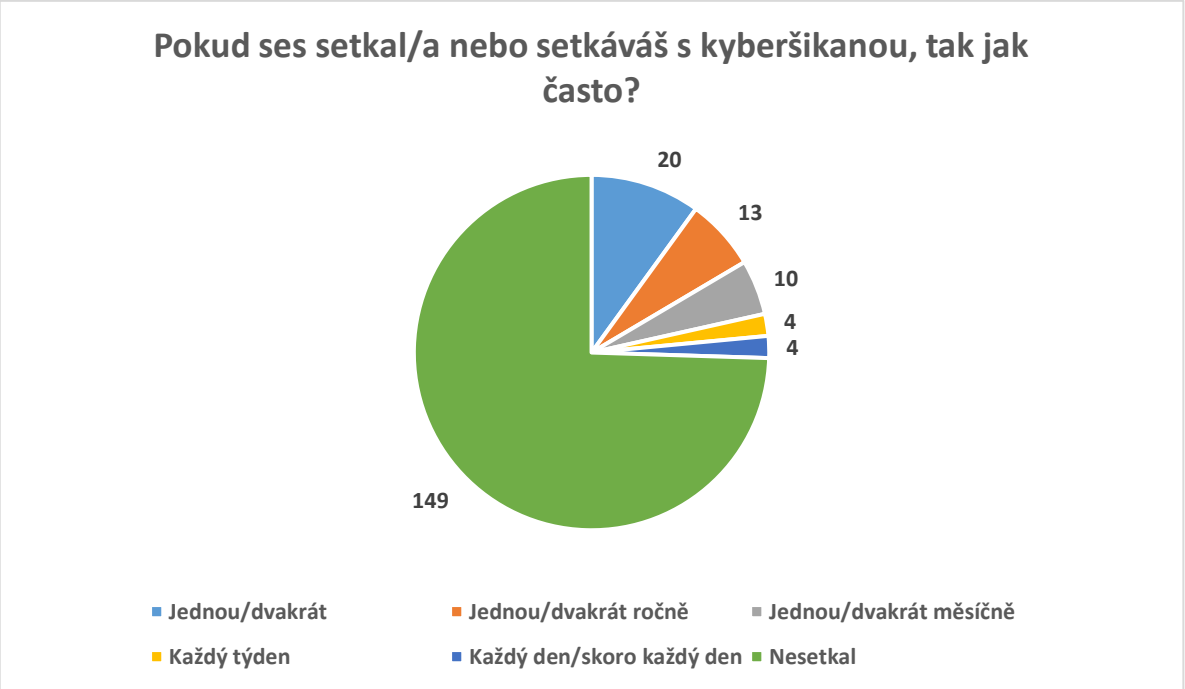


Obrázek 15 - Graf odpovědí na otázku č. 15 [vlastní]

Otázka č. 16: **Pokud ses setkal/a nebo setkáváš s kyberšikanou, tak jak často?**

Tato otázka navazuje na předchozí otázky, kde bylo zjišťováno, jestli se někdo z respondentů někdy setkal s kyberšikanou, případně s jakou formou a jakého typu. Cílem otázky bylo zjistit, jak často se respondenti s kyberšikanou setkávají.

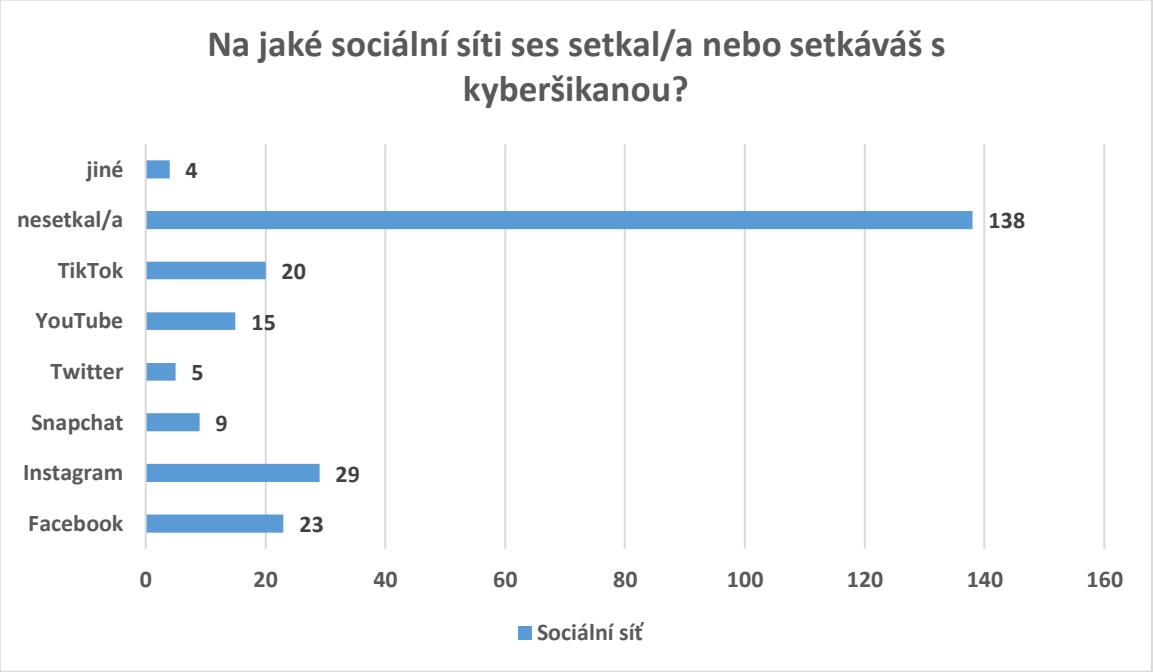
Celkem 149 dotazovaných (75 %) se s kyberšikanou nesetkalo. Respondenti, kteří měli s kyberšikanou nějakou zkušenost uvedli, že se ve většině případech jednalo o jedno až dvě setkání, což uvedlo 20 studentů (10 %). Následně 13 dotazovaných (7 %) se s tímto fenoménem potýká jednou až dvakrát ročně a 10 dotazovaných (5 %) dokonce jednou až dvakrát měsíčně. 4 respondenti (2 %) uvedli, že se s kyberšikanou setkávají každý týden a taktéž 4 respondenti jí čelí každý den/skoro každý den.



Obrázek 16 - Graf odpovědí na otázku č. 16 [vlastní]

Otázka č. 17: **Na jaké sociální síti ses setkal/a nebo setkáváš s kyberšikanou?**

Zde měli respondenti možnost výběru více odpovědí. Převážná část, tedy 138 dotázaných, se s kyberšikanou na sociálních sítích nesetkali. Sociální síť, kde se respondenti setkali nejčastěji s kyberšikanou je Instagram, který označilo 29 studentů. Další v pořadí, hned za Instagramem, je uvedena 23 respondenty sociální síť Facebook a 20 respondenty síť TikTok. Následující nejčastější setkání bylo na síti YouTube, který uvedlo 15 dotázaných, Snapchat určilo 9 dotázaných, 5 dotázaných Twitter a 4 dotázaní uvedli setkání na jiné sociální síti (Messenger, Discord). Z odpovědí vyplývá, že se respondenti setkávají s kyberšikanou na různých sociálních sítích.



Obrázek 17 - Graf odpovědí na otázku č. 17 [vlastní]

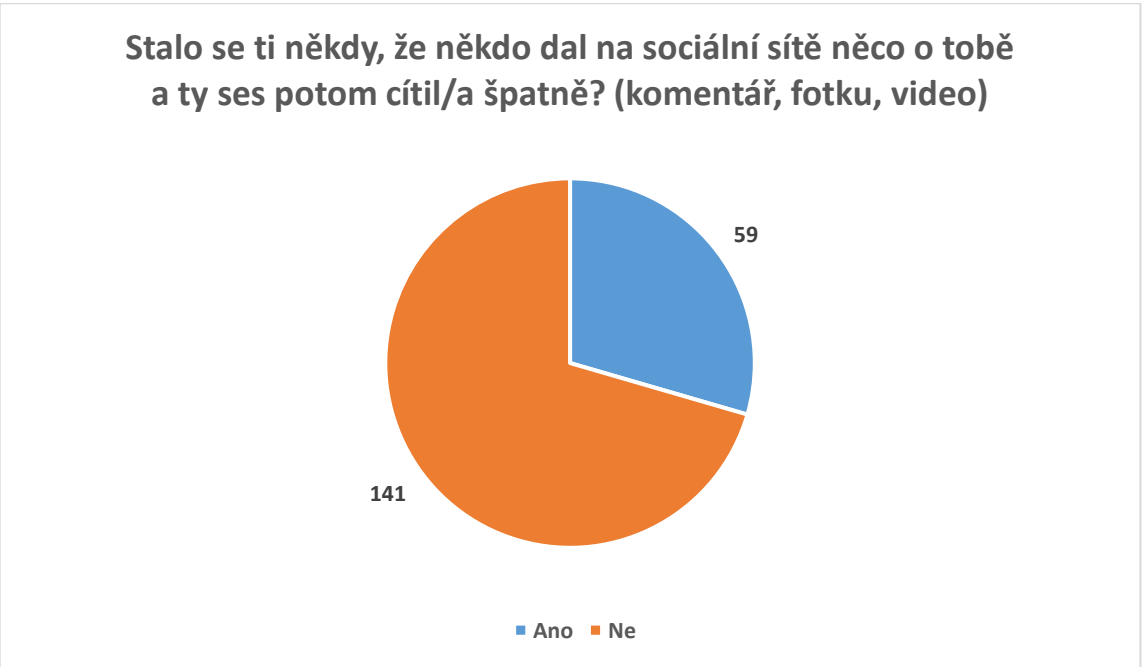
Otázka č. 18: **Stalo se ti někdy, že tě na sociální síti oslovil cizí člověk?**

Zprávy často využívají útočníci pro obtěžování nebo vyhrožování lidem. Většina dotázaných, tedy 147 (74 %), uvedlo, že je na sociální síti oslovil cizí člověk. Zbylým 53 respondentů (27 %) se taková situace nestala.

Obrázek 18 - Graf odpovědí na otázku č. 18 [vlastní]

Otázka č. 19: **Stalo se ti někdy, že někdo dal na sociální sítě něco o tobě a ty ses potom cítil/a špatně? (komentář, fotku, video)**

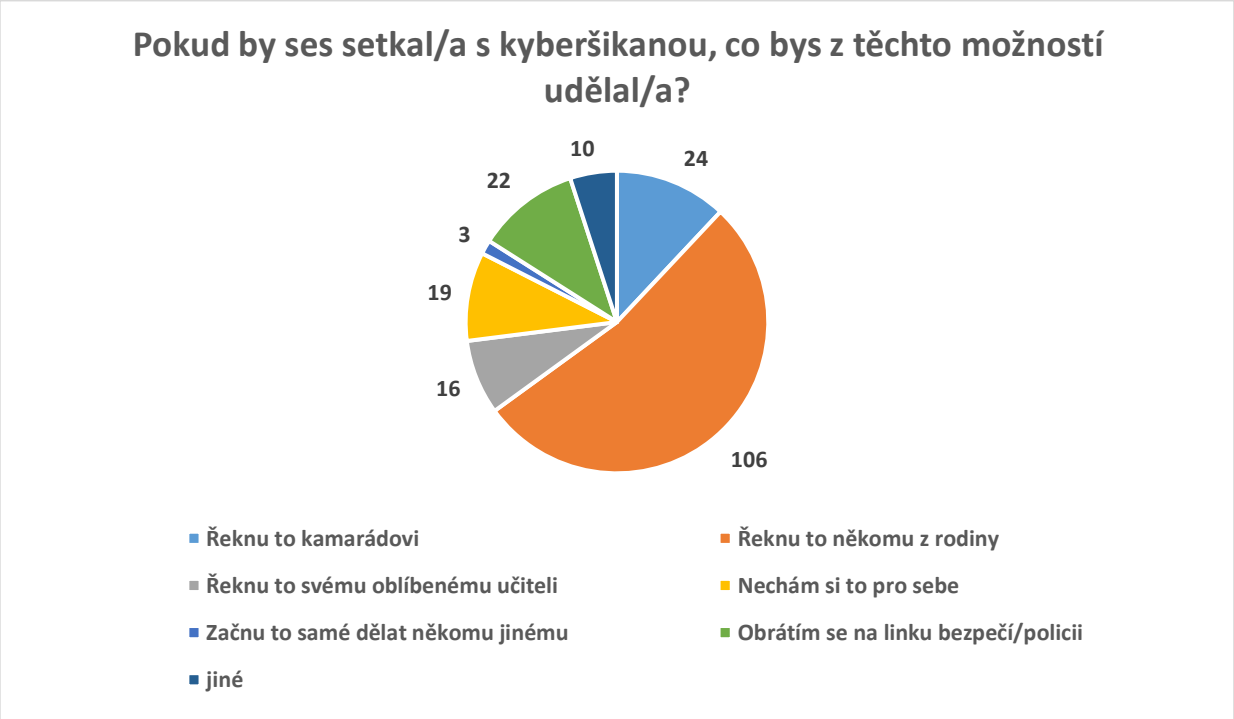
Celkem 141 respondentu (71 %) odpovědělo na tuto otázku negativně. Naopak 59 dotázaným (30 %) se někdy stalo, že dal někdo na sociální sítě něco o jejich osobě a oni se tak necítili dobře.



Obrázek 19 - Graf odpovědí na otázku č. 19 [vlastní]

Otázka č. 20: **Pokud by ses setkal/a s kyberšikanou, co bys z těchto možností udělal/a?**

Otázka zjišťovala, komu by se studenti svěřili, kdyby se stali obětí kyberšikany. Většina respondentů, tedy 106 studentů (53 %), zvolilo možnost, že by se svěřili někomu z rodiny, dále 24 (12 %) vybralo variantu říct to kamarádovi a 22 respondentů (11 %) zvolilo, že by se obrátili na linku bezpečí či policii. Naopak 19 dotazovaných (10 %) odpovědělo, že by si to nechali raději pro sebe a nikomu se nesvěřili. V 16 případech (8 %) by se studenti svěřili svému oblíbenému učiteli. Možnost jiné zvolilo 10 respondentů (5 %) a 3 respondenti (2 %) uvedli, že by to samé začali dělat někomu jinému.



Obrázek 20 - Graf odpovědí na otázku č. 20 [vlastní]

Získané odpovědi na výzkumné otázky:

Kolik dětí je seznámeno s problematikou kyberšikany?

- S pojmem kyberšikana se dle odpovědí v dotazníkovém šetření setkalo 190 dětí ze 200. Z výsledků je tedy zřejmé, že pouhých 10 respondentů není obeznámeno s problematikou kyberšikany.

Odkud se děti poprvé dozvídají o kyberšikaně?

- Na základě odpovědí na otázku č. 10 bylo zjištěno, že nejčastěji se děti o pojmu kyberšikana setkají poprvé ve škole. Dalšími možnostmi bylo například z internetu, či od rodičů.

Jaký je názor dětí na kyberšikanu?

- Z otázky č. 11 vychází, že děti berou kyberšikanu podobně jako klasickou šikanu, tedy fyzické napadání, nadávky a zesměšňování. Takto odpovědělo 109 respondentů ze 200, což je nadpoloviční většina.

Kolik dětí se již setkalo s kyberšikanou?

- Dle otázky č. 13 se s kyberšikanou setkalo 162 dětí ze 200 a 38 zatím nikoliv. Dá se tedy konstatovat, že velká část dětí se již někdy s kyberšikanou setkala.

Jaký je početní poměr mezi agresory, obětmi a přihlížejícími kyberšikaně?

- Z výsledků dotazníku vyplývá, že největší počet je přihlížejících kyberšikaně, tedy 31 z 57 respondentů, co se setkali s kyberšikanou. 25 dětí bylo obětí a pouze jeden se přiznal k roli agresora.

V případě, že by se děti setkaly s kyberšikanou, jak by se zachovaly?

- Nejčastěji by děti tuto skutečnost oznámily někomu z rodiny. Menší část by preferovala svěření se kamarádovi. 22 dětí z 200 by se obrátilo na linku bezpečí nebo policii a například 19 dětí by si, dle odpovědí na otázku č. 20 z dotazníku, nechalo tuto zkušenost pro sebe a nikomu by o tom neřeklo.

Ověření hypotéz:

1. Děti využívají sociální sítě hlavně kvůli komunikaci s přáteli.

Z odpovědí na šestou otázku v dotazníku byla tato hypotéza potvrzena. Ze 200 respondentů 150 odpovědělo právě, že nejvíce sociální sítě navštěvují kvůli komunikaci s přáteli.

2. Děti vnímají kyberšikanu stejně nebezpečnou jako klasickou fyzickou šikanu.

I tato hypotéza byla potvrzena na základě výsledků z dotazníku. 109 dětí ze 200 bere kyberšikanu stejně nebezpečnou jako klasickou šikanu.

3. Děti vědí, že ke kyberšikaně se využívají hlavně sociální sítě.

Velká část dětí odpověděla na otázku číslo 12, že nejčastěji podle nich se ke kyberšikaně využívají právě sociální sítě. Přesněji šlo o 183 respondentů ze 200. Tato hypotéza byla potvrzena.

5 MULTIKRITERIÁLNÍ HODNOCENÍ PROSTŘEDKŮ KYBERŠIKANY

Jak bylo zmíněno v teoretické části, existuje mnoho prostředků určených ke komunikaci mezi lidmi. Tyto prostředky mohou být někdy velice lehce zneužitelné ke kyberšikaně. Pro zjištění, který prostředek komunikace je z hlediska kyberšikany nejnebezpečnější, bude využito multikriteriálního hodnocení.

5.1 Použití multikriteriální hodnocení

Posouzením, zda vybraný prostředek komunikace splňuje či nesplňuje určité kritérium zjistíme, jaký druh prostředku je z hlediska možného zneužití ke kyberšikaně nejbezpečnější, a který naopak nejvíce odolný.

Pro multikriteriální hodnocení je využito vzorce pro výpočet váženého průměru.

Tento vzorec vychází z předpokladu souboru n hodnot kdy:

$$X = \{x_1, \dots, x_n\}$$

a k nim odpovídající váhy:

$$W = \{\omega_{1,} \dots, \omega_n\},$$

je dán vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$$

Dále je potřeba vybrat komparační kritéria, díky kterým se dá zjistit, jak moc daný prostředek komunikace je možný využít ke kyberšikaně, a tak k útoku na osoby. Nejdůležitějšími komparačními kritérii jsou velká rozšířenost prostředku komunikace mezi obyvatelstvem a nemožnost obrany proti útoku

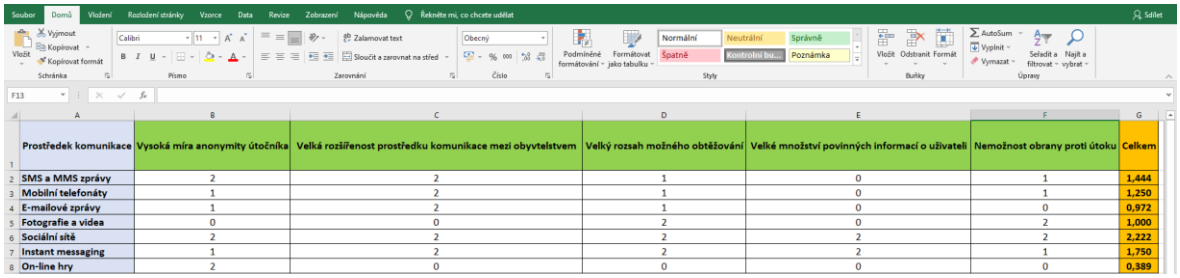
Pro jednotlivá kritéria (tedy soubory hodnot n) jsou přiděleny váhy, (v matematickém vzorci jako ω) označující důležitost tohoto kritéria. Následující tabulka zobrazuje, jaké váhy jsou kritériím přiřazeny. Čím vyšší je hodnota čísla, tím je důležitost pro dané kritérium vyšší.

Tabulka 1 - Hodnoty vah kritérií pro multikriteriální hodnocení [vlastní]

Kritérium	Přiřazená váha
Vysoká míra možné anonymity útočníka	7
Velká rozšířenost prostředku komunikace mezi obyvatelstvem	10
Velký rozsah možného obtěžování	8
Velké množství povinných informací o uživateli	5
Nemožnost obrany proti útoku	10

Dalším parametrem vzorce je x, která obsahuje číselné hodnocení prostředku komunikace. Toto hodnocení je zvoleno v rozmezí 0 – 2. Označuje se jím váha splnění kritéria, kdy 0 označuje nesplnění, hodnota 1 částečné splnění a úplné splnění hodnotou 2.

Pro usnadnění výpočtu je tento vzorec zanesen do programu Excel, díky čemuž byl vytvořen nástroj pro komparaci jednotlivých prostředků.



Prostředek komunikace	Vysoká míra anonymity útočníka	Velká rozšířenost prostředku komunikace mezi obyvtelstvem	Velký rozsah možného obtěžování	Velké množství povinných informací o uživateli	Nemožnost obrany proti útoku	Celkem
SMS a MMS zprávy	2	2	1	0	1	1,444
Mobilní telefonáty	1	2	1	0	1	1,250
E-mailové zprávy	1	2	1	0	0	0,972
Fotografie a videa	0	0	2	0	2	1,000
Sociální sítě	2	2	2	2	2	2,222
Instant messaging	1	2	2	2	1	1,750
On-line hry	2	0	0	0	0	0,389

Obr. 1 - Výpočet multikriteriálního hodnocení v Excelu [vlastní]

Takto jsou propočítány hodnoty pro každý druh prostředku komunikace a výsledná čísla byla zanesena do společné tabulky, kde jsou následně sestupně, podle získaného hodnocení, seřazeny.

5.2 Komparace jednotlivých prostředků komunikace z hlediska zneužitelnosti ke kyberšikaně

V dnešním světe se objevují nejčastěji následující druhy komunikace:

- SMS a MMS zprávy,
- mobilní telefonáty,
- e-mailové zprávy,
- sociální sítě,

- instant messaging,
- on-line hry.

Pomocí multikriteriálního hodnocení může být zjištěno který z těchto prostředků komunikace je z hlediska zneužitelnosti ke kyberšikaně nejnáchylnější. Popis multikriteriálního hodnocení a postupu, jakým způsobem se může postupovat při výpočtu hodnot multikriteriálního hodnocení jednotlivých prostředků bylo zmíněno výše. Nyní je potřeba tyto prostředky komunikace blíže popsat, podle výsledků multikriteriálního hodnocení porovnat, a tak zjistit, který prostředek

5.2.1 SMS a MMS zprávy

K výpočtu výsledného hodnocení byl použit výše zmínění vzorec:

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$$

Zde jde vidět, jakým způsobem byla získána výsledná hodnota

$$\bar{x_1} = \frac{(2 \times 7) + (2 \times 10) + (1 \times 8) + (0 \times 5) + (1 \times 10)}{7 + 10 + 8 + 5 + 10}$$

$$\bar{x_1} = 1{,}300$$

Tento vzorec byl převeden do programu Excel pro snadnější a rychlejší výpočet. Níže je uvedena tabulka, která obsahuje bodové ohodnocení, podle toho, zda prostředek komunikace splňuje (= 2), částečně splňuje (= 1), či nesplňuje (= 0) jednotlivá kritéria.

SMS a MMS zprávy, co by komunikační prostředek jsou velice rozšířeny. I když je dnes spíše nahrazují sociální sítě a instant messaging jedná se stále o velice důležitý prostředek prostřednictvím kterého lze provádět kyberšikaně útoky.

Z hlediska prvního kritéria, tedy anonymity útočníka je tento prostředek komunikace poměrně vhodným. V případě, že si útočník koupí předplacenou kartu například v trafice, není možné, jakkoliv dohledat potřebné informace k jeho dopadení.

Dále je u tohoto prostředku potřeba uvést jeho velké rozšíření mezi obyvatelstvem. Je zde tedy velká pravděpodobnost zneužití daného prostředku k účelům kyberšikany.

Tabulka 2 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

SMS a MMS zprávy				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
2	2	1	0	1
Výsledek: **1,300**				

5.2.2 Mobilní telefonáty

Podobně jako SMS a MMS zprávy i mobilní telefonáty jsou velice rozšířeným komunikačním prostředkem, který je často využíván ke kyberšikaně. Nejčastěji dochází k obtěžování a neustálému vytáčení majitele mobilního telefonu. Na rozdíl od SMS a MMS zpráv je zde alespoň šance rozpoznání hlasu útočníka a jeho anonymita se prostřednictvím tohoto prostředku snižuje.

Tabulka 3 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Mobilní telefonáty				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
1	2	1	0	1
Výsledek: **1,125**				

5.2.3 E-mailové zprávy

Využívání e-mailových zpráv ke kyberšikaně spočívá především v rozesílání obtěžujících zpráv. Ty mohou obsahovat fotky videa a zvukové nahrávky. Výhodou tohoto prostředku je poměrně lehká obrana proti útokům. Lze kdykoliv zablokovat adresu daného útočníka, a tak zabránit obtěžování.

Tabulka 4 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

E-mailové zprávy				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
1	2	1	0	0
Výsledek: **0,875**				

5.2.4 Sociální sítě

V dnešní době nejrozšířenějším a nejznámějším komunikačním prostředkem jsou právě sociální sítě. Možnost nahrávat fotky a videa na virtuální zdi je často zneužita a dochází tak k nevratnému poškození bezpečnosti soukromí osob.

Z hlediska anonymity je tento prostředek velice lákavý pro útočníky. Kdokoliv si zde může vytvořit účet s falešným jménem a fotkou. Rozsah možného obtěžování může být obří. Dostane-li se agresor k soukromým složkám oběti a dojde k odcizení různých fotek a videí, může útočník vydírat danou osobu a vyhrožovat umístěním citlivých fotek a videí na sociální sítě. Další velkou nevýhodou je poměrně špatná možnost obrany. Zablokování útočníka je sice možné, ale útočníci si často vytvářejí další profily a pokračují v agresi.

Tabulka 5 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Sociální sítě				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
2	2	2	2	2
Výsledek: **2,000**				

5.2.5 Instant messaging

Tento druh komunikace často využívá propojení s některými sociálními sítěmi. Jedná se zde, ale většinou s soukromou komunikaci mezi dvěma, či více osobami. V případě kyberšikany se zde nejvíce využívají obtěžující zprávy, nadávky či vyhrožování. Z hlediska možné obrany existuje možnost zablokování daného agresora a tím zabránění dalším útokům.

Tabulka 6 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

Instant messaging				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
1	2	2	2	1
Výsledek: **1,575**				

5.2.6 On-line hry

Jedná se o specifický komunikační prostředek, který je využíván při hraní on-line her. Primárně slouží ke komunikace mezi jednotlivými hráči. Z hlediska kyberšikany může být zneužit pro rozesílání obtěžujících zpráv a urážek, či zesměšňování druhých hráčů. Anonymita uživatelů tohoto prostředku je na velké úrovni, ovšem rozšířenost je velice malá.

Tabulka 7 - Ohodnocení jednotlivých kritérií a výsledné hodnocení [vlastní]

On-line hry				
Vysoká míra možné anonymity útočníka	**Velká rozšířenost prostředku komunikace mezi obyvatelstvem**	**Velký rozsah možného obtěžování**	**Velké množství povinných informací o uživateli**	**Nemožnost obrany proti útoku**
2	0	0	0	0
Výsledek: **0,350**				

5.3 Výsledky multikriteriálního hodnocení

Na základě ohodnocení daných kritérií u jednotlivých komunikačních prostředků, bylo získáno číselné hodnocení, které bude v této podkapitole vyhodnoceno a vzestupně seřazeno.

Tabulka 8 – Výsledky multikriteriálního hodnocení [vlastní]

Prostředek komunikace a pozice	Hodnocení
1. Sociální sítě	2,000
2. Instant messaging	1,575
3. SMS a MMS zprávy	1,300
4. Mobilní telefonáty	1,125
5. E-mailové zprávy	0,875
6. On-line hry	0,350

Na posledním místě se umístila komunikace prostřednictvím on-line her. Z hlediska zneužitelnosti ke kyberšikaně je tedy nejvíce v bezpečí, a to z několika důvodů:

- Rozšířenost tohoto komunikačního prostředku je velice malá.
- Rozsah obtěžování je na nízké úrovni.
- Vyžaduje minimální povinné informace o uživateli.
- Obrana proti tomuto druhu kyberšikany je poměrně dobrá a lehká.

Jak jde v této tabulce vidět, na prvním místě se umístila komunikace prostřednictvím sociálních sítí. Ze všech prostředků komunikace dostal nejvyšší hodnocení.
Důvody, proč je tento prostředek nejnebezpečnější jsou:

- Velká možnost anonymity útočníka.
- Obří rozšířenost tohoto komunikačního prostředků mezi obyvateli.
- Velký rozsah možného obtěžování.
- Velké množství povinných informací o uživateli.
- Malá možnost obrany proti útoku.

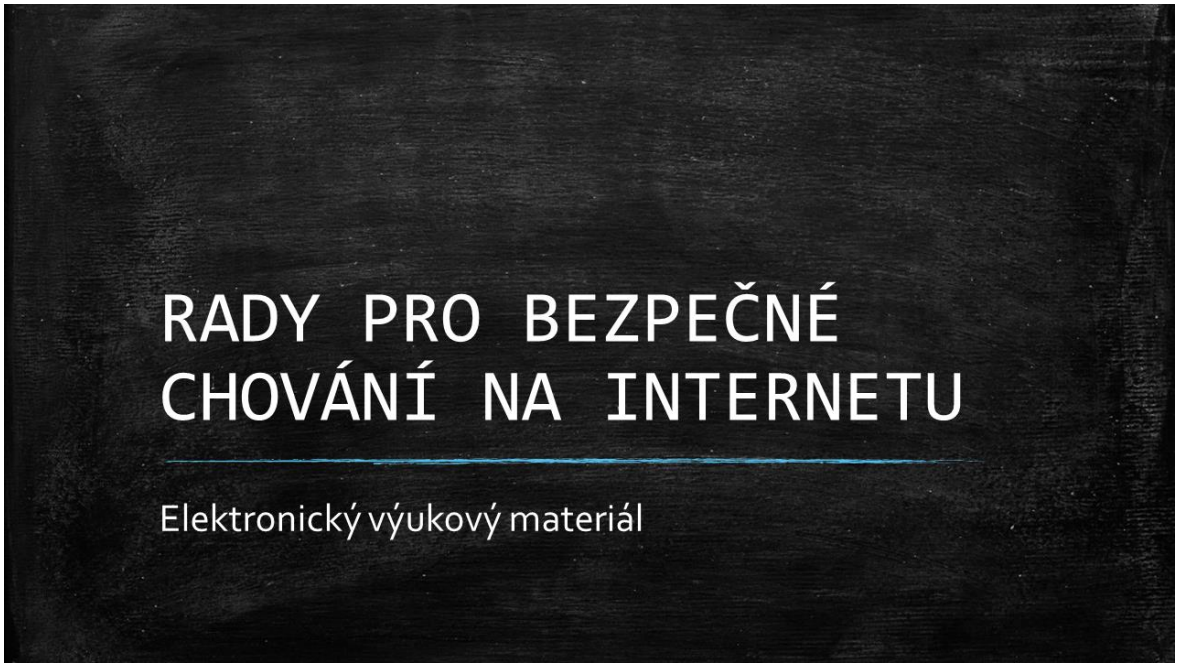
6 NÁVRH OPATŘENÍ NA VYTVOŘENÍ VÝUKOVÉHO MATERIÁLU PODPORUJÍCÍHO BEZPEČNOST NA INTERNETU

Jak bylo zmíněno v kapitolách výše, existuje mnoho dětí, co se již s kyberšikanou setkalo. Stále je ale mnoho těch, které tento pojem znají, ale nevědí, jak se kyberšikaně vyhnout. Jako ideální nástroj pro boj s kyberšikanou se nabízí výukový materiál určený pro předávání informací, jak se bezpečně pohybovat na internetu. Takovýto typ materiálu bude níže navrhnut.

6.1 Elektronický výukový materiál

V dotazníkovém šetření bylo zjištěno, že nejčastějším prostředkem komunikace využívaným ke kyberšikaně jsou sociální sítě. Tato skutečnost byla potvrzena díky využití multikriteriálního hodnocení, kde z mnoha komunikačních prostředků vyšly právě sociální sítě jako nejnebezpečnější.

V návaznosti na všechny informace a data získaná z předchozích kapitol, je potřeba vytvořit určitý výukový materiál podporující internetovou bezpečnost v oblasti kybernetické bezpečnosti. Vzhledem k tomu, že je tento materiál určen pro využívání ve školních zařízeních, zdá se být elektronická forma jako ideální. Elektronický výukový materiál je vytvořen jako prezentace, která obsahuje devět základních pravidel pro bezpečné chování na internetu. Každé pravidlo je následně blíže popsáno. Níže na obrázku číslo 21 jde již vidět úvodní snímek prezentace.



Obrázek 21 – Úvodní snímek prezentace [vlastní]

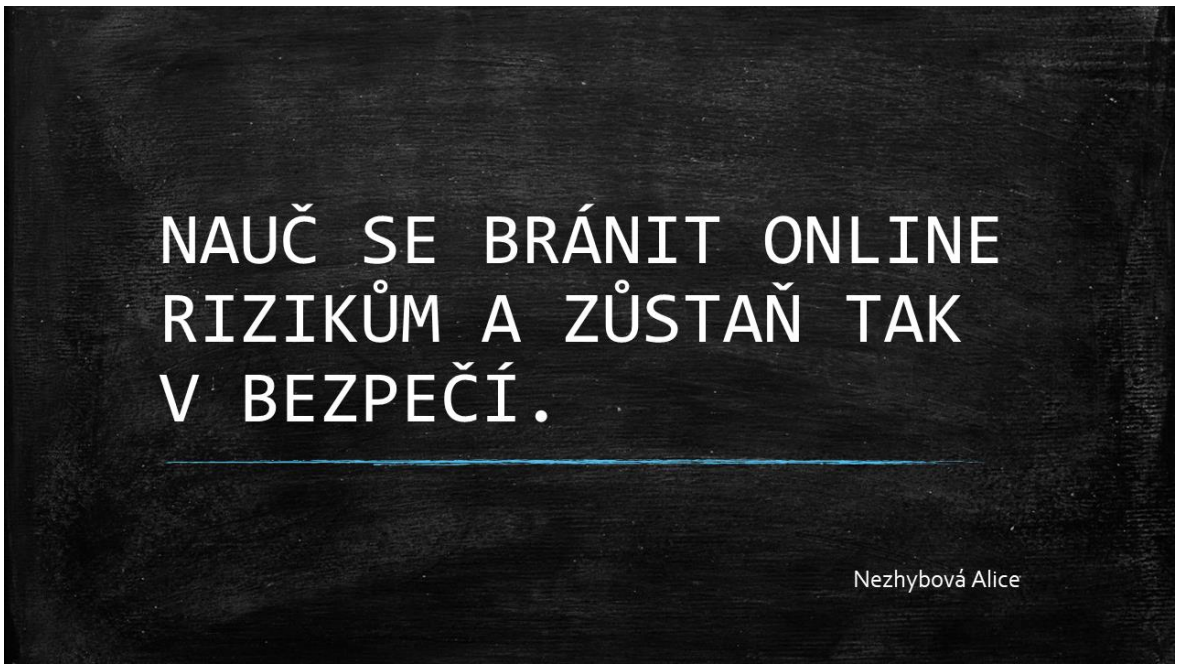
Na obrazu číslo 22 lze vidět, jak by vypadá pravidlo týkající se internetové bezpečnosti. Vzhled pravidel je heslovitý, tedy co nejkratší text (ideálně jedno slovo), které se dobře pamatuje.

Obrázek 22 – První rada v prezentaci [vlastní]

V několika bodech, jak lze vidět na obrázku číslo 23, je popsáno pravidlo. Obsahem těchto snímků je vždy velice přímí a reálný popis, jak se bezpečně pohybovat na internetu a vyhnout se kyberšikaně. Pro co nejlepší důraz, jsou využity i rozkazovací věty.

Obrázek 23 – Popis první rady [vlastní]

Obrázek číslo 24 již obsahuje vzhled závěrečného snímku s poslední radou a jménem autorky elektronického výukového materiálu.



Obrázek 24 – Závěrečný snímek [vlastní]

6.2 Informační plakát pro bezpečný pohyb na internetu

Další možností, jak zvýšit povědomí všech lidí o problematice bezpečného pohybu na internetu a kyberšikaně, je vytvoření plakátu obsahujícího základní pravidla, kterých se člověk musí držet, chce-li zůstat na internetu v bezpečí. Níže na obrázku číslo 25 lze již vidět návrh možné podoby takovéto informačního plakátu.

Obrázek 25 Informační plakát [vlastní]

ZÁVĚR

Z hlediska aktuálnosti se internetová bezpečnost společně s kyberšikanou řadí mezi vysoce živá témata, o kterých se v dnešní době neustále mluví. Společně s rozvojem moderní techniky a mobilních zařízení dochází čím dál častěji k jejich zneužití, a to především k provozování kyberšikany. Bohužel, nejčastějšími cíli těchto útoků se stávají děti ve školním věku.

Právě kvůli velké zranitelnosti dětí prostřednictvím kyberšikany, je potřeba se tomuto tématu více věnovat a snažit se implementovat opatření snižující pravděpodobnost výskytu kyberšikany, a to především na školách.

Bakalářská práce byla zaměřena na internetovou bezpečnost, a především problematiku kyberšikany. V teoretické části se práce zabývá definicí sociálních sítí, a to hlavně z hlediska historie tohoto komunikačního prostředku a výčtem typů uživatelů pohybujících se na sociálních sítích. Dále práce vysvětluje, jaké jsou druhy sociálních sítí a jaké jsou základní znaky těchto druhů. Nedílnou součástí teoretické části je samotná definice a seznámení s pojmem kyberšikana. Tato problematika byla v práci rozebrána z hlediska historie a práva. Dále byla provedena komparace s klasickou šikanou a popsány jednotlivé druhy kyberšikany společně s prostředky k tomu používanými.

Praktická část práce se zaměřila na analýzu vztahu dětí k problematice kyberšikany. K této analýze bylo využito především dotazníkového šetření, na které odpovědělo 200 dětí základních škol. Bylo tak získáno mnoho reálných informací, které následně odpověděly na předem stanovené výzkumné otázky a hypotézy. Na základě odpovědí z dotazníku bylo dále v práci provedeno multikriteriální hodnocení pro výběr nejnebezpečnějšího komunikačního prostředku z hlediska kyberšikany. Zde bylo zjištěno, že nejnebezpečnější z hlediska kyberšikany je právě sociální sít, jakožto komunikační prostředek využívaný dětmi. Na základě získaných informací byl v práci navržen výukový materiál, a to v podobě elektronické prezentace. Tento elektronický výukový materiál slouží jako prostředek pro získání základních informací o kyberšikaně a poučení o základních pravidlech pro bezpečný pohyb na internetu. Pro lepší informovanost a zvýšení povědomí o problematice internetové bezpečnosti a kyberšikany byl vytvořen plakát obsahující základní pravidla pro bezpečný pohyb na internetu.

Cílem této práce bylo provést dotazníkový průzkum v oblasti kyberšikany a následně zpracovat výukový materiál podporující internetovou bezpečnost. Cíl práce byl splněn.

SEZNAM POUŽITÉ LITERATURY

BEDNÁŘ, Vojtěch, 2011. *Marketing na sociálních sítích: Prosaďte se na Facebooku a Twitteru*. Brno: Computer Press. ISBN 978-80-251-3320-0.

Černá, A. (Ed.) Dědková, L., Macháčková, H., Ševčíková, A., Šmahel, D., 2013. *Kyberšikana: Průvodce novým fenoménem*. Praha: Grada Publishing. ISBN 978-80-247-4577-0.

ČESKO, 2009. *Zákon č. 40/2009 Sb.: Zákon trestní zákoník*. In: Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-40

CLAYPOOLE, Ted a Theresa PAYTON, 2017. *Protecting your internet identity: are you naked online?* Updated edition. Lanham: Rowman Littlefield, ISBN 9781442265394.

DOBOSIOVÁ, Martina, 2015. *Kategorie současných sociálních sítí a aktuální sociální sítě* [online]. [cit. 2021-03-30]. Dostupné z: https://clanky.rvp.cz/clanek/k/z/20145/KATEGORIE-SOUCASNYCH-SOCIALNICH-SITI-A-AKTUALNI-SOCIALNI-SITE.html/

DOČEKAL, Daniel, 2012. *Typologie sociálních aktivit uživatelů – Social Technographics Ladder* [online]. [cit. 2021-03-29]. Dostupné z: https://pooh.cz/2012/01/05/typologie-socialnich-aktivit-uzivatelu-social-technographics-ladder/

Flickr [online], 2021. [cit. 2021-03-30]. Dostupné z: https://www.flickr.com/

Global social media adoption in 2011 [online], 2012. [cit. 2021-03-29]. Dostupné z: http://www.mindjumpers.com/global-social-media-adoption-2011/

HOLLÁ, Katarína, 2013. *Kyberšikana*. Bratislava: Iris. ISBN 978-80-8153-011-1.

HULANOVÁ, Lenka, 2012. *Internetová kriminalita páchaná na dětech*. Praha: Stanislav Juhaňák – Triton. ISBN 978-80-7387-545-9.

JELIČ, Pavel, 2021. *Clubhouse: Co to je, jak se do něj dostat a proč by vás mohl bavit?* [online]. [cit. 2021-03-30]. Dostupné z: https://www.letemsvetemapplem.eu/2021/01/27/clubhouse-co-to-je-jak-se-do-nej-dostat-a-proc-by-vas-mohl-bavit/

KOVÁŘOVÁ, Pavla, 2019. *Informační bezpečnost žáků základních škol: lekce v knihovnách.* Brno: Filozofická fakulta, Masarykova univerzita, 261 s. Opera Facultatis philosophicae Universitatis Masarykianae. ISBN 9788021092709.

KOŽÍŠEK, Martin a Václav PÍSECKÝ, 2016. *Bezpečně na internetu: průvodce chováním ve světě online*. Praha: Grada Publishing. ISBN 978-80-247-5595-3.

Kyberšikana [online], 2019. [cit. 2021-03-30]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/32-sikana-v-mobilnich-telefonech-outing-happy-slapping-a-spol

Last.fm [online], 2021. [cit. 2021-03-30]. Dostupné z: https://www.last.fm/

MySpace [online], 2021. [cit. 2021-03-30]. Dostupné z: https://myspace.com/

Přehled sociálních sítí 2019: Znáte je všechny? [online], 2019. [cit. 2021-03-29]. Dostupné z: https://bloggersre.com/prehled-socialnich-siti-2019-znate-je-vsechny/

ROGERS, Vanessa, 2011. *Kyberšikana: Pracovní materiály pro učitele a žáky i studenty*. Praha: Portál. ISBN 978-80-7367-984-2.

Sociální sítě a jejich vývoj – pohled do historie. Objevit.cz [online]. 2013 [cit. 2021-03-28]. Dostupné z: https://www.objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280

Sociální sítě: Největší sociální sítě [online], 2020. [cit. 2021-03-29]. Dostupné z: https://sitevhrsti.cz/socialni-site/

Sociální sítě: Přehled sociálních sítí [online], 2013. [cit. 2021-03-30]. Dostupné z: http://facebook-profily.czech-this.com/socialni-site/

ŠAMBERGEROVÁ, Barbora, 2020. *Kyberšikana jako riziko virtuálního prostředí* [online]. [cit. 2021-03-30]. Dostupné z: https://medium.com/edtech-kisk/kyber%C5%A1ikana-jako-riziko-virtu%C3%A1ln%C3%ADho-prost%C5%99ed%C3%AD-619bbb5bcd5b#_ftn12

ŠEVČÍKOVÁ, Anna et al., 2014. *Děti a dospívající online: Vybraná rizika používání internetu*. Praha: Grada Publishing. ISBN 978-80-247-5010-1.

Tinder [online], 2021. [cit. 2021-03-30]. Dostupné z: https://tinder.com

Teenageři a komunikace na internetu [online], 2020. [cit. 2021-03-29]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace

TŮMOVÁ, Štěpánka, 2012. *Typologie uživatelů: sociální sítě a knihovny* [online]. [cit. 2021-03-29]. Dostupné z: http://eprints.rclis.org/17557/1/Tumova%20Stepanka%20-%20recenzovany%20clanek%20-%20Typologie%20uzivatelu%20socialni%20site%20a%20knihovny.pdf

VAŠUTOVÁ, Mária, 2010. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě. ISBN 978-80-7368-858-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

§	Paragraf
č.	Číslo
čl.	Článek
např.	Například
Sb.	Sbírka

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Internetová bezpečnost

Dobrý den,

jmenuji se Alice Nezhybová a jsem studentkou na Univerzitě Tomáše Bati. Studuji na Fakultě logistiky a krizového řízení v Uherském Hradišti, obor Ochrana obyvatelstva. V rámci své bakalářské práce na téma "Internetová bezpečnost" zpracovávám dotazníkové šetření. Dotazník je zcela anonymní.

Děkuji Vám za Vaši ochotu a čas, který jste dotazníku věnovali.

1. Jaké je tvé pohlaví?
   a) dívka
   b) chlapec

2. Jaký je tvůj věk?
   a) 10-12
   b) 13-15
   c) 15+

3. Máš založený účet na nějaké sociální síti?
   a) ano
   b) ne

4. Na které sociální síti máš založený účet?
   a) Facebook
   b) Instagram
   c) Snapchat
   d) Twitter
   e) YouTube

f) TikTok

g) nikde

h) jiné

5. Kterou sociální síť využíváš nejčastěji?

a) Facebook

b) Instagram

c) Snapchat

d) Twitter

e) YouTube

f) TikTok

g) žádnou

h) jiné

6. Z jakého důvodu sociální sítě navštěvuješ?

a) komunikace s přáteli

b) seznámení s novými lidmi

c) prohlížení příspěvků

d) sdílení fotek

e) vyhledávání informací

f) sledování známých lidí

7. Kolik času na nich denně trávíš?

a) méně než 1 hodinu

b) 1 hodinu

c) 1-2 hodiny

d) 2-3 hodiny

e) 3 a více hodin

8. Jak si chráníš svůj účet?

a) je zabezpečen pouze pro mé přátelé

b) nereaguji na zprávy a žádosti o přátelství od cizích lidí

c) nechráním

d) nemám účet

e) jiné

9. Víš, co znamená pojem kyberšikana?

a) ano

b) ne

10. Kde ses poprvé s pojmem kyberšikana setkal/a?

a) ve škole

b) od rodičů

c) na internetu z televize

d) nesetkal/a

11. Co je podle tebe nebezpečnější?

a) klasická šikana (fyzické napadání a zesměšňování před ostatními)

b) kyberšikana (psychické napadání a zesměšňování pomocí informačních a komunikačních technologií)

c) oboje stejně

12. Jaké prostředky podle tebe kyberšikana používá?

d) SMS a MMS zprávy

e) e-maily

f) sociální sítě

g) chat

h) on-line hry

13. Setkal/a ses někdy s kyberšikanou?

a) ano

b) ne

14. Pokud ano, byl/a jsi:

a) oběť

b) agresor

c) přihlížející

15. Pokud ses setkal/a nebo setkáváš s kyberšikanou, tak jakého typu?

a) napadáním nebo urážením

b) ponižováním nebo zesměšňováním

c) zastrašováním nebo vyhrožováním

d) zneužitím tvého účtu

e) nesetkal/a

16. Pokud ses setkal/a nebo setkáváš s kyberšikanou, tak jak často?

a) jednou/dvakrát

b) jednou/dvakrát ročně

c) jednou/dvakrát měsíčně

d) každý týden

e) každý den/skoro každý den

f) nesetkal/a

17. Na jaké sociální síti ses setkal/anebo setkáváš s kyberšikanou?

a) Facebook

b) Instagram

c) Snapchat

d) Twitter

e) YouTube
f) TikTok
g) Nesetkal/a

18. Stalo se ti někdy, že tě na sociální síti oslovil cizí člověk?

a) ano
b) ne

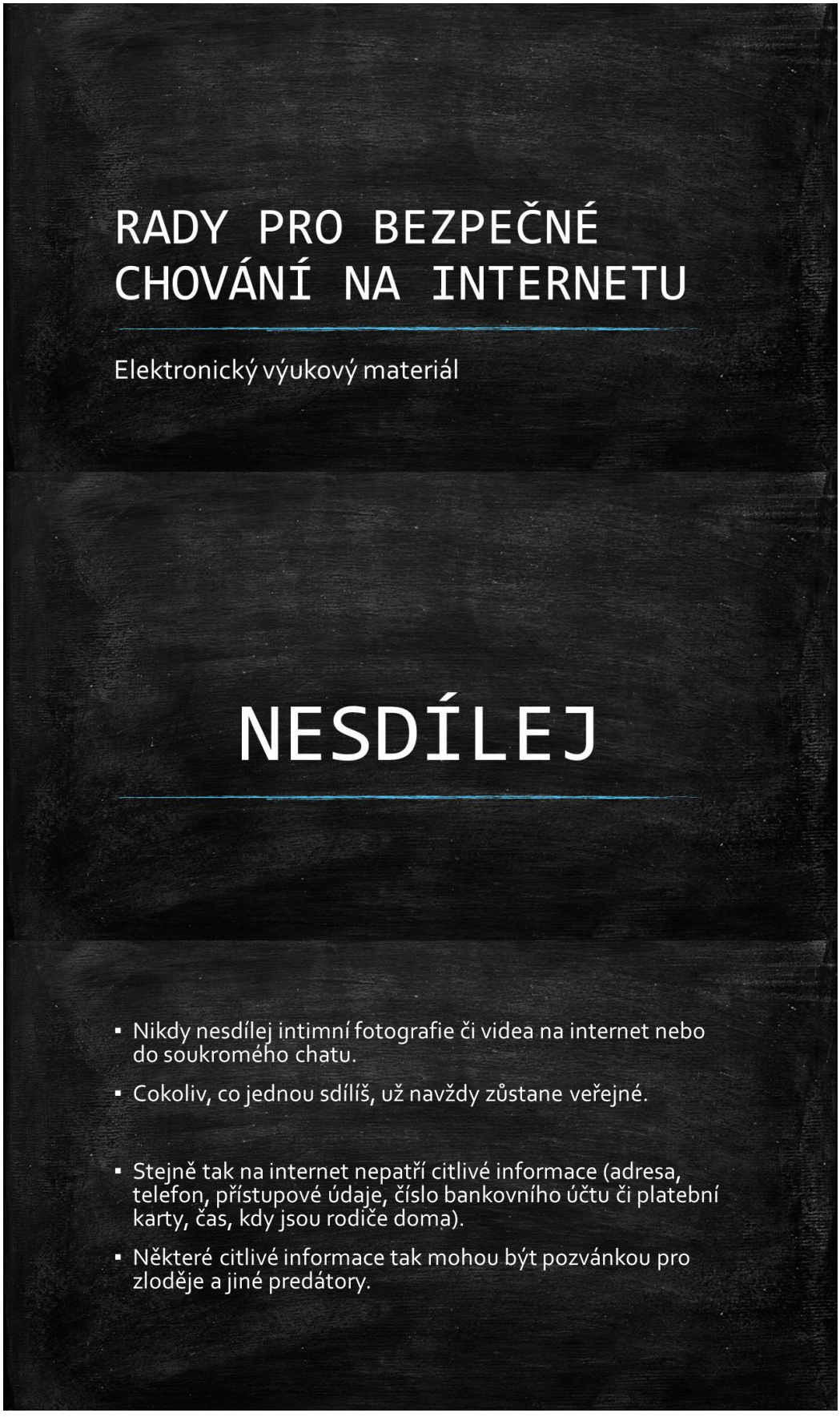
19. Stalo se ti někdy, že někdo dal na sociální sítě něco o tobě a ty ses potom cítil/a špatně? (komentář, fotku, video)

a) ano
b) ne

20. Pokud by ses setkal/a s kyberšikanou, co bys z těchto možností udělal/a?

a) řeknu to kamarádovi
b) řeknu to někomu z rodiny
c) řeknu to svému oblíbenému učiteli
d) nechám si to pro sebe
e) začnu to samé dělat někomu jinému
f) obrátím se na linku bezpečí/policii
g) jiné

PŘÍLOHA P II: ELEKTRONICKÝ VÝUKOVÝ MATERIÁL



SVĚŘUJ SE

- Neboj se svěřit rodičům, učitelům, napsat či zavolat na linku bezpečí, pokud ti na síti někdo vyhrožuje, obtěžuje tě nebo zastrašuje.

NEMAŽ

- Pokud tě někdo na síti vydírá, udělej si důkazy.
- Osobu si neblokuj, nemaž zprávy, ale naopak si vše ulož a zálohuj.
- Potom s tím jdi za někým, komu věříš.

NEFOŤ POD PEŘINOU

- Nefoť se nebo nenatáčej u jakéhokoliv erotického chování.
- Můžeš se tak stát tvůrcem, případně distributorem dětské pornografie, což je do 18 let trestné!

POZOR NA (NE)PŘÍTELE

- Pokud si zakládáš nebo máš profil na sociální síti, nastav si soukromí.
- Promysli si, co mají vidět všichni a co jen tví přátelé.
- Než si někoho přidáš do přátel, trochu si ho prolustruj.
- O kom vůbec nic nevíš, nepřidávej si ho!

NERISKUJ

- Nikdy nechoď na schůzku s někým, koho znáš pouze z internetu.
- Je vysoké riziko, že narazíš právě na predátora.
- Pokud na takovou schůzku půjdeš, řekni to někomu!
- Případně si domluv schůzku ve dne a na veřejném místě.
- Naopak nikdy si nedomlouvej schůzku na neznámém místě a nikdy k nikomu nesedej do auta!

POZOR NA LICHOTKY

- Přehnané lichotky jsou jen zástěrkou, abys druhému uvěřil a následně z tebe vytáhl fotky, videa nebo osobní údaje, které proti tobě může kdykoliv použít.

ZABEZPEČ

- Chraň si svá data jak v mobilu, tak i v počítači.
- Pokud to jde, nastav si na sociálních sítích i v e-mailu dvoufázové ověření.
- Neotvírej přílohu zprávy z neznámé adresy, pořiď si antivir.

POZNEJ FAKE „KAMARÁDA“

- Takový fake „kamarád“ často hledá kamaráda/kamarádku na pokec.
- Ale zároveň se za profilem krásné holky nebo kluka může skrývat „úchyl“, který z vás chce vytáhnout fotografie a videa.
- Profil podvodníka může mít málo nebo naopak hodně přátel, nemusí tam mít žádné své fotografie a může být založený teprve pár dnů.
- Dávej si pozor na pochybné profily!

NAUČ SE BRÁNIT ONLINE RIZIKŮM A ZŮSTAŇ TAK V BEZPEČÍ.

Nezhybová Alice