

Česká zemědělská univerzita v Praze

Institut vzdělávání a poradenství

Katedra celoživotního vzdělávání a podpory studia



**Rizika a hrozby využívání digitálních
technologií mládeží**

Bakalářská práce

Autor: Veronika Fousková

Vedoucí práce: Ing. Lukáš Herout, Ph.D.

2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Veronika Fousková

Poradenství v odborném vzdělávání

Název práce

Rizika a hrozby využívání digitálních technologií mládeží

Název anglicky

Risks and Threats of Using Digital Technologies for Youth

Cíle práce

Cílem bakalářské práce je zmapovat rizika a hrozby využívání digitálních technologií mládeží a na základě výsledků z realizovaného dotazníkového šetření navrhnout soubor konkrétních opatření a doporučení pro rodiče dětí a to ve formě vzdělávacího programu/kurzu.

Metodika

Teoretická část práce bude zaměřena na problematiku rizik a hrozeb spojených s využíváním digitálních technologií mládeží. To bude provedeno zejména s využitím analyticko-syntetických a induktivně-deduktivních metod nad dostupnými primárními a sekundárními prameny.

V praktické části práce bude provedena analýza současného stavu a to primárně s využitím dotazníkového šetření. V souladu s teoretickou částí práce a výsledky šetření bude navržen vzdělávací program/kurz zaměřený na edukaci rodičů ve výše uvedené oblasti. V shodě s teoretickou částí budou využity zejména analyticko-syntetické a induktivně-deduktivní metody.

Doporučený rozsah práce

Dle pravidel pro psaní bakalářských prací

Klíčová slova

Vzdělávání; digitální technologie; rizika; hrozby

Doporučené zdroje informací

- BLINKA, Lukáš. Online závislosti: jednání jako droga? : online hry, sex a sociální sítě : diagnostika závislosti na internetu : prevence a léčba. Praha: Grada, 2015. Psyché. ISBN 978-80-210-7975-5.
- FOX, Richard. Information technology: an introduction for today's digital world. Boca Raton: CRC Press, c2013. ISBN 978-1-4665-6828-0.
- KOHOUT, Roman a Radek KARCHŇÁK. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.
- KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
- KOPECKÝ, Kamil. Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming: The strategies of child manipulation in online environments with a focus on cyber grooming. *Pediatrica pre prax*. Bratislava: SOLEN, 2016, 17(2). ISSN 1336-8168.

Předběžný termín obhajoby

2018/19 LS – IVP

Vedoucí práce

Ing. Lukáš Herout, Ph.D.

Garantující pracoviště

Katedra celoživotního vzdělávání a podpory studia

Elektronicky schváleno dne 8. 3. 2019

PhDr. Lucie Smékalová, Ph.D. et Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 9. 3. 2019

Ing. Karel Němejc, Ph.D.

Pověřený ředitel

V Praze dne 25. 03. 2019

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Rizika a hrozby využívání digitálních technologií mládeží“ vypracovala samostatně a citovala jsem všechny informační zdroje, které jsem v práci použila a které jsem rovněž uvedla na konci práce v seznamu použitých informačních zdrojů.

Jsem si vědoma, 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, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

Jsem si vědoma, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek obhajoby.

Svým podpisem rovněž prohlašuji, že elektronická verze práce je totožná s verzí tištěnou a že s údaji uvedenými v práci bylo nakládáno v souvislosti s GDPR.

V Praze dne

.....
(Podpis)

PODĚKOVÁNÍ

Touto cestou bych chtěla především poděkovat Ing. Lukáši Heroutovi, Ph.D., za odborné vedení práce, za konzultaci a připomínky v průběhu zpracování této bakalářské práce.

NÁZEV: Rizika a hrozby využívání digitálních technologií mládeží

AUTOR: Veronika Fousková

KATEDRA: Katedra celoživotního vzdělávání a podpory studia

VEDOUcí PRÁCE: Ing. Lukáš Herout, PhD.

ABSTRAKT: Bakalářská práce pojednává o vlivu digitálních technologií na dospívající mládež. Teoretická část práce je zaměřena na využívání digitálních technologií, sociálních sítích a popisuje jednotlivá rizika s nimi spojená. Tato část práce rozebírá a porovnává odbornou literaturu. Praktická část práce se zabývá výzkumem, který zjišťuje, jak často a k čemu mládež využívá digitální technologie a jestli už se někdy setkala s vybranými rizikovými situacemi. K tomu navazuje výzkum povědomí rodičů o těchto faktech. K získání informací bylo využito empirické šetření, dotazníková výzkumná metoda. Z porovnání výsledků empirického šetření s teoretickými poznatky byl navržen kurz pro rodiče, seznamující je s hrozbami využívání digitálních technologií a bezpečností na digitálních zařízeních, obohacen o praktickou část, kde si účastníci budou učit zabezpečit digitální zařízení a internetové stránky.

Klíčová slova: Vzdělávání, digitální technologie, rizika, hrozby

TITLE: Risks and Threats of Using Digital Technologies for Youth

AUTHOR: Veronika Fousková

DEPARTMENT: Department of Professional and Personal Development

SUPERVISOR: Ing. Lukáš Herout, PhD.

ABSTRACT: Bachelor thesis deals with the influence of digital technologies on adolescents. The theoretical part is focused on the use of digital technologies, social networks and describes the risks associated with them. This part of the thesis analyzes and compares professional literature. The practical part of the thesis deals with research that investigates how often and why youth uses digital technology and if they ever have encountered selected risk situations. This is followed by research on parents awareness of these facts. An empirical survey, a questionnaire research method, was used to obtain information. Comparing the results of the empirical survey with theoretical knowledge, was introduced a course for parents to familiarize them with the threats of using digital technology and security on digital devices, enriched with a practical part where participants will learn to secure digital devices and websites.

KEYWORDS: Education, digital technology, risks, threats

Obsah

ÚVOD	10
1 CÍL A METODIKA PRÁCE	11
2 ÚVOD DO TEORETICKÉ ČÁSTI	12
2.1 PUBESCENCE A ADOLESCENCE	12
2.2 DIGITÁLNÍ TECHNOLOGIE	13
2.3 DIGITÁLNÍ ZAŘÍZENÍ	13
2.3.1 <i>Počítač</i>	14
2.3.2 <i>Smartphone</i>	14
2.4 INTERNET	14
2.5 SOCIÁLNÍ SÍŤ	15
2.5.1 <i>Facebook</i>	17
2.5.2 <i>Instagram</i>	17
2.5.3 <i>Tinder</i>	18
2.5.4 <i>YouTube</i>	19
2.5.5 <i>Snapchat</i>	19
2.6 ONLINE HRY	19
3 HROZBY A RIZIKA VYUŽÍVÁNÍ DIGITÁLNÍCH TECHNOLOGIÍ	21
3.1 BEHAVIORÁLNÍ ZÁVISLOST	21
3.2 KYBERSTALKING	22
3.3 SEXTING	23
3.4 KYBERŠIKANA	24
3.5 KYBERGROOMING	25
3.6 HOAX	26
3.7 PHISHING	26
4 BEZPEČNOST NA INTERNETU	27
4.1 ZACHÁZENÍ S OSOBNÍMI ÚDAJI	27
4.2 OCHRANA HESLA	28
4.3 OVĚŘENÍ IDENTITY	28
4.4 BLOKACE NEVHODNÉHO OBSAHU	29
4.5 GOOGLE FAMILY LINK	29
5 TVORBA VZDĚLÁVACÍ AKCE	30
5.1 ANALÝZA A IDENTIFIKACE VZDĚLÁVACÍCH POTŘEB	30
5.2 INTERPRETACE VÝSLEDKŮ ANALÝZY VZDĚLÁVACÍCH POTŘEB	30
5.3 FORMY A METODY VZDĚLÁVÁNÍ	31
5.4 VÝBĚR LEKTORŮ A MÍSTA KONÁNÍ	31
5.5 MATERIÁLNÍ A TECHNICKÉ ZAJIŠTĚNÍ	31
5.6 FINANČNÍ PLÁN	31
5.7 ZPŮSOB EVALUACE	31
6 VÝZKUMNÉ ŠETŘENÍ	33

6.1	POUŽITÁ METODA EMPIRICKÉHO ŠETŘENÍ.....	33
6.2	ZPRACOVÁNÍ A ANALÝZA DAT	34
6.2.1	<i>Základní údaje o respondentech</i>	34
6.2.2	<i>Digitální zařízení</i>	35
6.2.3	<i>Jak rodiče znají youtubery a hry</i>	37
6.2.4	<i>Sociální síť</i>	38
6.2.5	<i>Hrozby a rizika využívání digitálních technologií</i>	40
6.2.6	<i>Omezování aktivit v oblasti digitálních technologií</i>	41
6.2.7	<i>Bezpečnost využívání digitálních technologií</i>	42
6.2.8	<i>Kurz pro rodiče z oblasti digitálních technologií</i>	42
6.3	ZÁVĚR VÝZKUMNÉHO ŠETŘENÍ.....	43
7	NÁVRH VZDĚLÁVACÍHO PROGRAMU	45
7.1	PŘEDSTAVENÍ KURZU	45
7.2	CÍLOVÁ SKUPINA.....	45
7.3	CÍLE KURZU	46
7.4	FORMY A METODY VEDENÍ KURZU.....	46
7.5	DISeminACE KURZU	46
7.6	OBSAH KURZU.....	46
7.7	REALIZACE KURZU	49
7.8	EVALUACE KURZU	50
	ZÁVĚR	51
	SEZNAM LITERATURY:	52
	SEZNAM TABULEK:	56
	SEZNAM GRAFŮ:	57
	SEZNAM PŘÍLOH:.....	58

Úvod

Dnešní mládež tráví několik hodin denně aktivitami v oblasti digitálních technologií. Je zcela běžné, že dítě má od vstupu na ZŠ vlastní mobilní telefon ne-li další digitální zařízení. V tomto věku už děti mívají zkušenosti s ovládáním televizorů nebo tabletů, které jim rodiče v brzkém věku půjčují, aby je zabavili. Mobilní telefon je pro dnešní děti zcela běžnou součástí života. Není dne, kdy by děti nevyužily nějakého digitálního zařízení. Vypadá to, že na tom není nic špatného, neboť digitální technologie přece život ulehčují. Pomocí digitálních technologií si lze během chvíle vyhledat cestu domů, informace, které člověka zrovna zajímají nebo se během vteřiny dá spojit s člověkem na druhé straně zeměkoule.

Ovšem digitální technologie se nemůže spojovat pouze s pozitivy. Ne každý si uvědomuje, že digitální technologie neulehčují jenom běžný život, ale také napomáhají třeba podvodníkům nebo zlodějům. Bakalářská práce proto poukazuje především na ty negativnější stránky digitálních technologií a na jejich negativní vliv na mládež.

Teoretická část práce představuje nejběžnější zařízení, které děti denně využívají, poukazuje na to, co na nich dělají – hraní her, sdílení životů na sociálních sítích a také poukazuje na to, s čím se děti na internetu mohou setkat, a jak to může do jejich života zasáhnout.

Praktická část práce zjišťuje, jak se mladiství v oblasti digitálních technologií chovají, jaké aktivity na svých zařízeních provozují a zdali se setkaly se zmiňovanými nástrahami internetu. Dále průzkum v praktické části představuje povědomí rodičů, o tom, co děti na mobilních a jiných zařízeních dělají a jestli se své děti snaží chránit před nebezpečím internetu.

Cílem práce je poukázat na reálné povědomí rodičů o vztahu mezi digitálními technologiemi a jejich dětmi a je proto navržen kurz pro rodiče, týkající se hrozeb digitálních technologií a bezpečného zacházení s nimi.

1 Cíl a metodika práce

Cílem bakalářské práce je zmapovat rizika a hrozby využívání digitálních technologií mládeží a na základě výsledků z realizovaného dotazníkového šetření navrhnout soubor konkrétních opatření a doporučení pro rodiče dětí, a to ve formě vzdělávacího kurzu, který rodiče seznámí s hrozbami digitálních technologií a naučí je bezpečně pracovat s internetem.

Teoretická část práce bude zaměřena na problematiku rizik a hrozeb spojených s využíváním digitálních technologií mládeží. To bude provedeno zejména s využitím analyticko-syntetických a induktivně-deduktivních metod nad dostupnými primárními a sekundárními prameny. Bude provedeno vyhledání odborné literatury a elektronických internetových zdrojů, jejich studium a analýza.

Pro vypracování praktické části práce bude nutno vypracovat dotazníky zaměřené na výzkumné šetření, organizace a realizace výzkumného šetření. Dále bude provedeno vyhodnocení odpovědí z dotazníků, provedení analýzy a shrnutí výsledků šetření. V souladu s teoretickou částí práce a výsledky šetření bude navržen vzdělávací kurz zaměřený na edukaci rodičů ve výše uvedené oblasti. V shodě s teoretickou částí budou využity zejména analyticko-syntetické a induktivně-deduktivní metody.

2 Úvod do teoretické části

Tato práce se zabývá dnešní mládeží, která tráví většinu volného času na digitálních zařízeních v online světě. Je tedy třeba nejdříve si vymezit, co je myšleno pod pojmem mládež. Dále si určit, co jsou to digitální technologie a představit si nejběžnější digitální zařízení. V dalších kapitolách práce obsahuje informace o nejpoužívanějších sociálních sítích a online hrách. Dále jsou představeny jednotlivé hrozby a rizika využívání digitálních technologií. Poslední kapitola se pak zabývá tím, jakým způsobem se uživatelé digitálních technologií mohou před jistými hrozbami chránit.

2.1 Pubescence a adolescence

Jako mládež si lze definovat děti v období pubescence a adolescence. Věkově se obě tyto období řadí mezi 11. a 22. rok života. Pubescence trvá většinou od 11 do 15 let. V tomto věku dochází k tělesným i psychickým změnám. Podle Langmeiera (2006, str. 142) se pubescence dělí na fázi prepuberty a vlastní puberty. Fáze prepuberty začíná prvními známkami pohlavního dospívání a urychlením růstu. U dívek končí kolem 13. roku první menstruací. U chlapců končí zhruba o 1-2 roky později, a to první noční polucí. Po dokončení prepuberty, nastupuje druhá fáze, a to vlastní puberta. Její konec nastupuje s dosažením reprodukční schopnosti.

Během prepuberty se ve fyziologických pochodech zvyšuje činnost žláz s vnitřní sekrecí, které mají vliv na fyzické a psychické změny jedince. V tomto věku jsou jedinci často emočně labilní a nepozorní. Jsou citliví vůči nespravedlnosti a kritice. Prepuberta se také projevuje ostýchavostí projevovat city vůči rodičům. Pubescenti se snaží osamostatnit. Navazují více kontaktů s vrstevníky a sdružují se do skupin podle společných zájmů. Vztahy ovšem nebývají pevné, a tak často střídají přátele a dochází ke střetům mezi nimi. Kontakty mezi chlapci a děvčaty jsou někdy až averzní.

Období vlastní puberty, Vágnerová (2012, str. 214) nazývá obdobím staršího školního věku. Je to období 13-15 roku života. Tělesný a psychický vývoj se začíná vyrovnávat. V tomto období jedinci hledají vlastní identitu a svádějí boj se sebou samým.

Adolescence trvá přibližně od 15 do 20 roku života. Zacharová (2012, str. 62) uvádí, že adolescence má především psychosociální charakter, protože zásadní biologická změna proběhla již v pubertě. Sociálními mezníky adolescence jsou:

- Ukončení povinné školní docházky.
- První pohlavní styk.
- Dovršení profesní přípravy (s výjimkou vysokoškoláků).
- Právní dosažení plnoletosti.

Lidé v tomto životním období fyzicky dozrávají, osamostatňují se a hledají vlastní místo ve světě. Adolescenti mají často potřebu líbit se a dokázat společnosti, že už nejsou dětmi, ale dospělými.

2.2 Digitální technologie

Digitální technologie jsou všechna zařízení, způsoby a postupy používané pro komunikaci a práci s informacemi v digitálním světě. To znamená používány pro komunikaci mezi sítěmi, počítači, mobilními telefony a jinými zařízení. Podle Foxe (2013, str. 1) se obecně informační technologie používají pro vytváření, udržování a zpřístupňování informací. Lze tedy zjednodušeně říct, že technika je souhrnný název pro prostředky a technologie je chápána jako využívání těchto prostředků.

2.3 Digitální zařízení

„Průměrný školák ve věku mezi osmi a osmnácti lety dnes tráví třetinu života spánkem, třetinu ve škole a třetinu ponořený do nových médií, ať už to jsou smartphony, tablety, televize nebo notebooky. Tráví víc času komunikací skrze obrazovku, než tváří v tvář.“
(Alter, 2018, str. 217)

V této kapitole budou představeny zařízení, které v dnešní době využívá většina populace. Jsou to zařízení, které pracují na principu digitálního signálu. Digitální signál je zaznamenáván v podobě binárních číslic, tedy číslic 0 a 1 za pomoci elektrického napětí. Původní analogový signál je vyvzorkován na co nejmenší části a každá část je změřena. Tak části dostávají číselnou hodnotu a velikost, které jsou převedeny na soustavu nul a jedniček. Běžné informace, které jsou vnímány smysly, jsou analogové. Kdyby se převáděly do digitální podoby, musely by se vhodným zařízením digitalizovat. Např. digitálním fotoaparátem nebo kamerou, scannerem nebo diktafonem.

2.3.1 Počítač

Počítač je elektronické zařízení, které zpracovává data pomocí předem vytvořeného programu. Nejčastěji se jedná o stolní počítač nebo notebook. Je to zařízení, které se využívá v práci, ve škole nebo k zábavě. Na počítači lze pracovat s připojením do internetové sítě, ale i bez. Bez internetu lze na počítači hrát hry, tvořit textové dokumenty nebo třeba sledovat videa.

Počítač se skládá se ze dvou částí, a to z hardwaru a softwaru. Hardware představuje veškeré viditelné vybavení počítače, jako je například monitor nebo klávesnice. Software je tvořen operačním systémem a programy. Systémový software, je ten, díky kterému počítač funguje aplikační software, se kterým pracuje uživatel počítače.

2.3.2 Smartphone

Smartphone je v dnešní době nedílnou součástí života člověka. Využívají ho jak dospělí, tak děti nebo senioři. Kopecký (2018, str. 21) uvádí, že nejvíce dětí získává mobilní telefon mezi 7 a 9 rokem v souvislosti se vstupem na ZŠ.

Smartphone neboli chytrý telefon, je mobilní telefon, pro který je typická dotyková obrazovka, přední a zadní fotoaparát, bezdrátové připojení k internetu a možnost využívání různorodých aplikací. Smartphone, stejně jako všechna digitální zařízení, využívá operačního systému. Mobilní operační systém je např. Android nebo iOS. Každý tento systém má svůj virtuální obchod, který funguje díky připojení k internetu. Uživatel si zde může stahovat aplikace, dle jeho potřeb. Některé aplikace bývají jako součást telefonu už když si ho koupíte.

Portál Týden.cz (2018) uvádí, že: *„Takřka pětina mladých lidí ve věku mezi 16-24 let je na svých mobilních telefonech tak závislá, že jejich sledováním tráví více než sedm hodin denně. Své mobily mladí kontrolují každých dvanáct minut. Oproti starší generaci je to velká digitální propast.“* (Ofcom, 2018) Digitální propastí je myšlen rozdíl mezi lidmi, kteří digitální technologie ovládají a těmi, kteří do digitálního světa nejsou příliš zasvěceni.

2.4 Internet

„Internet je decentralizovaná rozsáhlá síť spojující počítače a jiné sítě (počítače v nich komunikují pomocí rodiny protokolů TCP/IP) na celém světě. Pokud se připojí počítač

do sítě Internet, tak lze získat přístup ke službám, které Internet poskytuje.” (ECDL, 2014) Internet lze rozdělit na tři části viz. Obrázek 1. Povrchový internet (Surface Web), hluboký internet (Deep Web) a temný internet (Dark Web). Povrchový internet je ten, který většina lidí zná. Zde se nachází vše, co se dá vyhledat běžnými internetovými vyhledávači, jako jsou např. Google, Seznam nebo Yahoo. Tato část však podle webu techlog360.com (2019) tvoří pouhých 4 % internetu. Vyhledávače pracují pouze v povrchovém internetu a nedostanou se tak na stránky chráněné heslem nebo platební bránou. Hluboký internet lze definovat jako heslem chráněné služby, které mají omezený přístup. Nejobtížněji dostupná část internetu se nazývá temný internet. Sem se dá připojit pouze pomocí speciálních programů, které je nutné nainstalovat do počítače. Tato část internetu slouží převážně k nelegálnímu dění. Slouží mafiánům, překupníkům drog, hackerům nebo obchodníkům s pornografií. Poslední 2 zmíněné části (hluboký a temný internet) jsou zde uvedeny pouze z důvodu komplexního přístupu ke zpracovanému tématu a bakalářská práce se jimi nebude dále zabývat.



Obrázek 1, Schéma Internetu (TechLog, 2019)

2.5 Sociální sítě

Sociální síť je virtuální propojení skupiny lidí, umožňující mezi nimi sdílet různý obsah. Mohou mezi sebou sdílet informace, hudbu, soubory, fotografie nebo videa. „Většina obsahu na sociálních sítích je tvořena jejími uživateli. Ti mohou

prostřednictvím příspěvků nebo veřejnou komunikací, chatů a dalších kanálů vytvářet obsah.” (Kožíšek, Písecký, 2016, str. 16).

Podle webu AMI Digital (2017), používalo v roce 2017 sociální sítě 69 % uživatelů internetu v České republice. V roce 2018 už 80 % uživatelů. Meziročně se také zvýšila doba, kterou uživatelé na sociálních sítích tráví, a to ze 144 minut na 149 minut denně.

Podle Stránského (2018), čas, který uživatelé na sociálních sítích tráví neustále roste. *„Je to v první řadě dáno stále se rozšiřujícím obsahem, který sociálních médií nabízí, ale přispívá k tomu i růst onlinové gramotnosti v populaci a také nové formáty, jako například instagramové a facebookové Stories nebo Whatsapp Status.“*

Husák (2018) uvedl ve studii Děti a sociální sítě, že děti si nejčastěji zřizují profily na sociálních sítích mezi 11. a 13. rokem života. Věková hranice zakládání profilů na sociálních sítích je 13 let. Když chce dítě mladší 13 let využívat nějakou sociální síť, je vyžadován souhlas rodičů. *„V případech s nízkým rizikem může být dostatečné ověření rodičovské zodpovědnosti pomocí e-mailu. V případech s vysokým rizikem může být naopak vhodné požádat o více důkazů tak, aby byl správce schopen ověřit a uchovávat informace podle čl. 7 odst. 1 obecného nařízení o ochraně osobních údajů.“* (UOOU, 2018)

Z výzkumu Husáka (2018) vyplývá, že 58 % dětí ve věku 10 až 18 let udává při tvorbě profilu nepravdivé údaje, což znamená, že jednají protiprávně. Nejčastějším nepravdivým údajem byl věk, který nejvíce pozměňují děti ve věku 10 až 12 let. Solove (2010) nazývá generaci dětí, které vyrůstají v prostředí digitálních technologií jako „Google generaci“. Tato generace vnímá internet nejen jako prostředek pro získávání informací, ale i jako prostředek pro komunikaci, zábavu a sociální existenci. Děti sociální sítě vnímají jako určitý trend a kdo je nemá, jako by nežil.

Boydová (2017, str. 16) ve své knize píše, že *„Většina teenagerů se připojuje on-line proto, aby se s lidmi ze svého okolí zkontaktovala.“* Alter (2018, str. 15) popisuje, jak nás při používání sociálních sítí ovlivňuje pohodlí. Pohodlí sdílení životů odkudkoli a kdykoli a okamžité získávání zpětné vazby prostřednictvím „lajků“ a komentářů.

2.5.1 Facebook

Sociální síť Facebook byla v roce 2004 založena Markem Zuckerbergem původně pro studenty Harvardu. Alter (2018, str. 15) ve své knize uvádí, že Facebook byl v roce 2004 zábava, nyní je návykový. *„Zážitek se vyvíjí a stává se z něj neodolatelná, nebezpečná verze původně zábavné kratochvíle.“*

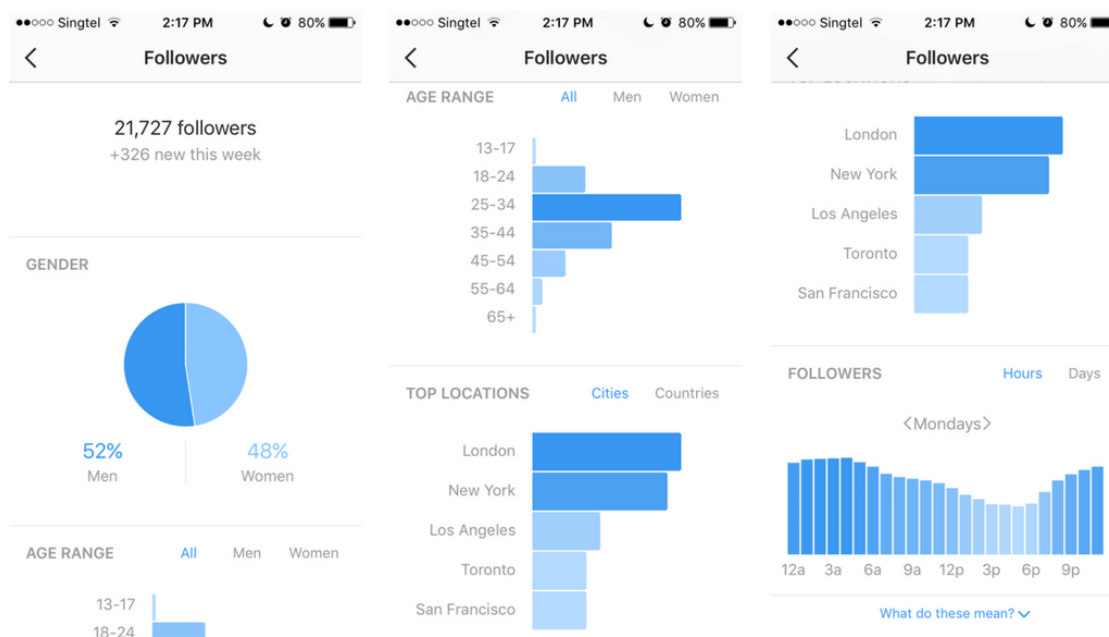
Facebook slouží ke komunikaci mezi lidmi, ke sdílení nebo uchovávání dat, a především k uchování vztahů a k zábavě. Statistika z webu facebook Newsroom k roku 2018 udává, že Facebook má 1,52 miliardy aktivních denních uživatelů a 2,32 miliard měsíčně aktivních uživatelů. Tato sociální síť je jednou z nejrozšířenějších a nejvyužívanějších. Na webu Markomu (2018) je Facebook vyhodnocen jako nejoblíbenější sociální síť roku 2018. Čtvrtou nejoblíbenější sociální sítí je pak Messenger, který byl vytvořen jako chatová aplikace Facebooku. Ovšem Pew Research Center (2018) zveřejnilo na svých webových stránkách, že teenagerů ve věku 13-17 let, kteří využívají facebook je pouze 51 %. Mnohem využívanější je mezi mladistvými Youtube 85 % a Instagram 72 %. Podle statistiky projektu E-bezpečí (2015, str. 8) *„Sociální síť Facebook využívá 78,9 % českých dětí. Děti využívají Facebook velmi aktivně - zaměříme-li se na respondenty mladší 13 let, zjišťujeme, že z nich má na Facebooku účet více než polovina (59,3%).“*

Člověk, který si chce založit účet na Facebooku, by si měl pečlivě rozmyslet, zda to udělá. Dá se lehce deaktivovat, což znamená, že profil nebude dohledatelný, ale obsah bude stále zachovalý a připravený pro případnou aktivaci. Jeho odstranění je složitější. Ovšem i přesto, že účet z Facebooku bude odstraněn, je možné ho do 90 dnů od odstranění stále znovu aktivovat.

2.5.2 Instagram

Podle AMI Digital (2018) v roce 2017 Instagram používalo 27 % českých uživatelů internetu. V roce 2018 již 44 %. Užívání Instagramu roste společně s jeho funkcemi. Je to sociální síť vyvinutá především pro sdílení fotografií a krátkých videí. Nyní už se navíc dá využívat i chat nebo příběhy, kam lidé nahrávají, co právě dělají. Tyto příběhy se dají okomentovat jen soukromou zprávou, tedy nikdo nevidí, jak kdo na danou fotografii nebo video reaguje. Za to člověk, který fotografii nebo video ve svém

příběhu zveřejní, pak vidí, kolik lidí danou věc vidělo, kolik to vidělo žen, kolik mužů a v jakém věku nebo třeba kolik lidí profil začalo sledovat, viz. Obrázek 2.



Obrázek 2, Statistiky Instagramu (DefPen, 2018)

Tyto statistiky pak mohou uživatele motivovat k častějšímu sdílení svých zážitků a dělat ho závislým. Lidé pak často sdílí i věci, které zasahují do jejich soukromí. Profil na Instagramu může být buď veřejný, což znamená, že příspěvky může vidět kdokoliiv anebo soukromý. U soukromého profilu může uživatel rozhodnout, kým budou jeho příspěvky sledovány.

2.5.3 Tinder

Tinder je aplikace založená na povědomí, že pro navázání vztahu je nejdůležitější vzhled. V této aplikaci se na displeji zobrazují fotografie potencionálních partnerů a uživatel je jen posouvá doleva nebo doprava, podle toho, zda se mu daný člověk líbí. Psychoterapeutka Šetinová (2018) v rozhovoru pro Aktuálně.cz uvádí, že se v dnešní době většina činností přesouvá na internet, a tak není divu, že velkým trendem je přesunutí komunikace s partnerem na internet, a to od seznámení až po rozchod.

Tinder ve svých podmínkách užívání uvádí, že ho smí užívat pouze lidé starší 18 let. Webový portál verywell family (2017) však uvádí, že 7 % uživatelů je ve věku 13 až 17 let.

2.5.4 YouTube

YouTube je největší internetový server pro bezplatné nahrávání a sledování videí. Podle statistiky z webu Statista.com (2019), je YouTube hned po Facebooku druhou nejpoužívanější sociální sítí. Za měsíc YouTube navštíví 1,9 miliardy lidí. V rozhovoru pro Tyinternety.cz zmiňuje obchodní ředitel YouTube Kyncl (2017), že na YouTube je každou minutu nahráno 400 hodin videí a každý den na něm lidé konzumují přes miliardu hodin, což je asi 114 000 let.

Jako jedna z mála sociálních sítí pro spuštění nevyžaduje registraci a přihlášení. Pokud se ovšem uživatel přihlásí, je mu umožněno komentovat videa nebo si je ukládat na později. Podle výzkumu společnosti Median (2014) tvořily v roce 2014 17 % uživatelů děti ve věku 12 až 17 let. Nejvíce sledují „vlogy“, tedy mluvené projevy Youtuberů nebo hraní her.

2.5.5 Snapchat

Snapchat je aplikace, kterou uživatelé využívají k zasílání fotografií nebo videí, které se dají obohatit o krátký text. Tato aplikace je založena na principu, že svým přátelům nebo jiným odběratelům uživatel zašle obsah, který se zobrazí pouze po dobu nastavenou odesílatelem. Například na 5 sekund. „*Tato funkce může vyvolávat falešný pocit bezpečí a anonymity, existuje však nespočet programů, které umí vytvořit screenshot obrazovky.*“ (Kožíšek, Písecký, 2016, str. 87)

Snapchat má 300 miliónů měsíčně aktivních uživatelů a 188 miliónů denních uživatelů. Denně se přes aplikaci Snapchat pošle 300 miliard fotografií a videí. Z výzkumu „Děti a sociální sítě“ vyplývá, že 34 % dětí ve věku 10-18 let aktivně používá sociální síť Snapchat. (Husák, 2018, str. 18)

2.6 Online hry

Podle Blinky (2015, str. 112) je pro online hry typické, že je v nich ve stejné době přítomno mnoho hráčů, kteří spolu mohou interagovat. Data z ČR z roku 2013 ukazují vysokou časovou investici online hráčů – v průměru hrají 31 hodin týdně. Online hry tak představují velmi výraznou volnočasovou aktivitu a v případě dětí i velmi výrazné socializační prostředí.

Mezi nejznámější patří hry World of Warcraft, League of Legends nebo hra roku 2018 Fortnite. „*Hry jako WoW přitahují mnoho teenagerů a mladých dospělých a až 40 % z nich si na hře vypěstuje závislost.*” Alter (2018, str. 27)

Různé hry jsou určeny od různého věku. Zpravidla to bývá od 4, 7, 12, 16 nebo 18 let. Tyto omezení se u her udávají z důvodu výskytu vulgarismu, rasismu, násilí, sexu, drog nebo hazardu ve hře. Průzkum britské společnosti Childcare (2018) však uvedl, že více než polovina rodičů nechává své děti hrát hry s hodnocením 18+ bez dozoru.

3 Hrozby a rizika využívání digitálních technologií

V této kapitole bude představeno několik rizikových jevů, se kterými se lze setkat při používání digitálních technologií, jak mohou člověka ohrozit a jaké na člověku mohou zanechat následky. Nejvíce se tyto hrozby týkají dětí, které většinou neví, jak zacházet s osobními údaji nebo neví čemu a komu mohou důvěřovat.

3.1 Behaviorální závislost

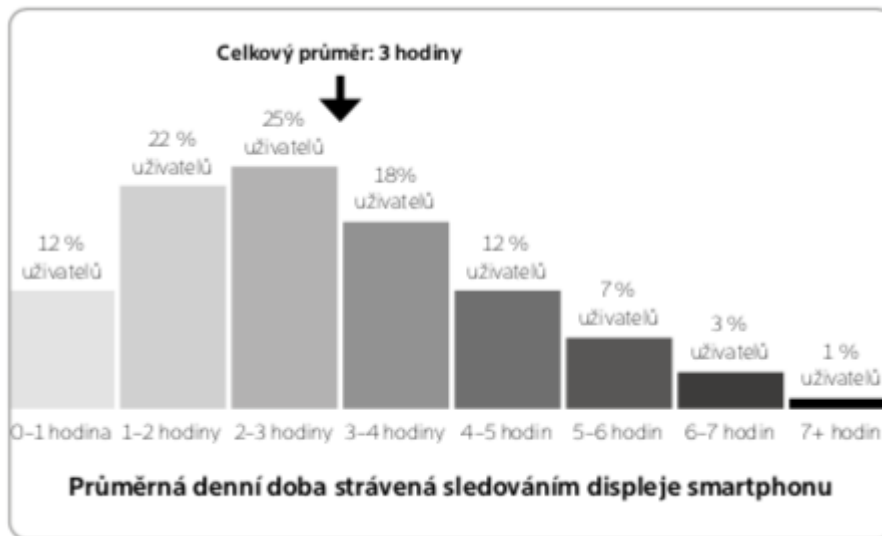
„O závislosti se obvykle hovoří v situacích, kdy jedinec není opakovaně schopen kontrolovat určitý typ jednání, jenž se vyznačuje značnou mírou kompulzivity, a pokračuje v něm i přesto, že si tím prokazatelně škodí.“ (Blinka, 2015, str. 21)

Rozlišují se závislosti látkové a nelátkové. Látkové závislosti jsou typické závislosti na nějaké látce. Např. Na drogách nebo alkoholu. Nelátkové neboli behaviorální závislosti se projevují jako závislost na určité aktivitě nebo procesu. Např. závislost na hazardu, na cvičení, nakupování nebo na internetu. *„Nahradí-li se termín návyková látka termínem návykový proces (behaviorální závislost), mohou se snadno znaky závislosti vypořádat i v samotném netholismu.“* (Kohout, Karchňák, 2016, str. 62)

Pod pojmem netholismus si lze představit veškeré závislosti spojené s internetem, tedy závislosti jako jsou: hraní online her, nakupování přes internet, chatování nebo sledování sociálních sítí.

„Vývojář aplikací Kevin Holesh si před pár lety uvědomil, že netráví dost času s rodinou. Viníkem byly technologie a hlavním pachatelem byl jeho smartpohone. Holesh chtěl vědět, kolik času denně stráví na telefonu, a proto vytvořil aplikaci s názvem Moment. Aplikace sledovala dobu, kterou stráví u displeje, a zaznamenávala, jak dlouho telefon každý den používá.“ (Alter, 2018, str. 23)

Alter (2018, str.24) ukazuje graf podle Holeshových dat, kolik hodin denně uživatelé smartphonů stráví sledováním displeje viz. Obrázek 3. Data jsou sesbírána od 8 000 uživatelů.



Obrázek 3, Schéma hodin strávených na smartphonu (Alter, 2018, str. 24)

Mezi internetové závislosti patří závislost na internetu jako takovém, závislost na online hrách, online sázkách, závislost na sociálních sítích nebo závislost na virtuální sexualitě.

Podle výzkumu od Cz.nic (2014) se závislost na internetu nejčastěji vyskytuje mezi mladými lidmi. Nejrizikovější skupinou jsou děti ve věku 12 až 15 let, jichž bezmála čtvrtina má podle českých průzkumů sklon k závislosti. Nejvíce závislí jsou pak lidé ve věku 16 až 29 let.

Následky těchto závislostí se mohou projevit:

- Narušením tělesných funkcí, jako jsou zhoršený zrak, bolest hlavy, bolest zad.
- Nespavostí, špatnou soustředěností.
- Depresí, pocity úzkosti.
- Agresivitou, změnou nálad.
- Obezitou.

3.2 Kyberstalking

Kyberstalking je takové jednání, které spočívá v opakovaném kontaktování oběti například zasíláním SMS zpráv, e-mailů, telefonáty, VoIP, messengery aj. Jednání útočníka se zpravidla stupňuje a zpravidla vyvolá u oběti obavy o svoje soukromí, zdraví, či život..” (Kolouch, 2016, str. 318)

Od 1.1.2010 je stalking trestným činem – je kvalifikován v § 354 jako nebezpečné pronásledování. Kyberstalking tak lze také vnímat jako trestný čin. Stalker si svou oběť vybírá záměrně s úmyslem oběť poškodit před společností, demonstrovat svou sílu nebo oběti vyhrožovat, obtěžovat ji nebo vydírat.

Kyberstalking může vést k:

- K psychickým poruchám.
- K sebevraždě nebo k pokusu o ni.
- K vraždám.
- K trestnímu stíhání pachatele.

3.3 Sexting

„ U takzvaného sextingu je nepochybné, že tímto uměle vytvořeným slovem (vzniklým ze spojení „sex” a „texting”) je míněno šíření intimních nebo pornografických textů, fotografií a videí pomocí počítačů nebo smartphonů a příslušných programů, respektive specializovaných internetových sociálních sítí.” (Spitzer, 2016, str. 243)

Podle Kožíška a Píseckého (2016, str. 83) má sexting dvě roviny. První z nich je výměna typu těchto zpráv s partnerem a druhá s neznámými osobami. Oba dva případy nesou rizika. Po odeslání zpráv s citlivým materiálem, nad nimi uživatelé ztrácí kontrolu. Např. partner může tyto intimní zprávy po rozchodu zveřejnit. Tudíž zaslání jakýkoliv materiálů vždy může být proti odesílateli zneužito. Sexting pak může být spojen s rizikovými jevy jako je vydírání, šikanování nebo šíření pornografie.

Kopecký (2017, str. 9) uvádí, že 24,76 % českých dětí provozuje sexting ve formě intimních a erotických zpráv. Sexting s rozesíláním intimních fotografií pak provozuje 15,37 % dětí a sexting s odesíláním svých intimních videí pak odesílá 6 % dětí. Naopak dětí, které obdržely takový materiál od jiné osoby je 40,96 % a 21,51 % dětí potvrdilo, že obdrželi erotické nebo pornografické video od svého internetového známého. Nejběžnějšími nástroji pro realizaci sextingu jsou podle Kopeckého (2017, str. 13) Facebook - 65,73 %, Facebook Messenger – 54,13 %, Snapchat 50,93 % a Instagram 12,40 %.

Rizika sextingu podle Kohouta a Karchňáka (2016, str. 49):

- Potencionální útočník obdrží citlivý materiál, který může v budoucnu zneužít.

- V případě zveřejnění citlivého materiálu na internetu je prakticky nemožné tento materiál „smazat“ – může být zneužit i po velice dlouhé době od zveřejnění.
- Trestní odpovědnost za šíření sextingu.
- Sexting se často stává prostředkem pro vydírání dětí v rámci tak zvaného kybergroomingu.

3.4 Kyberšikana

„Kyberšikana (Cyberbullying) je jakékoli chování, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií (zejména pak internetu nebo mobilního telefonu).“ (Kožíšek, Písecký, 2016, str. 62).

Kyberšikana je obdoba šikany, která probíhá v kyberprostoru, což je podle Spitzera (2016, str. 47) pomyslné prostředí, v němž probíhá komunikace v počítačových sítích. Aby bylo možné hovořit o kyberšikaně, musí být oběť napadána cíleně a opakovaně. *„Mezi nejčastější formy patří verbální útoky, zveřejňování fotografií a videí s nevhodnými komentáři, krádeže identity, v menší míře se pak setkáváme s vydíráním a vyhrožováním.“* (Kopecký, 2018). Na rozdíl od šikany se v kyberšikaně neprojevuje nepoměr mezi obětí a agresorem. V kyberprostoru mohou lidé svou převahu získávat větší technickou zdatností a mohou využívat své anonymity. *„U kyberšikany se vyskytuje fenomén tzv. sekundární kyberšikany, kdy se mohou zapojit do šikany i osoby, které oběť vůbec neznají. Najednou může mít takové hanlivé video tisíce zhlédnutí, což daleko přesahuje velikost publika u fyzické šikany.“* (Porubský, 2018)

Z projektu E-bezpečí (2016) vyplývá, že 40 % agresorů tvoří žáci škol. Nešikanují však a pouze své spolužáky, ale i učitele. Průzkum ukazuje, že 21,73 % českých učitelů si prožilo kyberšikanu.

„Nejčastěji jsou děti v České republice vystaveny průnikům na účet (prolomení hesla do online účtu), které potvrzuje více než 34 % (34,80 %) oslovených dětí. Na dalších pozicích pomyslného žebříčku nejčastějších forem kyberšikany se objevují verbální útoky (34,33 %) a poměrně rozšířené je také vyhrožování a zastrašování (17,84%).“ (Kopecký a kol., 2015, str. 55)

Mezi nepřímé ukazatele dítěte, které je obětí kyberšikany podle Látala (2009) patří:

- Náhle přestane využívat počítač, mobil.
- Často mění náladu a chování.
- Nechce chodit do školy nebo vůbec mezi lidi.
- Před cestou do školy trpí bolestmi břicha nebo hlavy.
- Vyhýbá se rozhovoru o tom, co dělá na počítači.
- Chodí „za školu“.
- Zhorší se jeho prospěch ve škole.
- Je apatické, někdy naopak nezvykle agresivní.
- Má poruchy soustředění.
- Špatně usíná, má noční můry.

3.5 Kybergrooming

„Kybergrooming je psychická manipulace prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.“ (Kohout, Karchňák, 2016, str. 49). Útočník si nejprve získává důvěru osoby. *„Útočník ji může získat tím, že se staví do role osoby, která dítěti rozumí, má stejné problémy nebo zájmy. Pokud útočník osloví oběť, bývá to zpravidla díky údajům, které má uvedeny na internetu.“* (Kožíšek, Písecký, 2016, str. 72)

Útočník si vybírá oběť zpravidla podle fotek, věku, zájmů nebo bydliště. Zde může hrát velkou roli klamavé udávání údajů. Například vyšší věk nebo fotografie stažené z internetu. Útočník oběť oslovuje pod nějakou záminkou. Třeba jestli už se někde neviděli nebo, že mají stejné zájmy. *„Útočníci mají většinou několik identit, některé využívají k tomu, aby potvrdili pravost jiného profilu „zeptej se, že mě zná.“ Mnohdy mají svoje účty v přátelích a snaží se působit dojem, že spolu chodí do třídy, na kroužek apod.“* (Kožíšek, Písecký, 2016, str. 73). Podle Kohouta a Karchňáka (2016, str. 49) se nejčastějšími oběťmi stávají dívky ve věku 11-17 let, které využívají informační a komunikační technologie, trpí nedostatkem sebedůvěry nebo pocitem osamění. Výzkum Pedagogické fakulty Univerzity Palackého v Olomouci a společnosti O2 Czech Republic (2017) dokázal, že každé druhé dítě v ČR chatuje s cizími lidmi a pětina z nich by neodmítla osobní schůzku.

3.6 Hoax

Hoax znamená v překladu „falešná zpráva“. Kohout a Karchňák (2016, str. 27) definují hoax jako poplašnou zprávu, která např. varuje před neexistujícím nebezpečím, před počítačovým virem, prosí o pomoc, anebo chce pouze pobavit. Hoax lidé používají za účelem zaujmout pozornost, vyvolat strach nebo si vystřelit z důvěřivých uživatelů. Tyto falešné zprávy se zprvu objevují na sociálních sítích. Často se tyto zprávy snaží poškodit nějakou instituci, výrobek, anebo se snaží zmanipulovat názory lidí. Bohužel provozovatelé sociálních sítí nemají nástroje na to, aby mohli ověřovat pravost informací. Obecně ale platí, že článek nebo informace, pod kterou není uvedený autor nebo je uvedený pod nějakou přezdívkou bývají klamavé. Vždy je lepší informaci ověřit z více zdrojů.

3.7 Phishing

„Jde o podvodnou techniku, která je založena na získávání údajů, jimiž mohou být hesla, kreditní karty nebo jiné údaje. Většinou je tato metoda využívána v elektronické komunikaci, kde se pod nějakou záminkou (e-maily ze služby, banky, sociální sítě), snaží získat z uživatelů citlivé údaje.“ (Kožišek, Písecký, 2016, str. 123)

Phisingové zprávy vypadají jako zprávy od důvěryhodných organizací. Například jako běžný e-mail od banky. Většinou je v těchto e-mailech odkaz na aktualizaci informací nebo potvrzení hesla. Po kliknutí na odkaz je pak uživatel přesměrován na falešné stránky, kde má zadat informace nebo heslo k účtu.

Mezi rizika otevření phisingového e-mailu patří:

- Získání citlivých informací.
- Odcizení identity.
- Odcizení peněz z účtu.

4 Bezpečnost na internetu

Jak už bylo uvedeno, na internetu je několik rizikových jevů, před kterými je nutno chránit nejen děti, ale i dospělé. V této kapitole tudíž bude představeno, jak se některá tato rizika dají regulovat a přecházet.

4.1 Zacházení s osobními údaji

„Pro děti ale také dospělé uživatele internetu je v současnosti zcela normální sdílet v prostředí internetových služeb velké množství osobních údajů. Údaje mohou být centralizovány (např. v prostředí sociálních sítí), mohou však být na internetu také roztržštěné na více místech. V zásadě je však poměrně snadné osobní údaje na internetu vyhledat a spojit je do profilu potenciální oběti.“ (Kopecký a kol., 2015, str. 69)

Kohout a Karchňák (2016, str. 40) uvádí, že uživatelé často nečtou smluvní podmínky užívání sociálních sítí a v rámci této nevědomosti tak mohou své osobní údaje poskytnout i třetí straně. V lepším případě jsou pak osobní údaje využity pro marketingové účely a v horším pro páchání trestných činů. Podle Zoomsphere byl k 19. 5. 2013 celkový počet uživatelů Facebooku v České republice 3 943 240, přičemž je z toho odhadován počet dětských uživatelů sdílejících své osobní údaje na síti na cca 927 000. Aby se zabránilo zneužívání osobních údajů k níže zmíněným rizikovým jevům, je nutné dodržovat jistá opatření.

Několik zásad bezpečného užívání sociálních sítí podle Kohouta a Karchňáka (2016, str. 41):

1. Nepoužívejte stejná hesla k více internetovým službám najednou.
1. Před každým potvrzením si vždy přečtete veškeré podmínky.
2. Na profilech sociálních sítí nikdy neuvádějte své telefonní číslo, rodné číslo nebo adresu.
3. Nenechte se označovat jinými uživateli na fotografiích (v nastavení soukromí nastavte vyšší úroveň kontroly).
4. Ignorujte neslušné zprávy a neodpovídejte na ně.
5. Pokud s někým nechcete komunikovat, nekomunikujte.

6. Na schůzku domluvenou přes internet nechoďte, aniž byste o tom řekli další osobě.
7. Nesdílejte své intimní fotografie, mohou být dále rozesílány.
8. Nesdílejte věci, které někdo může použít proti vám.

4.2 Ochrana hesla

V dnešní době je na člověka vyvíjen tlak, mít na každé internetové stránce nebo aplikaci heslo. Toto bezpečnostní opatření je pro uživatele internetu určitou výhodou, protože chrání jejich osobní a jiné údaje. Na druhou stranu je však těžké mít v paměti různá hesla k různým stránkám a aplikacím, a tak se často stává, že uživatelé mají na vše nastavené stejné heslo. To však z bezpečnostního hlediska není správně. „*Jednou ze zavedených praxí útočníků je prolomit a zjistit heslo u méně zabezpečených služeb a toto následně užít u těch lépe zabezpečených, např. zjistit heslo u diskusního fóra, kam se uživatel přihlásil a toto poté použít např. u sociální sítě Facebook.*“ (Kohout, Karchňák, 2016, str. 18)

Uživatel by měl v rámci ochrany svého hesla vždy zvážit na jakém zařízení a při jakém připojení k internetu bude své přihlašovací údaje zadávat. Na veřejných prostranstvích se například mohou vyskytovat počítače s programem keylogger. Keylogger je software, který zaznamenává každou stisknutou klávesu, tedy zaznamenává i hesla. Další nevhodnou cestou pro přihlašování a zadávání hesel je přihlášení přes veřejné sítě Wi-Fi, které mohou být monitorovány.

4.3 Ověření identity

Na internetu lze snadno narazit na člověka se smyšlenou nebo ukradenou identitou. Tito lidé mívají svou falešnou identitu do detailu promyšlenou. Často mají na sociálních sítích profil s fotografiemi cizích lidí, uvedené místo bydliště, datum narození a nechybí ani falešní přátelé. Mezi přáteli nebo sledujícími mívají většinou jiné falešné profily, aby své identitě přidali více reálných rysů. Při seznamování s neznámým člověkem skrze internet, by lidé měli být obezřetní a nezveřejňovat žádné osobní údaje. Mezi nejefektivnější způsob ověření identity patří zaslání fotografie, kde je vidět obličej a aktuální datum nebo text, který si uživatel po svém neznámém příteli vyžádá. Pokud se tento člověk začne vymlouvat, že fotografii nemůže zaslat, je to

podezřelé. Podle Kožíška a Píseckého (2016, str.103) je hlavní podmínkou pro zaslání takovéto fotografie, že musí být zaslána do 5 minut, aby byla eliminována možnost, že si daný člověk fotografii najde na internetu, popřípadě ji v nějakém grafickém editoru upraví.

Pro ověření identity lze také použít služby Google obrázky nebo TinEye. Pomocí této služby lze vložit do vyhledávače URL adresu fotografie nebo přímo fotografii a vyhledávač najde místa, kde je fotka zveřejněna. Dalším způsobem, jak ověřit identitu je videohovor.

4.4 Blokace nevhodného obsahu

Na internetu jsou dostupné i stránky s nevhodným obsahem pro děti. Takovými stránkami mohou být např. Erotické stránky, stránky s gamblerstvím nebo násilím. Přesto, že se u většiny těchto stránek při otevírání objeví takzvaný „Disclaimer“, tedy okno s dotazem, zda uživateli bylo 18 let, nebrání dětem, aby se na takovou stránku dostaly. Rodiče však tyto stránky pro své děti mohou úplně zablokovat, a to např. pomocí webu I-bezpecne.cz nebo programu WebLocker.

4.5 Google Family Link

Family link je služba, která umožňuje rodičům sledovat aktivity svých dětí na mobilních zařízeních. Služba umožňuje zjistit, kolik času dítě tráví na svém zařízení a kolik času tráví různými aktivitami. Tento čas pak mohou rodiče omezit. Můžou dítěti zamknout telefon třeba v čase, kdy má spát. Dále pak rodiče mohou sledovat jeho polohu. Family link je jedinečný v tom, že rodiče mohou vytvořit účet dítěti mladšímu 13 let a dítě tak nikde nemusí udávat nepravdivé údaje a lhát o svém věku.

5 Tvorba vzdělávací akce

Vzdělávací akce je forma promyšleného, plánovitého a organizovaného vzdělávacího působení jednotlivců, skupin nebo institucí, jehož cílem je předávání edukačních informací. Pro úspěšnou realizaci vzdělávací akce je nutné vytvořit kvalitní projekt. Fáze projektu si lze vymezit pomocí otázek: Proč? Koho? Co? Kdy? Jak? Kdo? Kde? Zač? Následující body tak budou představovat nutné kroky pro realizaci projektu a zároveň odpovědi na zmíněné otázky.

- Analýza a identifikace vzdělávacích potřeb
- Interpretace výsledků analýzy vzdělávacích potřeb
- Volba forem a metod vzdělávání
- Výběr lektorů a místa konání
- Materiální a technické zajištění
- Finanční plán
- Způsob evaluace

5.1 Analýza a identifikace vzdělávacích potřeb

Analýza a identifikace vzdělávacích potřeb je prvním krokem pro tvorbu projektu vzdělávací akce. Tato analýza spočívá ve shromažďování informací o současném stavu znalostí a dovedností určité skupiny lidí. Tyto informace se pak porovnávají s požadovanou úrovní znalostí a dovedností. Metodami sběru informací mohou být například dotazník, rozhovor nebo pozorování.

5.2 Interpretace výsledků analýzy vzdělávacích potřeb

Na základě identifikace vzdělávacích potřeb si lze přesně určit, jaká bude cílová skupina, tedy pro koho bude vzdělávací akce určena. Dále je nutné vymezit si vzdělávací cíle. Vzdělávací cíle představují měřitelné změny znalostí, dovedností či postojů. Tedy co by měl účastník na konci kurzu znát umět. Z těchto cílů pak vyplývá i obsah vzdělávací akce.

5.3 Formy a metody vzdělávání

Formy vzdělávání představují, jak bude zprostředkována výuka. Tedy jestli ve formě prezenčního studia, kombinovaného nebo například ve formě řízeného samostudia s individuální konzultací.

Metody jsou prostředky, které se využívají k dosahování vzdělávacích cílů. Jsou to tedy způsoby, kterými se předávají informace od vzdělavatele vzdělanému. Metodou může být například přednáška, výklad, pozorování nebo nácvik činností.

5.4 Výběr lektorů a místa konání

Pro kvalitní přenos informací je nutné vybrat profesionální tým lektorů, který bude disponovat odpovídající odborností. Pro kvalitu kurzu je také důležitý výběr místa konání. Místo by mělo mít odpovídající velikost pro daný počet účastníků, mělo by být dobře dostupné a mělo by vyhovovat technickým vybavením.

5.5 Materiální a technické zajištění

Pro správný chod kurzu je nutné zajistit veškeré potřebné materiály. Může se jednat například o materiály využité pro marketing akce nebo přímo pro výuku. Pod materiálním zajištěním tedy lze chápat výběr studijní opory, tisk dokumentů nebo zajištění didaktických pomůcek. Technické zajištění zde znamená, že pro kurz bude připravena veškerá technika, která je nutná pro určité vzdělávací metody. Například dataprojektor a počítač pro přednášku obohacenou o prezentaci.

5.6 Finanční plán

Aby bylo jasné, jaké bude mít pořadatel vzdělávací akce výdaje a příjmy, je nutné vytvořit finanční rozpočet. Tento rozpočet pak udává, jaký minimální počet účastníků se musí kurzu zúčastnit, aby byly pokryty veškeré výdaje. Výdaji jsou myšleny výplaty lektorům, pronájem místnosti, materiální a technické zajištění a další.

5.7 Způsob evaluace

Evaluaci vzdělávací akce lze chápat jako hodnocení a zjišťování kvality akce. Jak byli účastníci, ale i lektoři s kurzem spokojeni či nespokojeni. Evaluace vzdělávacích akcí může probíhat během vzdělávacích aktivit, na konci kurzu nebo zpětně po jeho skončení. Mezi nejběžnější metody evaluace vzdělávací akce patří dotazník, rozhovor

nebo pozorování. Na ukázkou byl vybrán evaluační dotazník dostupný ze stránek MVČR, který je součástí příloh práce.

6 Výzkumné šetření

K výzkumu byly vybrány děti druhého stupně základních škol. Tyto školy byly navštíveny v rámci odborné praxe. Během prevenčních programů pro tyto děti, byla problematika digitálních technologií a internetu velkým tématem. Zajímavé bylo, jak některé děti vnímají sociální sítě a online hry jako nedílnou součást jejich života. Pro práci tedy bylo stěžejní, kolik času děti tráví na digitálních zařízeních, co přesně na nich dělají nebo co zveřejňují na sociálních sítích. V souvislosti s tím byl výzkum zaměřen i na rodiče dětí tohoto věku a na jejich povědomí, o tom, co děti na digitálních zařízeních dělají a s čím se na internetu setkávají.

Výzkumný problém:

- Cílem empirického šetření je zjistit, jaké povědomí mají rodiče pubescentů a adolescentů o činnostech svých dětí v oblasti digitálních technologií. Jak je chrání před možnými hrozbami a riziky v kyberprostoru a navrhnout pro ně vzdělávací kurz z této oblasti.

Výzkumné otázky:

- Kolik času tráví mládež využíváním digitálních technologií a jak rodiče tento čas regulují?
- Čím z oblasti digitálních technologií tráví mladiství nejvíce času?
- Do jaké míry děti sdílí svůj život na sociálních sítích? Vědí rodiče, co jejich děti sdílí a s kým sdílí?
- Mají mladiství zkušenost s hrozbami internetu, jako jsou kyberšikana, kybergrooming nebo sexting? Vědí rodiče o těchto hrozbách?

6.1 Použitá metoda empirického šetření

Pro praktickou část bakalářské práce byl použit kvantitativní empirický průzkum. Byla provedena analýza současného stavu, a to primárně s využitím dotazníkového šetření. Dotazníky obsahovaly uzavřené, poloúavřené a otevřené otázky.

Dotazníky byly dva. Jeden pro děti a druhý pro rodiče. Dotazník pro děti obsahoval 18 otázek, kde v prvních dvou otázkách byly zjišťovány základní údaje o respondentech. Zbytek otázek se vázal k problematice digitálních technologií. Dotazník pro rodiče

obsahoval 21 otázek, kde se pouze první otázka vázala k získání údajů o respondentech a zbytek otázek se týkal jejich dětí, digitálních technologií a jejich vlivu na děti.

První dotazník byl určen pro děti ve věku 11–17 let. Byl použit v tištěné podobě na druhém stupni různých základních škol. Těchto dotazníků bylo rozdáno 63 a bylo z nich použito 46. 17 dotazníků bylo vyřazeno z důvodu neúplné odpovědi nebo nezodpovězení všech otázek.

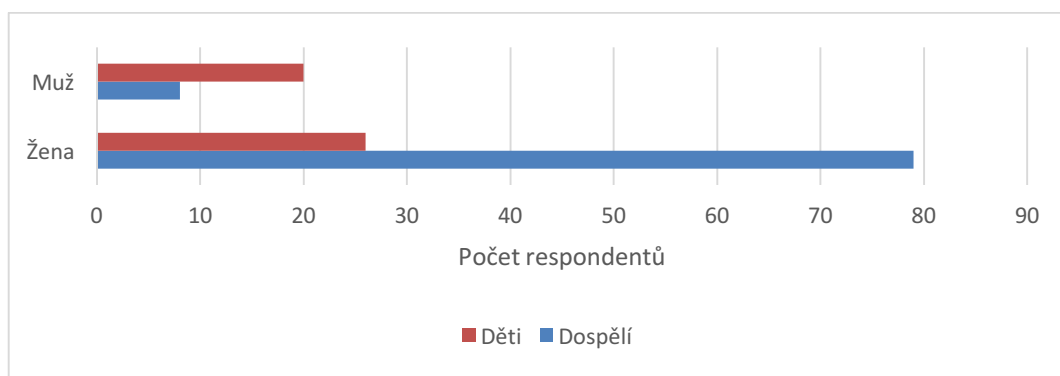
Druhý dotazník byl určen pro rodiče dětí ve věku 11-17 let. Tento dotazník byl vytvořen ve formě Google formuláře a byl zveřejněn v internetových diskuzích určených rodičům. Celkem byly sesbírané dotazníky od 105 respondentů, z nichž bylo vyřazeno 18, a to z důvodu neodpovídajícího věku dítěte. Z druhého dotazníku tedy bylo celkem pro výzkum použito odpovědí od 87 respondentů.

6.2 Zpracování a analýza dat

Oba dva dotazníky mají podobně zaměřené otázky, a tak budou vždy uvedeny témata s grafy nebo tabulkami, týkající se dotazníků určených rodičům a okomentovány v souvislosti s daty sesbíraných od dětí.

6.2.1 Základní údaje o respondentech

V této kapitole se nachází dva grafy. První graf se váže k pohlaví dětí, které odpovídaly v prvním dotazníku a k pohlaví dětí, za které odpovídali rodiče ve druhém dotazníku. Druhý graf se týká věku všech dětí.

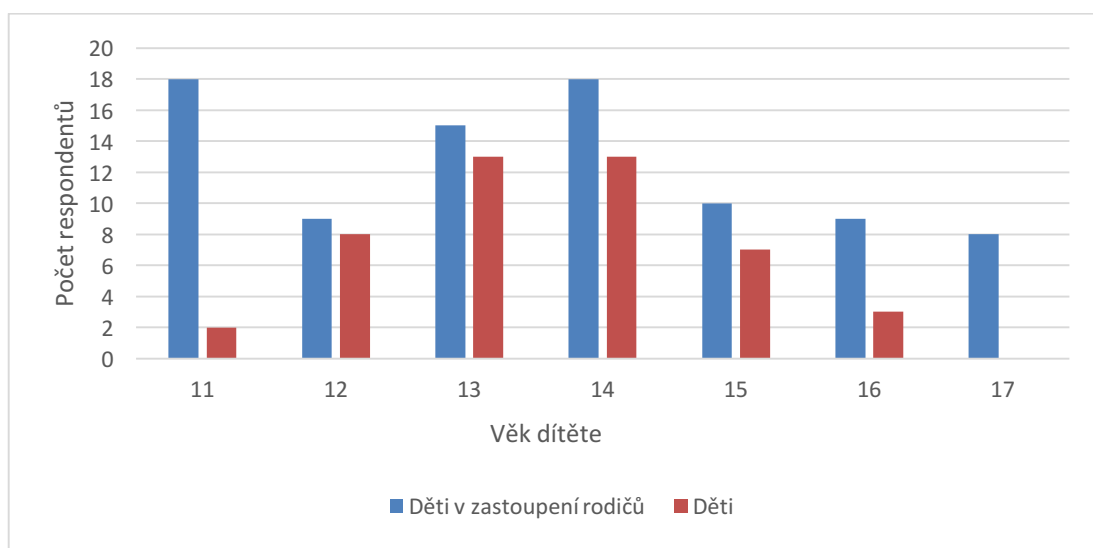


Graf č. 1: Pohlaví respondentů

Online dotazník vyplnilo 79 žen a 8 mužů. Vliv na tuto skutečnost může mít, že Facebookové skupiny určené pro rodiče a internetovou stránku Mimibazar.cz, kde byl

dotazník zveřejněn, navštěvuje více žen než mužů nebo jsou jen ženy ochotnější dotazníky vyplňovat. Ve školách vyplnilo dotazník pro děti 20 chlapců a 26 dívek.

Přesto, že na začátku teoretické části byla mládež definována jako období pubescence a adolescence, tedy věk mezi 11. a 22. rokem života, byl dotazník určen pouze pro rodiče dětí ve věku 11-17 let, a to z toho důvodu, že starší děti rodiče tolik nekontrolují. V grafu č.2, tak lze vidět počet zástupců jednotlivých věkových kategorií. Nejvíce se dotazníku účastnili rodiče dětí ve věku 11 a 14 let a děti ve věku 13 a 14 let.



Graf č. 2: Věk dětských respondentů a dětí dospělých respondentů

6.2.2 Digitální zařízení

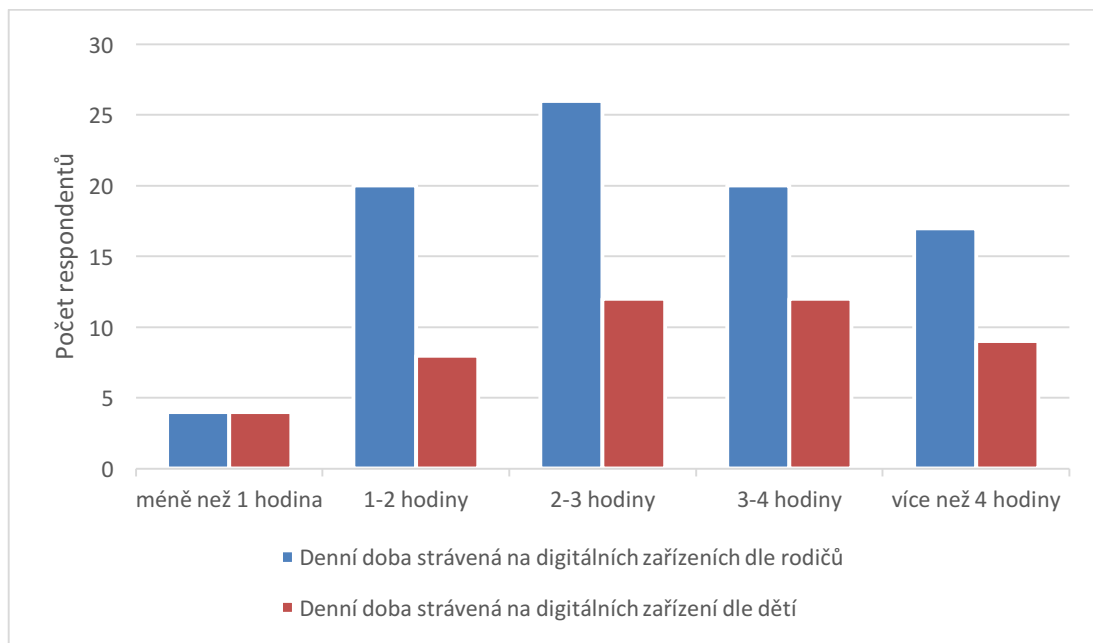
Podle získaných dat, pouhé 2,2 % dětí, tedy 1 dítě ze 46 dotázaných, nevlastní žádné digitální zařízení. Další 2 (4,3 %) děti nevlastní smartphone, ale využívají jiné zařízení ze zmíněných. Ze zbylých 43 dětí mají pouze 4 (8,7 %) jen jedno zařízení a 39 (84,8 %) z nich vlastní 2 a více digitálních zařízení. 5 (10,9 %) z nich dokonce uvedlo, že vlastní všechny zmíněná zařízení.

Tabulka č. 1: Digitální zařízení, která děti vlastní

Smartphone	Tablet	PC/notebook	Herní konzole
43 (93,5 %)	13 (28,3 %)	30 (65,2 %)	22 (47,8 %)

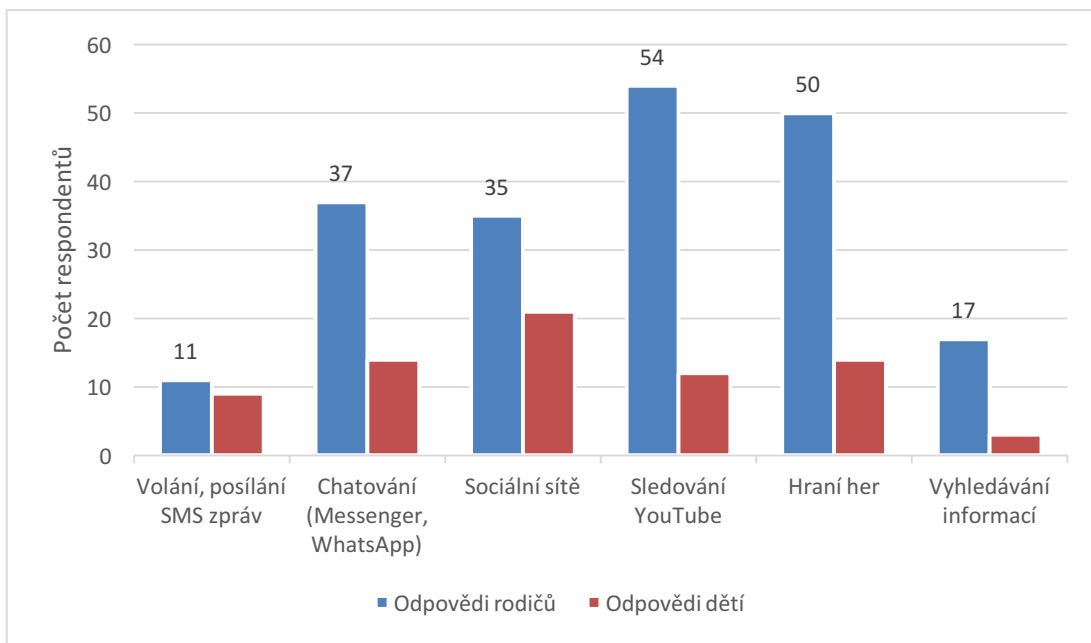
Nejvíce dospělých respondentů (29,9 %) odpovědělo, že jejich děti tráví 2-3 hodiny využíváním digitálních zařízení denně. Stejně na tom pak byly časové úseky 1-2

hodiny (23 %) a 3-4 hodiny (23 %) denně. Podle výsledků dotazníkového šetření pouze 4 děti z 87, tedy 4,6 % tráví na zařízeních méně než 1 hodinu denně. Oproti tomu dobu delší než 4 hodiny tráví na digitálních zařízeních 17 dětí z 87, tedy 19,5 %.



Graf č. 3: Doba strávená využíváním digitálních technologií

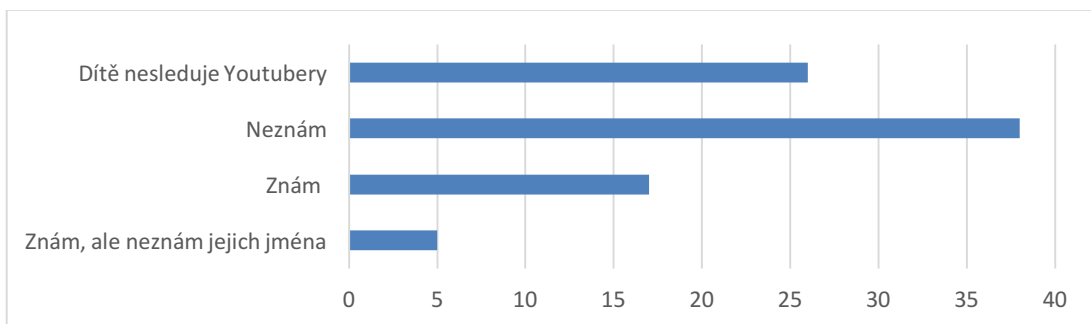
Rodiče dětí si myslí, že jejich děti na digitálních zařízeních nejčastěji sledují YouTube (62,1 %) a hrají hry (57,5 %). Dále pak vede chatování a využívání sociálních sítí. Nejméně dle rodičů děti telefonují a posílají SMS zprávy. Pouze 1 respondent odpověděl, že neví, co jeho dítě v oblasti digitálních technologií dělá. Většina rodičů má přehled o tom, co jejich děti na telefonech a počítačích dělají, jelikož se výsledky podobají odpovědím dětí. Dle dětí mezi nimi, ale nevede YouTube (26,1 %), ale sociální sítě (45,7 %).



Graf č. 4: Co nejčastěji děti dělají v oblasti digitálních technologií

6.2.3 Jak rodiče znají youtubery a hry

Nejvíce rodičů uvedlo, že jejich děti tráví nejvíce času na digitálních zařízeních sledováním YouTube a hraním her, ale o tom, koho sledují nebo co hrají hodně z nich přehled nemá.

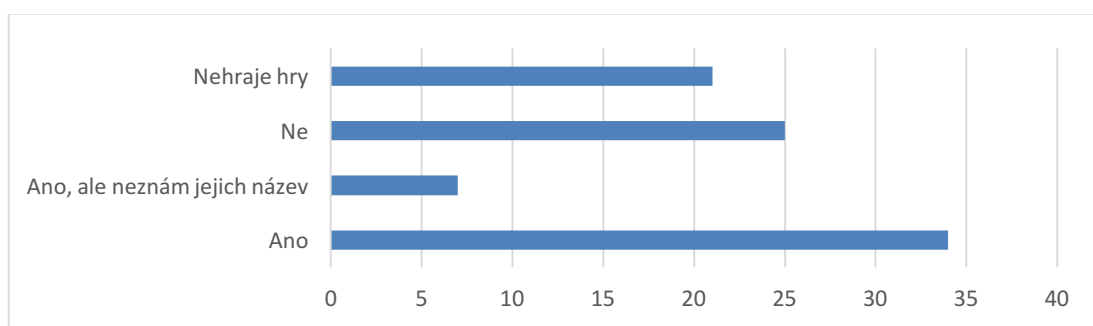


Graf č. 5: Znalost youtuberů

Téměř polovina rodičů (43,7 %) ví, že jejich dítě sleduje youtubery, ale nezná je. Dalších 5,5 % rodičů tvrdí, že youtubery zná, ale nepamatuje si jejich jméno. 29,9 % respondentů tvrdí, že jejich dítě youtubery nesleduje a pouhých 18,7 % rodičů dovedlo vyjmenovat alespoň jednoho youtubera, kterého jejich dítě sleduje. Mezi nejčastěji jmenované patří Tary (7x), Kovy (7x) a Jirka Král (4x). Vliv youtuberů na dnešní mládež je velký, proto by se rodiče měli více zajímat co a koho jejich dítě na YouTube

sleduje a pustit si některá videa také. Ne každý vliv musí být pozitivní. Třeba youtuber Tary, který na YouTube zveřejňuje přestupky, ne-li dokonce trestné činy, určitě dobrý vliv na výchovu mládeže nemá.

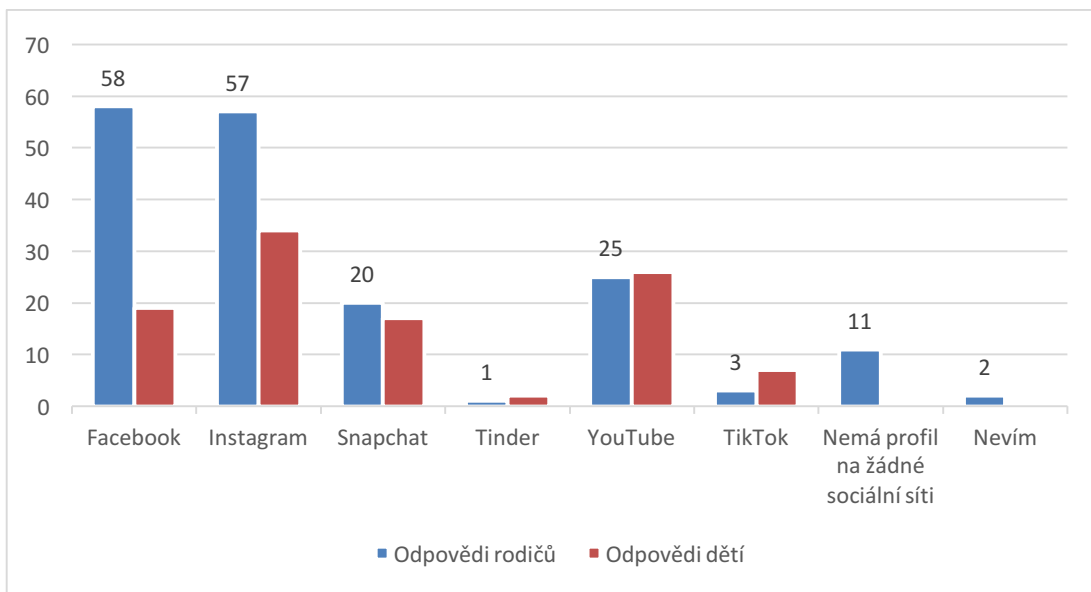
Oproti youtuberům, které dokázalo vyjmenovat pouhých 18,7 % rodičů, hry dokázalo vyjmenovat dvakrát tolik rodičů, tedy 39,5 %. Mezi nejčastěji zmiňované hry patří Minecraft (7x) a Fortnite (5x), tedy online hry, kde děti často hrají a komunikují s cizími lidmi. Oproti tomu 28,7 % respondentů odpovědělo, že hry nezná a 24,1 %, že jejich děti hry nehrají. Povědomí o hraní her by se mělo určitě zvýšit. Některé hry obsahují násilí nebo sprostá slova, která děti denně sledují a poslouchají. Rodiče pak často ani netuší, kde k takovým výrazům přišli.



Graf č. 6: Znalost her

6.2.4 Sociální sítě

Podle rodičů mají nejvíce děti profil na Facebooku (66,7 %) a na Instagramu (65,5 %). Méně často pak dle rodičů mají děti účty na sociálních sítích Snapchat (23 %) a YouTube (28,7 %). Jelikož 26,6 % respondentů odpovědělo, že jejich dítě je ve věku 11 nebo 12 let a sociální sítě smí děti používat až od 13 let, odpovědělo pouhých 12,6 % respondentů, že jejich dítě nemá profil na žádné sociální síti. Zbytek dětí tedy muselo své osobní údaje falšovat. Naproti tomu odpovědi dětí poukazují na to, že 97,8 % dětí má v tomto věku profil na sociální síti a 91,3 % dětí má profil rovnou na 2 a více sociálních sítích. 100 % dětí z těch, co mají účty na sociálních sítích pak potvrdilo, že si účet zakládali dříve než ve 13 letech, kdy je to povolené.



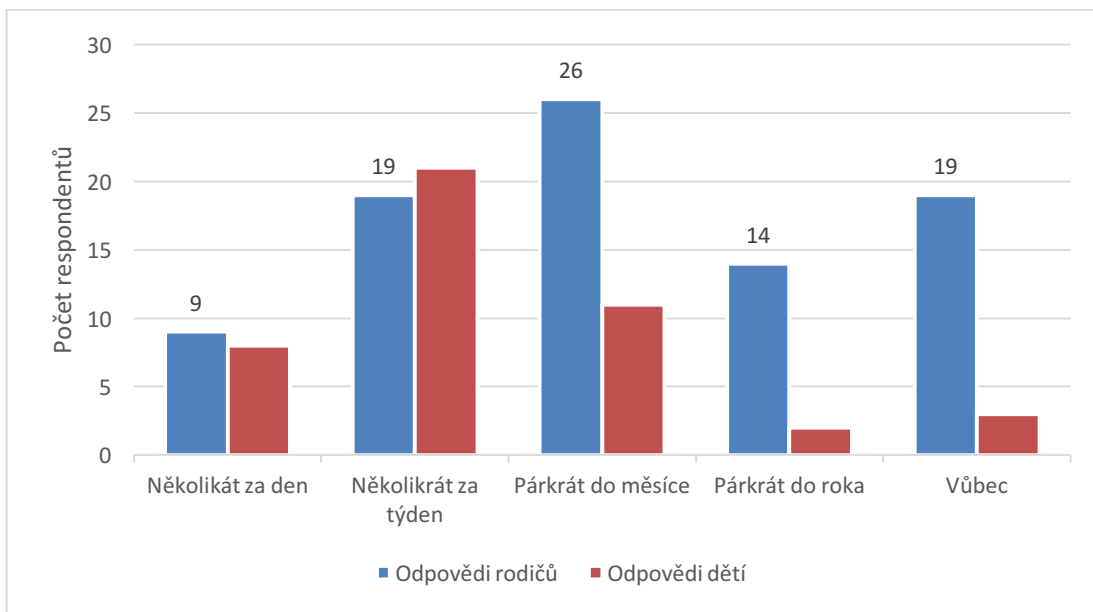
Graf č. 7: Na jaké sociální síti mají děti profil

Z tabulky č. 2 vyplývá, že nejčastěji si děti zakládají účty na sociálních sítích již v 10 letech a jelikož 44,8 % rodičů odpovědělo, že dětem při zakládání účtu nepomáhalo, nemohou ani vědět, jaké reálné nebo smyšlené údaje jejich děti zveřejňují.

Tabulka č.2: Věk založení prvního účtu na sociální síti

8 let	9 let	10 let	11 let	12 let
2 (4,4 %)	9 (20 %)	20 (44,4 %)	11 (24,4 %)	3 (6,7 %)

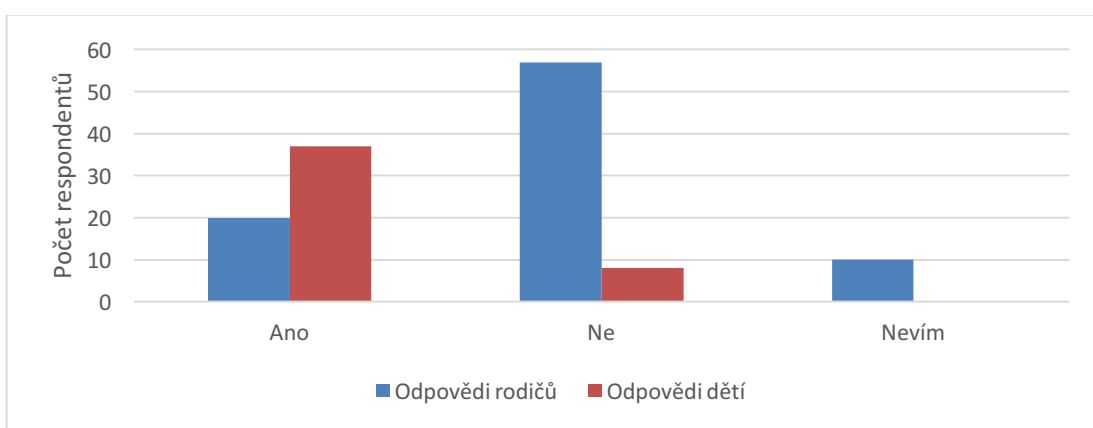
Nejvíce rodičů (29,9 %) si myslí, že jejich dítě sdílí příspěvky jen párkrát do měsíce a 21,8 % rodičů si myslí, že jejich děti žádné příspěvky nesdílí. 64 % rodičů si pak myslí, že pokud jejich dítě sdílí příspěvky, tak sdílí pouze s přáteli. Výzkum ale prokázal, že nejvíce dětí (45,7 %) sdílí příspěvky několikrát do týdne a 52,4 % z těch co sdílí, sdílí příspěvky veřejně.



Graf č. 8: Jak často děti sdílí příspěvky

6.2.5 Hrozby a rizika využívání digitálních technologií

65,5 % rodičů je přesvědčena, že si jejich dítě nikdy nepsalo s nikým cizím. 82,2 % dětí však potvrdilo, že si s cizím člověkem psali. Nejvíce z nich s takovým člověkem přišlo do styku přes Instagram (37,8 %), při hraní online her (29,7 %) nebo přes Snapchat (21,6 %). 89,7 % rodičů si myslí, že by jejich dítě nikdy nešlo na osobní schůzku s někým, koho znají pouze přes internet. 46,9 % dětí by ale na osobní schůzku s cizím člověkem šla.



Graf č. 9: Psaní s cizím člověkem

Většina rodičů (81,6 %) si myslí, že se jejich dítě nikdy neseťkalo s kyberšikanou, avšak 69,6 % dětí se s ní setkala. 19,4 % dětí z těch který se s ní setkaly, se dokonce

stalo obětí kyberšikany, a to v podobě urážlivých komentářů nebo „vtipných fotek“. V odpovědích rodičů se objevilo pouze 8 % těch, jejichž dítě se stalo obětí kyberšikany. Z toho vychází najevo, že rodiče o tom, že je jejich dítě šikanované často ani nevědí.

Tabulka č. 3: Setkalo se dítě s kyberšikanou?

	Ano	Ne
Odpovědi rodičů	19 (21,8 %)	71 (81,6 %)
Odpovědi dětí	31 (69,6 %)	14 (30,4 %)

Téměř všichni rodiče (96,6 %) tvrdí, že jejich děti nikomu neposílají intimní obsah. Odpovědi dětí to z 80 % potvrzují. Pouhých 20 % dětí odpovědělo, že svou intimní fotografii poslali partnerovi nebo kamarádovi.

Tabulka č. 4: Sexting – zasílání intimních fotografií či videí

	Ano	Ne
Odpovědi rodičů	3 (3,4 %)	84 (96,6 %)
Odpovědi dětí	9 (20 %)	36 (80 %)

Polovina rodičů tvrdí, že jejich děti někdy navštívily stránky přístupné od 18 let a polovina, že ne. I v tomto případě se děti v odpovědích téměř shodují. Nemyslím si však, že je v pořádku, že děti ve věku 11-16 navštěvují tyto stránky. Od 18 nejsou přístupné jen tak.

Tabulka č. 5: Stránky přístupné od 18 let

	Ano	Ne
Odpovědi rodičů	44 (50,6 %)	43 (49,4 %)
Odpovědi dětí	26 (56,6 %)	20 (43,4 %)

6.2.6 Omezování aktivit v oblasti digitálních technologií

Většina rodičů (81,6 %) říká, že dětem aktivitu na digitálních technologiích omezuje, ale pouze 26,1 % dětí tvrdí, že je tomu tak. 63,6 % z těchto dětí kontrolují rodiče zařízení přes aplikace a 36,4 % omezují domluvou.

Tabulka č. 6: Omezování využívání digitálních technologií

	Ano	Ne
Odpovědi rodičů	71 (81,6 %)	16 (18,4 %)
Odpovědi dětí	11 (26,1 %)	34 (73,9 %)

6.2.7 Bezpečnost využívání digitálních technologií

Dvě třetiny respondentů si myslí, že využívání digitálních technologií není bezpečné, a přesto je své děti nechá volně užívat. Třetina rodičů si myslí, že využívání digitálních technologií je zcela bezpečné.

Tabulka č. 7: Jsou digitální technologie bezpečné?

	Ano	Ne
Odpovědi rodičů	26 (29,9 %)	61 (70,1 %)

95,4 % rodičů své děti údajně poučuje, o tom, s čím se mohou setkat v oblasti digitálních technologií, otázkou ale je, do jaké míry takové ponaučení provádí, když si 82,2 % dětí píše s cizím člověkem nebo rozesílá své intimní fotografie (20 %).

Tabulka č.8: Poučování dětí o možných hrozbách digitálních technologií

	Ano	Ne
Odpovědi rodičů	83 (95,4 %)	4 (4,6 %)

6.2.8 Kurz pro rodiče z oblasti digitálních technologií

Pokud by existoval kurz, který by rodičům dodával přehled o tom, co děti dělají v prostředí digitálních technologií, pomohl jim regulovat hrozby, které se vyskytují na internetu a naučil je zabezpečit jejich zařízení, 50,6 % respondentů z řad rodičů by se zúčastnila.

Tabulka č.9: Účast na kurzu

	Ano	Ne
Odpovědi rodičů	44 (50,6 %)	43 (49,4 %)

6.3 Závěr výzkumného šetření

Z výzkumu vyplývá, že většina rodičů si přikrášluje, co jejich děti v prostředí digitálních technologií dělají. Všechny děti z těch, co využívají sociální sítě, na nich měly vytvořený profil dříve než, to zákon umožňuje. Znamená to, že se možným rizikům vystavují dříve než, je to nutné.

Často si rodiče nechtějí přiznat, že zrovna jejich dítě by mohlo být součástí kyberšikany. Při tom se děti s kyberšikanou běžně setkávají. I když někteří z nich zmínily kyberšikanu v podobě fotografických koláží a nevhodných komentářů, na dítě, které si prochází obdobím puberty a není zrovna emočně vyrovnané, tyto komentáře mohou mít velký vliv. Nejen komentáře, ale i jiné druhy kyberšikany mohou děti ohrozit. Děti, které jsou kyberšikanované pak mohou chodit „za školu“, mít zhoršený prospěch nebo trpět úzkostmi.

Rodiče si také nepřipouští, že by si jejich dítě mohlo psát s někým cizím. Přitom většina dětí vnímá cizí lidi, s kterými například hraje online hry, stejně rovnocenně jako kamarády ve škole, a tak často nevnímá hranici, kdy není vhodné některé věci s cizími lidmi sdílet nebo se s nimi dokonce scházet. Stejně tak si rodiče myslí, že jejich děti sdílí své údaje, fotografie atd. pouze s přáteli, zatím co popovina dotázaných dětí sdílí příspěvky veřejně. To pak může z dětí udělat oběti kybergroomingu, kyberstalkingu nebo sextingu.

Polovina rodičů pak odpověděla, že jejich dítě někdy navštívilo stránku přístupnou od 18 let, což více než polovina dětí potvrdila. Někteří rodiče si nejspíše neuvědomují, proč jsou takovéto stránky od 18 let a neblokují obsah těchto stránek. Buď proto, že to neumí nebo, že jim to nepřijde důležité. Blokace nevhodného obsahu by ale pro rodiče měla být prioritou, když své děti nechávají volně se pohybovat v kyberprostoru.

Dále rodiče v dotazníkovém šetření odpovídali, že znají youtubery a hry, které jejich děti sledují a hrají. Ovšem málokterý z nich dokázal nějakého youtubera nebo hru jmenovat. YouTube a herní portály jsou pro dnešní děti výrazným socializačním prostředím. A jelikož v tomto prostředí děti tráví několik hodin denně, měli by jejich rodiče mít pod kontrolou, koho sledují nebo co hrají. Ne každý youtuber nebo hra může dítě ovlivnit pozitivním směrem. Naopak násilí nebo přítomnost drog a alkoholu ve hrách dítě určitě pozitivně neovlivní.

Více než polovina rodičů odpověděla, že využívání digitálních technologií není bezpečné a že omezují aktivity svých dětí v této oblasti. Ovšem téměř $\frac{3}{4}$ dětí potvrdilo, že tomu tak není. Jen pár dětí odpovědělo, že by je jejich rodiče omezovali ve využívání mobilů, počítačů a podobných zařízeních. A to ze zmíněných důvodů není správně. Proto byl navržen kurz pro rodiče, který jim má být nápomocen pochopit, jak některé věci z prostředí digitálních technologií dokážou děti do velké míry ovlivnit nebo jim ublížit.

7 Návrh vzdělávacího programu

Cílem kapitoly je na základě teoretických poznatků uvedených v této práci a realizovaného výzkumného šetření vytvořit návrh vzdělávacího programu pro rodiče dětí. Kurz má rodičům poskytnout informace důležité pro bezpečí dětí v online prostředí a informace o možných hrozbách na internetu. Jedná se primárně o návrh obsahový, který není vytvářen pro žádný konkrétní subjekt. Vzhledem k tomu není možné některé kapitoly do detailu rozpracovat. Jako příklad je možné uvést kalkulaci projektu, případně lektory kurzu nebo diseminaci. Detailní návrh by vycházel až z konkrétní poptávky po tomto kurzu a zohledňoval by všechny požadované aspekty (místo, čas, počet účastníků...).

7.1 Představení kurzu

Mnoho rodičů neví, co jejich děti na svých telefonech a počítačích dělají a jaké rizika jim v souvislosti s využíváním těchto zařízení a internetu hrozí. Tento kurz by měl být nápomocný lidem, kteří jsou rodiči nebo pracují s dětmi. Kurz by jim měl pomoci porozumět funkcím běžných digitálních zařízení, vysvětlit, jak své děti chránit před nebezpečím skrývajícím se na internetu a naučit je, jak se dá v prostředí digitálních technologií pohybovat bezpečně.

Tento kurz není pouze teoreticky zaměřený, ale je doplněn o praktická cvičení realizovaná v počítačové učebně. Ty mají účastníkům pomoci pochopit a prohloubit jejich znalosti a dovednosti z oblasti zabezpečení internetových stránek a účtů na sociálních sítích.

7.2 Cílová skupina

Cílovou skupinou pro tento kurz jsou rodiče, kteří mají dítě ve věku 6-17 let, tedy dítě chodící na základní, případně střední školu. Tento kurz je zejména pro rodiče, kteří se chtějí dozvědět, co jejich děti dělají na telefonech, počítačích a jiných digitálních zařízeních a jak své děti mohou chránit před nástrahami internetu. Kromě rodičů je tento kurz určený i pro pedagogy, lektory nebo jiné zájemce, kteří pracují s dětmi nebo se o této problematice chtějí dozvědět něco víc. Předpokládá se, že účastník má základní znalosti a dovednosti v oblasti digitálních technologií, tj. umí ovládat běžná

digitálních zařízení jako jsou dotykový telefon nebo počítač, umí vyhledávat v prostředí internetu a zná probírané pojmy, jako jsou sociální sítě nebo online hry.

7.3 Cíle kurzu

Cílem kurzu je obohatit účastníky o znalosti a dovednosti z oblasti digitálních technologií. Kurz má účastníky naučit orientovat se v online prostředí a naučit je, jak se v něm dá pohybovat bezpečně.

Účastníci na konci vzdělávací akce:

- By měli být schopni vytvořit a správně zabezpečit účet na sociální síti.
- Dále by měli být schopni zablokovat nevhodný obsah internetových stránek.
- Měli by porozumět fungování online her a vyjmenovat a popsat jednotlivé kategorie přístupnosti her dle nevhodného obsahu.
- Budou znát význam pojmů souvisejících s hrozbami na internetu, jako jsou kybergrooming, kyberšikna a kyberstalking a zároveň budou umět popsat následky těchto hrozeb.

7.4 Formy a metody vedení kurzu

Cílem kurzu je nejen předat poznatky z výše uvedené oblasti, ale také rozvíjet potřebné dovednosti k předcházení rizik s nimi spojených. Vzhledem k tomu bude kurz probíhat ve formě prezenčního studia, aby mohly být použity metody názorně-demostrační a dovednostně-praktické, jejichž užití je pro kurz klíčovým faktorem. Kurz totiž spočívá v obohacování nejen vědomostí, ale i v získávání nových dovedností.

7.5 Diseminace kurzu

Kurz bude propagován především ve školách, a to v prostorech, kam se dostanou rodiče, tedy například školní družina. Budou zveřejněny ve formě plakátů a letáků. Také by mohly být uveřejněny v zájmových centrech nebo v dětských hernách.

7.6 Obsah kurzu

Kurz je členěn do 7 na sebe navazujících bloků, a to primárně podle vybraných témat a zvolených vzdělávacích metod. Tyto bloky jsou proloženy 15 minutovými přestávkami. Kurz je vzhledem ke svému zaměření zakončen závěrečnou diskuzí, v které budou shrnuty a objasněny problémové části a nejasná místa z předchozího

vzdělávání. Součástí ukončení kurzu bude také evaluační šetření a předání osvědčení o absolvování kurzu.

1.blok

První blok se zabývá představením lektorů a uvedením do tématu. Účastníkům bude puštěno video na YouTube a na to bude navazovat aktivizace účastníků s využitím diskuze na téma „Jak youtubeři ovlivňují naše děti“.

- Cíl: Účastníci budou umět objasnit vliv obsahu YouTube na jejich děti.
- Metoda: názorně-demonstrační

1. Blok

Druhý blok zahrnuje přednášku o sociálních sítích a problematice soukromí, tzn. jak sociální sítě fungují, jaké údaje o sobě děti na sociálních sítích zveřejňují, a proč je lepší to nedělat. Blok se dále zaměřuje na problematiku internetových stránek s nevhodným obsahem pro děti.

- Cíl: Účastníci získají nové vědomosti o fungování sociálních sítích, stránek přístupných od 18 let a o zveřejňování osobních údajů a pochopí souvislosti mezi zveřejňováním osobních údajů a tím, co k tomu jejich děti vede.
- Metoda: přednáška

2. Blok

Třetí blok probíhá metodou dovednostně-praktickou. Účastníci mohou uplatnit získané vědomosti z předchozího bloku a osvojí si dovednosti v oblasti práce s internetem. Naučí se, jak správně zabezpečit účet na sociální síti a jak na internetu zablokovat nevhodný obsah.

- Cíl: Účastníci si osvojí nové dovednosti v oblasti digitálních technologií. Budou umět zveřejnit a skrýt údaje na sociálních sítích a zablokovat nevhodný obsah na internetu.
- Metoda: dovednostně-praktická

3. Blok

Ve čtvrtém bloku jsou pomocí výkladu představeny nejpopulárnější hry a na nich poukázáno na nevhodný obsah pro děti. Tím je myšleno násilí, drogy, sex a podobné.

Dále je poukázáno, jak snadno se děti nejen během online her, na internetu seznámí s cizím člověkem.

- Cíl: Účastníci budou znát nevhodný obsah her a měli by chápat, jak se lze seznámit s cizím člověkem na internetu.
- Metoda: Výklad

4. blok

V pátém bloku je použita aktivizační metoda, a to ve formě hry. Účastníci se přihlásí na herní server a zahrají si vybranou online hru. Nejde o to, jak budou hrát, ale o to, aby si mohli vyzkoušet v jakém prostředí se děti pohybují.

- Cíl: Účastníci budou znát prostředí online her.
- Metoda: aktivizační - hra

5. blok

V šestém bloku jsou formou přednášky představeny nejběžnější hrozby internetu. Rodiče budou seznámeni s pojmy kybergrooming, kyberšikana a kyberstalking. Také je jim vysvětleno, jak k těmto jevům dochází a jaké následky mohou tyto hrozby zanechat nejen na dětech.

- Cíl: Účastníci budou znát pojmy kybergrooming, kyberšikana, kyberstalking a chápat následky s nimi spojené.
- Metoda: přednáška

6. blok

Poslední sedmý blok probíhá jako diskuze, a to jako rekapitulace celého kurzu. Dále je zmíněno, jakými formami mohou být děti kontrolovány, např. pomocí aplikace.

- Cíl: Účastníci pochopí souvislosti mezi všemi zmíněnými tématy a budou znát formy kontroly v prostředí digitálních technologií.
- Metoda: Diskuze

Orientační časový harmonogram

Čas	Blok	Obsah
11:00	1. blok	Zahájení kurzu, představení lektorů, představení tématu, úvodní diskuze
12:00	2. blok	Sociální sítě a soukromí, jak se se děti dostanou na stránky od omezeného věku a jak jim v tom zabránit
13:00-13:15	přestávka	
13:15	3. blok	Blokace stránek s nevhodným obsahem, zabezpečení účtů na sociálních sítích
15:00-15:15	přestávka	
15:15	4. blok	Online hry, na koho může dítě narazit na internetu, kamarádi online
16:15	5. blok	Jak fungují online hry
17:00-17:15	přestávka	
17:15	6. blok	Kybergrooming, kyberšikana, kyberstalking
18:15	7. blok	Závěrečná diskuze
18:45	Ukončení	Ukončení kurzu, evaluace, předání osvědčení o absolvování

7.7 Realizace kurzu

Tým lektorů

Kurz je veden dvěma lektory, a to proto, aby jeden mohl přednášet a druhý mohl být účastníkům nápomocný při práci na počítačích. Požadavky na lektory:

- Vysokoškolské vzdělání v oblasti pedagogiky nebo andragogiky
- Minimálně 2letá praxe v práci s dětmi jako učitel nebo lektor
- Zkušenost se vzděláváním dospělých – vedení alespoň 3 kurzů

- Certifikát nebo zkouška z oblasti digitálních technologií
- Komunikativnost
- Odbornost
- Empatie
- Trpělivost
- Autorita
- Odpovědnost
- Schopnost řešit problémy

Oba dva lektori by měli mít bohaté znalosti z oblasti kyberprostoru a umět pracovat s dospělými jedinci.

Plánované místo konání kurzu

Kurz se uskuteční v počítačové učebně, neboť pro realizaci kurzu jsou nutné počítače. Místnost by měla disponovat takovou velikostí, aby se do ní pohodlně vešlo 20-25 účastníků.

Technické a materiální zajištění

Jak už bylo zmíněno v předchozí kapitole, pro kurz jsou nezbytné počítače, dále dataprojektor, plátно, ozvučení a tabule nebo flipchart. Pro účastníky je nutné zajistit materiál na poznámky, tedy papíry a psací potřeby. Také je nutné zajistit tisk dotazníků pro zpětnou vazbu, osvědčení a tisk případného propagačního materiálu.

7.8 Evaluace kurzu

Evaluace proběhne na konci kurzu, a to ve formě evaluačního dotazníku. Bude se hodnotit obsah a organizace kurzu, vedení, technické a materiální zajištění. Evaluační dotazník také zjistí, zda by účastníci měli zájem o podobné vzdělávací akce.

ZÁVĚR

Bakalářská práce „Hrozby a rizika využívání digitálních technologií mládeží“ je rozdělena na teoretickou a praktickou část. Cílem bakalářské práce bylo zjistit a srovnat povědomí rodičů o využívání digitálních technologií jejich dětmi s realitou. V teoretické části byly vysvětleny pojmy, jako pubescence, adolescence, internet, sociální sítě, online hry a jednotlivé hrozby využívání digitálních technologií a bezpečné zacházení s nimi, pro správné chápání části praktické. V této části práce byly také zmíněny zásady tvorby vzdělávací akce, jelikož výstupem praktické části je právě návrh vzdělávacího kurzu. Teoretická část byla zpracována na základě analýzy odborné literatury.

Praktická část byla vypracována pomocí průzkumu ve formě dotazníkového šetření. Toto šetření se skládalo ze dvou dotazníků, a to jednoho pro rodiče a druhého pro děti. Výsledky dotazníkového šetření prokázaly, že většina dotázaných rodičů nemá přehled s čím se jejich děti v oblasti digitálních technologií setkávají. Například, že se děti běžně setkávají s kyberšikanou, píšou si s cizími lidmi nebo že veřejně sdílí příspěvky na sociálních sítích a tímto způsobem se vystavují různým hrozbám jako je kybergrooming, kyberstalking nebo sexting. Dále se během průzkumu ukázalo, že rodiče sice vědí, že jejich děti hrají online hry nebo sledují YouTube, ovšem neznají obsah, který děti sledují. Proto byl jako výstup praktické části práce vytvořen vzdělávací kurz, který má rodičům poskytnout nové znalosti a dovednosti v oblasti digitálních technologií tak, aby se oni, a především jejich děti mohli bezpečně pohybovat v online světě. Kurz je rozdělen do 7 bloků, kde pro každý blok je zvolený určitý obsah a metody, jak bude obsah předán. V kurzu jsou využity především metody názorně-demostrační a dovednostně-praktické, které jsou klíčové pro získávání nových dovedností. Účastníci si na kurzu osvojí nové znalosti z oblasti sociálních sítí, online her, nevhodného obsahu na internetu a budou seznámeni s nejběžnějšími hrozbami, které se na internetu nachází. Dále si pak osvojí nové dovednosti, které budou získávány pomocí zmíněných metod. Účastníci se naučí bezpečně zacházet s osobními údaji na sociálních sítích, pohybovat se v oblasti online her nebo blokovat nevhodný obsah stránek přístupných od 18 let.

SEZNAM LITERATURY:

LANGMEIER, Josef a Dana KREJČÍŘOVÁ, 2006. *Vývojová psychologie*. 2., aktualiz. vyd. Praha: Grada. Psyché (Grada). ISBN 978-80-247-1284-0.

VÁGNEROVÁ, Marie, 2012 *Vývojová psychologie: dětství a dospívání*. Vyd. 2., dopl. a přeprac. Praha: Karolinum. ISBN 978-80-246-2153-1.

ZACHAROVÁ, Eva, 2012. *Základy vývojové psychologie*. Ostrava: Ostravská univerzita v Ostravě. ISBN 978-80-7464-220-3.

FOX, Richard, 2013. *Information technology: an introduction for today's digital world*. Boca Raton: CRC Press. ISBN 978-1-4665-6828-0

KAVALÍR, Aleš, 2009. ed. *Kyberšikana a její prevence: příručka pro učitele*. Plzeň: Pro město Plzeň zpracovala společnost Člověk v tísni, pobočka Plzeň. ISBN 978-80-86961-78-1.

KOPECKÝ, Kamil, 2016, 17(2). Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming: The strategies of child manipulation in online environments with a focus on cyber grooming. *Pediatrica pre prax*. Bratislava: SOLEN. ISSN 1336-8168.

KOHOUT, Roman a Radek KARCHŇÁK, 2016. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary. ISBN isbn978-80-260-9543-9.

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

SPITZER, Manfred, 2016. *Kybernemoc!: jak nám digitalizovaný život ničí zdraví*. Přeložil Iva ZÜNDORF. Brno: Host - vydavatelství. ISBN 978-80-7491-792-9.

BLINKA, Lukáš, 2015. *Online závislosti: jednání jako droga? : online hry, sex a sociální sítě : diagnostika závislosti na internetu : prevence a léčba*. Praha: Grada. Psyché. ISBN 978-80-210-7975-5.

ALTER, Adam, 2018. *Neodolatelné: vzestup návykových technologií a byznys se závislostí*. Přeložil Julie TESLA. Brno: Host. ISBN 978-80-7577-460-6.

BOYD, danah, 2017. *Je to složitější: sociální život teenagerů na sociálních sítích*. Přeložil Lukáš NOVÁK. Praha: Akropolis. ISBN 978-80-7470-165-8.

KOLOUCH, Jan, 2016. *CyberCrime*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-15-7.

KOPECKÝ, Kamil, 2015. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-4861-9.

Mladí tráví sledováním mobilu více než sedm hodin denně | Týden.cz. *Týden.cz - Aktuální zpravodajství v souvislostech* [online]. Dostupné z: https://www.tyden.cz/rubriky/veda/mladi-travi-sledovanim-mobilu-vice-nez-sedm-hodin-denne_492262.html.

CRHA, Vladan. AMI Digital Index: osm z deseti uživatelů internetu je na sociálních sítích denně. *Amidigital.cz* [online]. 19.6.2018. Dostupné z <https://www.amidigital.cz/digikydy/ami-digital-index-osm-z-deseti-uzivatelu-internetu-je-na-socialnich-sitich-denne/>.

ČRDM - Česká rada dětí a mládeže [online]. Copyright © [cit. 16.02.2019]. Dostupné z: <http://crdm.cz/download/publikace/CRDM-Zprava-Deti-a-socialni-site.pdf>

Teens, Social Media & Technology 2018 | Pew Research Center. *Internet & Technology - Pew Research Center* [online]. Dostupné z: <http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>.

What Every Parent Needs to Know About Tinder. *Verywell Family - Know More. Grow Together*. [online]. Dostupné z: <https://www.verywellfamily.com/what-every-parent-needs-to-know-about-tinder-2609052>

BREJLOVÁ Iva, Lidé denně konzumují na YouTube přes miliardu hodin, říká Robert Kyncl. *Tyinternety.cz – nejen o těch internetech!* [online]. Copyright © 2019 [cit. 13.02.2019]. Dostupné z: <https://tyinternety.cz/rozhovory/lide-denne-konzumuji-youtube-pres-miliardu-hodin-rika-robert-kyncl-nejvyse-postaveny-cech-online-videi/>

Sociální sítě: Twitter má v Česku nejmladší uživatele | MediaGuru. *Homepage | MediaGuru* [online]. Copyright © 2019 [cit. 13.02.2019]. Dostupné z: <https://www.mediaguru.cz/clanky/2015/04/socialni-site-twitter-ma-v-cesku-nejmladsi-uzivatele/>

YouTube a děti ve věku 3-7 let (výsledky průzkumu) | Vyplňto.cz - řešení pro online průzkumy. *Vytvořit dotazník | Vyplňto.cz - řešení pro online průzkumy* [online]. Copyright © [cit. 14.02.2019]. Dostupné z: <https://www.vyplnto.cz/realizovane-pruzkumy/youtube-a-deti-ve-veku-3-7-l/>

Více než polovina rodičů nechá své děti hrát hry určené starším 18ti let. *PCTuning - Titulni stranka* [online]. Copyright © 2009 [cit. 14.02.2019]. Dostupné z: https://pctuning.tyden.cz/index.php?option=com_content&view=article&id=52573&catid=1&Itemid=57

Projekt E-Bezpečí - Projekt E-bezpečí [online]. Copyright © [cit. 15.02.2019]. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/96-sexting-a-rizikove-seznamovani-2017/file>

Projekt E-Bezpečí - Téměř každé šesté dítě sdílí své intimní fotografie a videa. Nezdráhají se ani videochatů nebo osobních schůzek s cizími lidmi. *Projekt E-Bezpečí - Projekt E-bezpečí* [online]. Dostupné z: <http://www.e-bezpeci.cz/index.php/tiskove-zpravy/1246-vyzkum-sexting-2017>

Projekt E-Bezpečí - Projekt E-bezpečí [online]. Copyright © [cit. 18.02.2019]. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/107-rodic-a-rodicovstvi-v-digitalni-ere-2018/file>

Kyberšikana: Jak se liší od fyzické šikany ve třídách škol a jak jí úspěšně čelit | Reflex.cz. *Reflex.cz - Komentáře, zprávy, výrazné autorské fotografie* [online]. Copyright © 2001 [cit. 14.02.2019]. Dostupné z: <https://www.reflex.cz/clanek/ctete-v-tistenem-reflexu/85743/kybersikana-jak-se-lisi-od-fyzicke-sikany-ve-tridach-skol-a-jak-ji-uspesne-celit.html>

Mýty a fakta o sexuálním zneužívání dětí - Šance Dětem. *Informační portál - Šance Dětem* [online]. Copyright © Nadace Sirius [cit. 14.02.2019]. Dostupné z: <https://www.sancedetem.cz/srv/www/content/pub/cs/clanky/myty-a-fakta-o-sexualnim-zneuzivani-deti-63.html#nasledky-sexualniho-zneuzivani>

Darknet vs Dark Web vs Deep Web vs Surface Web — Different Parts Of The World Wide Web. *TechLog360 - It's All About Technology* [online]. Copyright © 2019

TechLog360 [cit. 16.02.2019]. Dostupné z: <https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/>

Snapchat by the Numbers (2019): Stats, Demographics & Fun Facts. *Omnicores Medical & Healthcare Digital Marketing Agency* [online]. Copyright © 2009 [cit. 16.02.2019]. Dostupné z: <https://www.omnicoreagency.com/snapchat-statistics/>

ECDL, Základy práce s internetem a komunikace [online]. Dostupné z: [\[online\]](#). Copyright © [cit. 16.02.2019]. Dostupné z: <http://www.ecdl.uzlabina.cz/e-learning/modul7.pdf>

Sexting.cz - vse, co chcete vedet o sextingu. *Sexting.cz - vse, co chcete vedet o sextingu* [online]. Dostupné z: <http://sexting.cz>

SEZNAM TABULEK:

Tabulka č.1: Digitální zařízení, která děti vlastní

Tabulka č.2: Věk založení prvního účtu na sociální síti

Tabulka č.3: Setkalo se dítě s kyberšikanou?

Tabulka č.4: Sexting – zasílání intimních fotografií a videí

Tabulka č.5: Stránky přístupné od 18 let

Tabulka č.6: Omezování využívání digitálních technologií

Tabulka č.7: Jsou digitální technologie bezpečné?

Tabulka č.8: Poučování dětí o možných hrozbách digitálních technologií

Tabulka č.9: Účast na kurzu

SEZNAM GRAFŮ:

Graf 1: Pohlaví respondentů

Graf 2: Věk dětských respondentů a dětí dospělých respondentů

Graf 3: Doba strávená využíváním digitálních technologií

Graf 4: Co nejčastěji děti dělají v oblasti digitálních technologií

Graf 5: Znalost youtuberů

Graf 6: Znalost her

Graf 7: Na jaké sociální síti mají děti profil

Graf 8: Jak často děti sdílí příspěvky

Graf 9: Psaní s cizím člověkem

SEZNAM PŘÍLOH:

Příloha č.1: Dotazník pro rodiče

Příloha č.2: Dotazník pro děti

Příloha č.3: Evaluační dotazník