Second Life - Bezpečnost ve virtuální realitě

Martin Vavroš

Bakalářská práce

2015

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Vavroš**
Osobní číslo:	**L12405**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Druhý život: Bezpečnost ve virtuální realitě**

Zásady pro vypracování:

1. **Zpracujte teoretické poznatky, zabývající se problematikou bezpečnosti ve virtuální realitě.**
2. **Analyzujte a zhodnoťte rizikové faktory virtuální reality.**
3. **Proveďte průzkum veřejného mínění na téma bezpečnosti ve virtuálním prostředí.**
4. **Navrhněte a formulujte doporučení pro eliminaci rizik.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: Rádce zodpovědného rodiče. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.

[2] STROSS, Randall E. Planeta Google: o troufalém plánu jedné firmy organizovat všechno, co známe. Brno: Computer Press, 2009, 296 s. ISBN 978-80-251-2412-3.

[3] AUKSTAKALNIS, Steve a David BLATNER. Reálně o virtuální realitě: umění a věda virtuální reality. Překlad Jan Klimeš. Brno: Jota, 1994, 283 s., [12] s. barev. il. Nové obzory. ISBN 80-856-1741-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **RNDr. Jakub Trojan**
Ústav environmentální bezpečnosti

Datum zadání bakalářské práce: **5. února 2016**

Termín odevzdání bakalářské práce: **9. května 2016**

V Uherském Hradišti dne 12. února 2016

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

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce je zaměřena na problematiku bezpečnosti ve virtuální realitě. Práce je rozdělena na 2 části. V první, teoretické, jsou blíže rozebrány pojmy jako virtuální realita, internet, či druhy počítačových her se zaměřením na tzv. MMORPG. Do této kategorie koneckonců spadá i projekt Second Life, jenž je zde podrobněji rozebrán. Ve druhé, praktické části, se čtenář seznamuje s problémem bezpečnosti ve virtuálním prostoru a aplikovanými metodami analýzy rizik. Setká se s pojmy jako kyberšikana, rizika veřejných Wi-Fi sítí, nebo získá povědomí o projektu EU Kids online. Hlavním cílem praktické části však bylo vytvoření dotazníku. Následná analýza a vyhodnocení nasbíraných dat, pak názorně vykresluje povědomí české veřejnosti o rizicích ukrytých ve virtuálním prostředí. Na základě těchto zjištění, jsou v závěrečné části práce navrhnuta příslušná doporučení, vedoucí ke zvýšení virtuální bezpečnosti.

Klíčová slova: virtuální realita, bezpečnost, internet, Second Life, kyberšikana

ABSTRACT

This bachelor thesis is focused on safety issues in virtual reality. The work is divided into two parts. In the first part, the theoretical one, concepts and terms such as virtual reality, the Internet, or the types of computer games with a focus on so-called MMORPG are described more specifically. After all, this category also includes the Second Life project, which is analyzed in detail. In the second part, the practical one, the reader gets familiar with the problem of security in the virtual space and applied methods of risk analysis. He becomes acquainted with the terms like cyberbully, risks on public Wi-Fi networks, or acquires awareness of the Kids online EU project. The main aim of the practical part, however, was the construction of the questionnaire. Subsequent analysis and evaluation of the data collected portray vividly the Czech public's awareness of the risks hidden in the virtual environment. Based on these findings appropriate recommendations to increase virtual security are proposed in the final part.

Keywords: virtual reality, security, Internet, Second Life, cyberbully

Poděkování

Touto cestou bych rád poděkoval svému vedoucímu RNDr. Jakubu Trojanovi, MSc, MBA za jeho trpělivost, ochotu a cenné rady, které mi v průběhu tvorby bakalářské práce věnoval. Můj vděk za podporu rovněž míří k rodině a přítelkyni, ale také mým spolubydlícím na internátu Policejního vzdělávání a služební přípravy Policejního prezídia ČR v Holešově, za jejich ohleduplnost, kterou mi vytvořili příznivé podmínky k tvorbě bakalářské práce.

Motto

„Cílem vzdělání a moudrosti je, aby člověk viděl před sebou jasnou cestu života, po ní opatrně vykračoval, pamatoval na minulost, znal přítomnost a předvídal budoucnost.“

Jan Amos Komenský

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 25.3.2016

.....

podpis studenta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 VIRTUÁLNÍ REALITA **11**
1.1 DRUHY TECHNOLOGIÍ VIRTUÁLNÍ REALITY: 12
1.1.1 Přehled headsetů pro virtuální a rozšiřující realitu 13
1.1.1.1 Oculus Rift 14
1.2 VYMEZENÍ POJMŮ VIRTUÁLNÍ REALITA A VIRTUÁLNÍ SVĚT 15
1.2.1 Virtuální světy a socializace 16
1.2.2 Virtuální identita – iluze či realita? 17
2 INTERNET **18**
2.1 ANONYMITA NA INTERNETU (VE VIRTUÁLNÍM PROSTŘEDÍ) 18
2.1.1 Dospívající a jejich virtuální vztahy 19
2.2 PROSTŘEDÍ ODREAGOVÁNÍ A ZÁBAVY 20
2.2.1 Počítačové hry jako zlo 20
2.2.2 Žánry počítačových her 21
2.2.2.1 Systém PEGI 22
2.2.3 MMORPG 22
3 SECOND LIFE **24**
3.1 CHARAKTERISTIKA VIRTUÁLNÍHO SVĚTA SECOND LIFE 24
3.2 ZAČLENĚNÍ SECOND LIFE 24
3.3 EKONOMICKÝ ASPEKT 25
3.3.1 Vlastnická práva 25
3.3.2 Zastoupení reálných firem 25
3.4 SECOND LIFE JAKO BEZPEČNOSTNÍ HROZBA 26
4 KYBERŠIKANA **27**
4.1 PONÍŽENÍ NA PRACOVIŠTI 28
4.2 NÁSLEDKY KYBERŠIKANY 28
4.3 KYBERGROOMING 29
4.4 STALKING 29
5 ZÁKLADNÍ METODY STANOVENÍ RIZIK **30**
II PRAKTICKÁ ČÁST **32**
6 BEZPEČNOST VE VIRTUÁLNÍM PROSTŘEDÍ **33**
6.1 INTERNETOVÁ BEZPEČNOST 33
6.1.1 Rizika veřejných Wi-Fi sítí 34
6.1.2 Osvětou proti nástrahám internetu 34
6.1.3 EU Kids Online 35
7 UŽITÉ METODY ANALÝZY RIZIK **37**

7.1 WHAT-IF (CO SE STANE KDYŽ) 37
7.2 CHECK LIST (KONTROLNÍ SEZNAM) 40
7.2.1 Výpočet míry rizika 40
7.2.2 Závažnost následků rizika 41
7.2.3 Výsledná míra rizika 42
7.2.4 Shrnutí metody Check List 42
7.3 METODIKA ZÁVĚREČNÉ PRÁCE 43
8 PRŮZKUM VEŘEJNÉHO MÍNĚNÍ 44
8.1 VÝHODY A NEVÝHODY DOTAZNÍKOVÉHO ŠETŘENÍ 44
8.2 CÍLE DOTAZNÍKU 44
8.3 SBĚR A VYHODNOCENÍ DAT 44
8.4 VÝSLEDKY ZJIŠTĚNÉ DOTAZNÍKOVÝM ŠETŘENÍM 46
9 NÁVRHY A DOPORUČENÍ 63
9.1 RADY PRO RODIČE 63
ZÁVĚR 64
SEZNAM POUŽITÉ LITERATURY 65
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 69
SEZNAM OBRÁZKŮ 70
SEZNAM TABULEK 71
SEZNAM PŘÍLOH 72

ÚVOD

Téma své bakalářské práce jsem vybíral pečlivě, hledíce zejména na jeho aktuálnost a vnitřní potřebu realizace v dané oblasti. S postupem času, zdokonalováním technologií a bouráním sociálních bariér, bude pojem „Bezpečnost ve virtuální realitě“ stále skloňovanějším tématem. Pokud se na věc podíváme z hlediska kyberšikany, jsou nejvíce ohroženou skupinou nesporně děti či mladiství. S rozvojem sociálních sítí jejich ohrožení na internetu stále roste a problému není zdaleka věnována taková pozornost, jakou by si zasloužil. Proč si tedy právě v bakalářské práci nepřiblížit oblasti, jež se svou koncepcí daného tématu dotýkají. Dnešní virtuální svět nás na jednu stranu dokáže spojit s lidmi z druhého konce světa a na tu druhou odloučit od našich blízkých. Jeho prostřednictvím můžeme neohroženě odhodit komunikační bariéry, které nás v reálném světě svazují. Přitom si však nemůžeme být jisti, pravou identitou člověka na druhém konci zařízení, zmítaném ve spleti jedniček a nul. Virtuální realita, jakožto fenomén blízké budoucnosti, v sobě skrývá nesmírný potenciál, ale rovněž rizika, která lidstvo nesmí podceňovat.

Hlavním cílem práce proto není pouze vymezení pojmů a stanovení rizik virtuálního prostředí, ale i tvorba a vyhodnocení dotazníkového šetření. Díky množství odpovědí nám respondenti přiblíží povědomí české veřejnosti o dané problematice. Poskytnou nám tak velmi aktuální data, jejichž vyhodnocením a návrhem opatření se práce rovněž zabývá.

I. TEORETICKÁ ČÁST

1 VIRTUÁLNÍ REALITA

Virtuální realita je druh zobrazení složitých informací, manipulace a interakce člověka s nimi prostřednictvím počítače. Způsob komunikace mezi člověkem a počítačem se nazývá rozhraní (interface) a virtuální realita je jen nejnovější v celé řadě těchto rozhraní.

Tři stupně virtuální reality:

Pasivní - Zde můžeme pozorovat, poslouchat a vnímat hmatem děj okolo nás.

Aktivní – V tomto stupni můžeme prostředí probádat. Na rozdíl od prvního stupně, je zde možnost pohybovat se ve virtuálním prostředí ať už létáním, chůzí, plaváním, či jiným způsobem. Můžeme zde kupříkladu uskutečnit procházky budovami či realizovat umělecká díla.

Interaktivní stupeň – Poslední a nejintenzivnější stupeň virtuální reality. Systém nám umožňuje seznámit se s prostředím, prozkoumat jej, a dokonce ho i měnit: vzít knihu a prolistovat ji či v simulované místnosti rozestavit nábytek dle naší představivosti.

Záměrem systémů pro virtuální realitu (dále jen VR) je poskytnutí uživateli, či skupině uživatelů iluzi, že jsou přítomni v umělém prostředí, jež nazýváme virtuální svět, virtuální scéna či virtuální prostředí. Právě v paměti počítače můžeme nejčastěji nalézt prostředí VR, může však existovat i jako skutečný svět doplněný počítačem o objekty. Pokud ovlivníme lidské smysly jako zrak, sluch, popř. hmat a v simulátorech i rovnováha, uživatel dosahuje pocitu přítomnosti ve virtuálním prostoru. Zejména v technických aplikacích by mělo být chování dílčích součástí virtuálního prostředí plně v souladu s fyzikálními zákony. [1]

Z hlediska investic do virtuální reality, se počínaje armádou, nemalou měrou podílí i zábavný sektor. Filmová studia, zábavné parky, tvůrci videoher a výrobci hraček už vědí, že VR je příslibem druhé velké vlny ve vývoji zábavy a reakce. [2]

	Definice	Příklady
Virtuální v obecném významu	Pomyslný, falešný, iluzorní, nereálný, možný	
Virtuální ve filozofickém smyslu	Existuje jako síla a ne jako jednání, existuje, aniž je přítomno	Strom v semeni (na rozdíl od stromu, který skutečně vyrostl). Slovo v jazyce (na rozdíl od chvíle, kdy je proneseno).
Virtuální svět ve smyslu vypočitatelnosti v informatice	Vesmír možného, vypočitatelného na základě digitálního modelu a vstupů zadaných uživatelem	Komplex poselství, která mohou být předávána přes: -software pro písmo, kreslení nebo hudbu -hypertextové systémy -databáze -expertní systémy -interaktivní simulace atd.
Virtuální svět ve smyslu počítačového vybavení	Sdělení je prostorem pro interakci zblízka, průzkumník v něm může kontrolovat přímo svou osobní reprezentaci	-dynamické datové karty, které představují informaci podle „úhlu pohledu“ -síťové hry na role -videohry -letecké simulátory
Virtuální svět v úzce technologickém smyslu	Iluze senzomotorické interakce s počítačovým modelem	Použití stereoskopických brýlí, datových rukavic nebo kombinézy k návštěvě rekonstruovaných momentů, tréninku chirurgických operací atd.

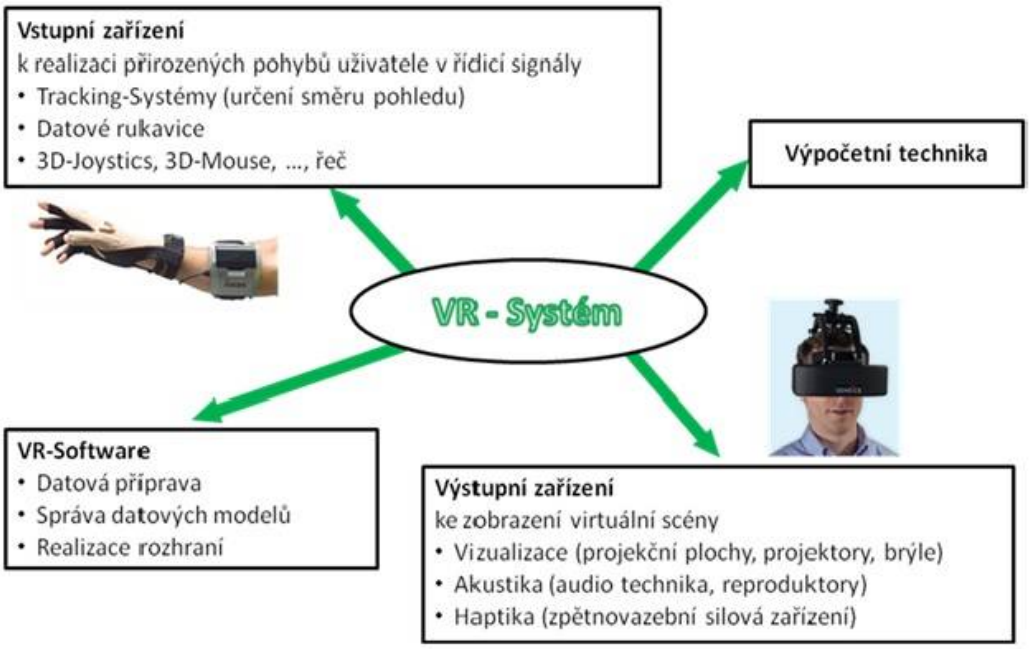
Tabulka 1: Významy slova virtuální, od nejslabšího po nejsilnější. Zdroj: [3]

1.1 Druhy technologií virtuální reality:

Rozlišujeme dva základní typy aplikací VR:

Pohlcující virtuální realita - je vždy spjata se speciálními technickými zařízeními, která mají uživatele co nejvíce oprostit (odříznout) od vjemů skutečného světa a vnuknout mu pocit, že je zcela ponořen do světa virtuálního. Nejčastěji zde řadíme periferní zařízení, kam patří přilba se stereoskopickými brýlemi a sluchátky (tzv. headset), snímače detekující prostorovou polohu uživatele, či datové rukavice nahrazující jednodušší vstupní zařízení.

Rozšiřující realita (Augmented Reality - AR) - informace z reálného okolního světa jsou propojeny s doplněnými prvky VR. Součástí systému bývá například kamera, která díky množství různých senzorů snímá pohyb uživatele. [4]



Obrázek 1: Složky systému virtuální reality. Zdroj: [4]

1.1.1 Přehled headsetů pro virtuální a rozšiřující realitu

VR Headset (Pro virtuální realitu) - zcela překryje realitu okolo nás a nahradí ji svou vlastní, a to včetně zvuků. *(Oculus Rift, Project Morpheus, SteamVR: HTC Vive, Fove VR, Razer OSVR, Zeiss VR One, Google CardBoard, Samsung Gear VR)*

AR Headset (Pro rozšiřující realitu) - za pomocí kamer je možné rozšířit vjem z normálního světa. *(Google Glass, HoloLens)*

Zjednodušeně řečeno, jestliže má zařízení průhledný displej, jedná se o AR Headset, pokud ne, jedná se o VR Headset. [5]

Obrázek 2: Přilba pro prostorové vidění. Zdroj: [6]

1.1.1.1 Oculus Rift

Na poli prostorového vnímání VR jsou nejpokročilejší technikou brýle Oculus Rift. Fakticky Oculus VR spadá do platformy Facebook, který vývoj „virtuálních brýlí" financuje. Tento headset využívá dvojici OLED displejů s celkovým rozlišením 2160x1200 pixelů při frekvenci 90 Hz, včetně nastavitelných sluchátek.

Headset je snímán externím senzorem, pomocí systému využívajícího infračervených LED. To umožňuje přesné zaměření polohy brýlí v rozsahu 360°, a to jak jejich pozice, tak směru pohledu. Cena se na našem trhu v současné době pohybuje od 17 tis. Kč.

DOPORUČENÉ POŽADAVKY:

- Grafická karta: NVIDIA GTX 970 / AMD R9 290 ekvivalent a vyšší
- Procesor: Intel i5-4590 ekvivalent a vyšší
- Pamět (RAM): 8GB a více
- Video výstup: HDMI 1.3
- USB Porty: 3x USB 3.0 + 1x USB 2.0
- Operační systém: Windows 7 SP1 64b. nebo novější [7, 8]

1.2 Vymezení pojmů virtuální realita a virtuální svět

Představa virtuálního světa umožněného technologickým pokrokem v lidech vzbuzovala touhu již před desítkami let. Její aplikace jsme mohli nalézt v umění, vzdělání, vědě, či vojenství. Ještě než začala druhá světová válka, vyráběly se letecké simulátory, nejprve simulující chování letounu. Od roku 1941 byl přidán i prvek simulace virtuálního prostředí v podobě pohyblivé hvězdné mapy. [9]

Na aplikace VR se můžeme dívat i z hlediska množství uživatelů, kteří se současně nacházejí ve virtuálním prostředí. Aplikace pro jednoho uživatele, lze snadno zpřístupnit více lidem, kteří spolu sledují zobrazovací zařízení (např. Powerwall)[1] nebo sdílejí společný prostor (např. Virtual CAVE)[2]. Nejčastěji jsou však jen v pozici diváků a interaktivní akce ve VR vykonává pouze jeden z nich. Následně až pokročilejší aplikace, které dovolují všem uživatelům aktivně se zúčastnit dění ve virtuálním prostředí, se správně nazývají *víceuživatelská virtuální realita* (multi-user VR). V takových systémech mohou být uživatelé fyzicky vzdáleni, iluze společného pobytu ve VR, je totiž zajištěna propojením jejich počítačů do sítě. VR se pak v takovém případě stává prostředkem komunikace mezi lidmi. S těmito aplikacemi se můžeme setkat i pod názvem *distribuovaná virtuální realita* (distributed VR). [4]

V obecnějším významu, počínaje Maroldovým panoramatem[3] či Tolkienovou Středozemí[4] a konče „hrou“ Second Life, je virtuální svět jakýkoliv prostor, který nepovažujeme za reálný, ale je možno k němu mít zprostředkovaný přístup, tedy jakýkoli mediovaný prostor. Z dnešního odborného hlediska, jej pak můžeme popsat v užším smyslu – virtuálním prostorem zpravidla chápeme prostředí simulované počítačem, ve kterém se v reálném čase pohybuje a komunikuje určitá komunita uživatelů, kteří jej zároveň mohou do jisté míry měnit svou činností. Pro příklady nemusíme chodit daleko, třeba už zmíněné virtuální

[1] Powerwall – jednosměrný projekční systém, využívající zadní pasivní stereoskopické projekce založené na technologii kruhové polarizace. [4]
[2] Virtual CAVE – projekční systém, využívající zadní pasivní stereoskopické projekce, sestávající ze tří vertikálních projekčních stěn. [4]
[3] Maroldovo panorama – panoramatický obraz Bitvy u Lipan českého malíře Luďka Marolda. S výškou 11 m a délkou 95 m jde o největší obraz svého druhu u nás. Dílo navozuje iluzi trojrozměrného prostoru. [10]
[4] Tolkienova Středozem – fiktivní kontinent vytvořený spisovatelem J. R. R. Tolkienem

prostředí Second Life, dětské virtuální „hřiště“ Habbo[5] nebo světy MMORPG her jako např. World of Warcraft (WoW). Pokud se budeme dívat trochu s nadhledem, můžeme mezi virtuální světy řadit i počítačové hry pro jednoho hráče, stejně jako MUDy, textové předchůdce dnešních MMORPG her.

Termín virtuální svět je svým významem propojen s pojmem virtuální realita. Ačkoliv se význam těchto frází může zdát téměř stejný, nejčastěji se virtuální realita spojuje spíše se smyslovou iluzí jiného světa, kdežto virtuální svět se pojí s koncepty interakce či komunity. [9]

1.2.1 Virtuální světy a socializace

Vedle bojových MMORPG existuje i řada virtuálních světů zaměřených primárně k socializaci. Projekt Second Life vyvíjený firmou Linden Lab je kupříkladu otevřeně inspirovaný Stephensonovým *Sněhem*[6]. Navzdory tomu, že se mu podařilo přitáhnout nemalou pozornost médií i odborné veřejnosti, poslední dobou už tolik populární není. S podobným nápadem přišla na trh i firma Google, která ovšem svůj projekt Lively uzavřela 31.12.2008, nedlouho poté, co jej spustila. Uživatelé zde mohli mít pověšené na zdi třeba oblíbená videa z Youtube.

Jedním z nejvíce výdělečných primárně socializačních světů je již výše zmíněné Habbo (dříve Habbo Hotel). Využívá pouze jednoduchou izometrickou grafiku a lze jej spustit přímo z okna prohlížeče. Uživatelé se zde mohou primárně socializovat a popustit uzdu fantazie dekoraci pokojů – místnosti především vyjadřují osobitost a kreativitu uživatele, neboli jeho avatara[7]. Habbo umožňuje i chat s přáteli a okamžitou teleportaci na jejich pozici. V jistém směru má tedy dimenzi sociální sítě.

Sociální sítě nevytvářejí virtuální prostor ve smyslu, v jakém jsme si jej doposud představili. Sociální síť Facebook je spíše zrcadlovým světem, v němž jsou zvýrazněny některé prvky sociální skutečnosti na úkor jiných, některé další jsou přidány. Jsou tedy spíše

---

[5] Habbo – virtuální socializační svět určený dětem, provozovaný finskou firmou Sulake. [9]
[6] Sníh – tzv. cyberpunkový román od spisovatele Neala Stephensona, zabývající se vizí postmoderní společnosti. Originál byl vydán v roce 1992 pod názvem Snow Crash. [11]
[7] Avatar – V počítačovém kontextu se jedná o vizuální reprezentaci uživatele ve virtuálním světě. Avatary mohou být trojrozměrné, dvojrozměrné, nebo je může vyjadřovat jediný znak. [13]

alternativou k formě virtuálních světů. Jejich samozřejmost a jednoduchá ovladatelnost ve webovém prohlížeči, která nám umožňuje přecházet mezi rozdělanou kancelářskou prací a interakci v sociální síti, z nich ovšem učinilo alternativu velmi atraktivní. [9, 12]

1.2.2 Virtuální identita – iluze či realita?

V internetovém prostředí nenalezneme jedince jako fyzický subjekt, ale zachází se zde pouze s reprezentacemi sebe sama. Neovlivňujeme tedy přímo sami sebe, ale působíme hlavně na svou „virtuální reprezentaci". Tato pak často obsahuje jistým způsobem uloženou a uchovávanou informaci o tom, „kdo jsme" v prostředí internetu, jaké zde máme jméno, či přezdívku (nick)[8], jaká je naše historie a jakého jsme dosáhli v rámci virtuální společnosti statusu. Mluvíme-li proto o virtuální identitě, myslíme tím, co fakticky přiřazujeme (virtuální) identitě naší reprezentace v prostředí internetu. Stejně jako běžná identita, obsahuje také identita virtuální aspekt osobní a sociální identity.

Osobní virtuální identita se vztahuje k tomu, čím jsem jako osoba ve virtuálním prostředí, či spíše čím je moje reprezentace této osoby ve virtuálním prostředí.

Sociální virtuální identita charakterizuje to, kam patřím ve virtuálním prostředí, čeho jsem součástí, respektive kam patří moje virtuální reprezentace. [14]

[8] Nick – zkrácená verze anglického slova „nickname", což v překladu znamená „přezdívka". Tento pojem často označuje uživatelské jméno (neboli username), pod kterým uživatel vystupuje např. v diskusních fórech.

2 INTERNET

Internet můžeme charakterizovat jako „prostředím bez zábran“ („disinhibited environment“). Fenomén prostředí bez zábran má jak pozitivní, tak negativní důsledky pro prostředí reálného života, výuky, výzkum a komerci na internetu a je pravděpodobně nejznámějším a nejčastěji popisovaným jevem ve virtuálním světě. S jistotou můžeme prohlásit, že ve virtuálním světě mají lidé méně zábran, než ve světě reálném. Odbourává se absence úzkosti ze sociálních situací a ztráta obav z odhalení sebe sama. Na internetu také lidem méně záleží na tom, co si o nich druzí myslí, potřeba sebeprezentace je mnohdy omezená. Běžná omezení, pravidla a normy reálné komunikace zde nemusí v řadě případů platit. Výsledky výzkumů ukazují, že „flameng“ což je ve zkratce agresivní chování vedené formou slovního napadení, je v prostředí VR až čtyřikrát častější, než v běžném životě. [15]

Z výzkumu, který řešil otevřenost respondentů při vyplňování dotazníků, vyplynulo, že respondenti pociťovali prostřednictvím internetu podstatně menší úzkost, než když dotazy zodpovídali psanou formou na papír. To se však povedlo pouze za dodržení jedné nezbytné podmínky a to anonymity. Pokud se tak nestalo, ve výsledku to vedlo k vytracení efektu. [15, 16].

2.1 Anonymita na internetu (ve virtuálním prostředí)

Mnoho lidí žije v omylu, že je internet zcela anonymní. Domnívají se, že když na internetu něco udělají, či podniknou, nejsou už žádné prostředky k jejich odhalení a následnému postihnutí. Je potřeba říci, že tato domněnka se v žádném případě nezakládá na pravdě. Běžný uživatel internetu je většinou anonymní jen ve velmi omezené míře a počítačový odborník (ale i vzdělaný laik) je mnohdy schopen odhalit přinejmenším to, odkud má člověk k internetu přístup, a tím se dostat přímo k jeho reálné identitě. Ve valné většině případů je anonymita běžných uživatelů na nepříliš vysoké úrovni. Anonymitu na internetu můžeme rozdělit na dva základní typy – anonymitu objektivní a subjektivní.

Anonymita objektivní - popisuje, jaká je reálná možnost identifikace identity uživatelů internetu (jak moc bude někdo úspěšný), bude-li pátrat po jejich skutečném jménu, příjmení apod. Můžeme ji také popsat jako míru odhalitelnosti technickými prostředky.

Anonymita subjektivní - naproti tomu pojednává o tom, co si my sami myslíme o své anonymitě na internetu, jaký je náš subjektivní názor na míru našeho „utajení“. V míře anonymity objektivní a subjektivní mohou být pochopitelně velké rozdíly. [15]

2.1.1 Dospívající a jejich virtuální vztahy

Virtuální prostředí se stává pro dospívající prostředkem pro navazování vztahů – přátelských, partnerských, ale i pracovních. Právě jev hledání partnera v prostředí internetu, je u dospívajících dětí častým jevem. Mnoho autorů řadí navazování nových vztahů přímo mezi vývojové potřeby adolescence. [14, 17]

Dospívající často uvádějí, že v prostředí internetu mají šanci najít nespočet lidí - potencionálních partnerů. Je pravdou, že možnosti hledání jsou takřka nevyčerpatelné. Tito lidé jsou navíc snadno dostupní a komunikaci se nebrání, zatímco v reálném světě tento jev nemusí být zdaleka tak častý. Díky nepřebernému množství lidí v internetovém prostředí, se s ohledem na společné záliby či zájmy, šance výběru vhodného partnera značně zvyšuje.

Navázání kontaktu - neboli „seznámení“, je v dnešní době tak snadné, že lidé nemusejí ani promluvit. Vlastně stačí jen poklepat myší na příslušný obrázek, či ikonu.

„Myslím si, že mnoho lidí by se jinak než přes net s opačným pohlavím neseznámila, tady je to mnohem jednodušší, třeba na chatu jen klikneš…“ (Carmen, 15 let)

Jakoby už samotným „kliknutím“ byl kontakt navázán, naproti tomu ve skutečném světě, je něco podobného mnohdy nesrovnatelně obtížnější. Pro některé dospívající je navázání kontaktu v reálném světě skutečný problém, zatímco v tom virtuálním jsou příležitosti vyrovnané i pro sociálně méně zdatné. Mezi sociální handicap můžeme řadit nesmělost, úzkost při navazování kontaktu nebo fyzická (ne)přitažlivost. [14]

Možnost ukončení kontaktu - ve virtuálním prostředí je důležité, že zde existuje možnost kdykoliv přerušit komunikaci, ukončit kontakt. Člověka nikdo nenutí pokračovat v komunikaci, pokud je mu jakkoliv nepříjemná nebo je dokonce ohrožujícího charakteru.

Nezávislost na lokalitě - dospívající se mohou bavit s lidmi napříč světem, poznávat jinou mentalitu, jiné kulturní prostředí, či zvyklosti a v neposlední řadě mají možnosti si vyzkoušet znalost cizího jazyka. [14, 15]

Ne nadarmo se říká, že vzdálenosti se stále zkracují. Díky dnešním vymoženostem moderního světa, mají mladí lidé u nohou možnosti, o kterých se předchozím generacím ani nesnilo.

2.2 Prostředí odreagování a zábavy

Prostředí internetu je také vnímáno jako zábava, prostředek k odreagování, relaxaci a povyražení. Srovnejme to se vstupem do zábavního parku – dospívající, či dospělý si sedá k počítači a má podobný pocit, jako když vstupuje do zábavního parku – vstupuje někam, kam se jde především bavit, odreagovat, relaxovat.

Dospívající často popisují, že na internetu zažívají stav, který v psychologii nazýváme „flow“. Je to stav, kdy je člověk pohlcen svou činností, vtažen do děje tak, že zapomíná na sebe, svou únavu a jde mu jen o prováděnou činnost bez ohledu na výsledek. [15]

Ze života - možná jste už zaslechli o příbězích lidí, kteří zemřeli po dlouhých hodinách hraní počítačových her. Stejně tak se už několikrát psalo o případech, kdy děti napadly, vážně zranily či dokonce zabily své rodiče poté, co jim byla zakázána počítačová hra. *Osmnáctiletý hoch z Tchaj-wanu si 13. července v tamní internetové kavárně rezervoval soukromou místnost, ve které hrál Diablo 3 čtyřicet hodin v kuse a poté zemřel. O případu informoval tchajwanský deník United Daily News.* [18]

2.2.1 Počítačové hry jako zlo

Dnešní tříleté děti umí ovládat YouTube a pouštět si videa ze svých oblíbených pohádek. O něco později se dostávají k mobilům nebo tabletům a hrají na nich hry. Zpravidla to umí podstatně lépe než jejich rodiče. Pro rodiče skvělá možnost, jak se dítka na nějakou dobu „zbavit“. Zároveň se však objevuje nové riziko ve formě možného vzniku závislosti.

V pokročilejším věku je běžné, že děti i dospělí dokážou u pc her trávit hodiny denně. Tvůrci her to ostatně chtějí. Hry jsou vytvářeny tak, aby byly svým způsobem návykové. Aby vyvolávaly chuť hrát a touhu „poznat, co je dál“, případně dosáhnout nějakých cílů. S příchodem sociálních síti, vznikla i „nová“ kategorie her (FarmVille, CityVille, The Sims Social apod..) Podobně založené jsou i další webové „klikací“ hry jako Travian, Divoké kmeny, Farmerama apod. V principu jde jen o navození potřeby co nejčastějšího návratu.

Typickou ukázkou her s možností vzniku závislosti jsou tzv. MMO (Massive Multiplayer Online) hry (více v odstavci 2.2.3 MMORPG). Největší z nich, World of Warcraft, hraje řada hráčů už pět a déle let. Virtuální světy, ve kterých si vytváříme postavy, vybavujeme je schopnostmi, zbraněmi a dalšími vlastnostmi, jsou velmi chytlavé.

Tyto hry mohou vést až ke snům, ze kterých se lidé probouzí zmateni a nejisti tím, kým a kde vlastně jsou. Stejně tak, jako je typické, pokud hru hrát přestaneme, do několika měsíců máme opět mít chuť se vrátit. Mějme proto na paměti, že v případě pc her a dětí je velmi důležité, aby rodiče věděli, jaké počítačové hry jejich děti hrají (více v odstavci 2.2.2.1 Systém PEGI). [18]

2.2.2 Žánry počítačových her

Akční agentury	GTA (Grand Theft Auto), Assassin´s Creed
Adventury	Polda, Posel Smrti
Arkády	Pacman, Mortal Kombat
Logické hry	Mahjong, Minesweeper
Společenské hry	Solitaire, Buzz
Jump and Run	Prince of Persia, Super Mario
Manažerské hry	Football Manager, Rollercoaster Tycoon
Hry na hrdiny	World of Warcraft, Diablo
Střílecí hry	Unreal Tournament, FarCry
Sportovní hry	NHL, NBA
Strategie	Age of Mythology, Stronghold
Vzdělávací hry	Souboj mozků, Dobyvatel

Tabulka 2: Přehled žánrů pc her s příklady. Zdroj: [19]

2.2.2.1 Systém PEGI

Počítačové hry zpravidla nesou označení pomocí systému PEGI (Pan-European Game Information), který byl spuštěn v roce 2003 a kde v zásadě jde o velmi jednoduché označení číslem určující věk, od kterého je vhodné počítačovou hru hrát. Odstupňování je přitom poměrně jednoduché – 3, 7, 12, 16 a 18 (a více let). Poslední, osmnáctka, samozřejmě znamená, že jde o hry vhodné pro dospělé – ať už z pohledu objemu násilí, nevhodných výrazů či sexuálních aktivit. Na obalu hry pak ještě zpravidla najdeme další informace o tom, proč má hra takové zařazení – piktogramy znázorňující přítomnost násilí, vulgární mluvy, strachu, sexu, drog, diskriminace, gamblerství a zda může být hra hrána online.

Obrázek 3: Piktogramy obsahu u pc her. Zdroj: [20]

V jiných částech světa fungují označování jiná, případně vůbec žádná. V Evropě se označování pomocí PEGI začalo používat v roce 2003 a dnes je používáno ve více než třiceti zemích. Systém je podporován hlavními výrobci herních zařízení včetně Sony, Microsoftu a Nintenda, jakož i vydavateli a tvůrci videoher v Evropě. Věkový rating PEGI byl založen Evropskou federací interaktivního softwaru. [18, 20]

2.2.3 MMORPG

Pochází z anglického (Massive Multiplayer Online Role Playing Games). Volně přeloženo jako „Online Hra o velkém množství hráčů s RPG prvky“.

Výhoda moderních MMORPG – Obrovské virtuální světy, kontakt s dalšími hráči, přísun stále nového obsahu. V praxi tak jde o hry, které „nikdy nekončí“. [18]

Od klasických počítačových her se liší tím, že:

- Mají dlouhou herní dobu (nejsou založeny na překonávání jednotlivých úrovní)
- Herní svět existuje a vyvíjí se i po vypnutí hry jedním hráčem
- Pokroky ve hře jsou dané organizací v rámci herního společenství [19]

Samotné hraní probíhá tak, že se hráči prostřednictvím internetových serverů připojují do virtuálních světů, na kterých pak participují, mohou zde plnit úkoly, díky kterým si vylepšují svůj herní charakter. Připojení probíhá přes herní účty, kde si každý hráč může vytvořit svoji postavu, tedy jakousi alternativní identitu. Počty uživatelů hrajících společně na jednom serveru se mohou pohybovat od stovek po několik tisíc, záleží na velikosti a popularitě jednotlivých serverů.

MMORPG jsou dnes velmi oblíbenou zábavou, která se vyznačuje vysokým množstvím uživatelů a časovou náročností. Mezi nejznámější hry tohoto druhu patří například WoW, EverQuest, Lineage, Second Life, nebo Lord of the Rings. [21]

3 SECOND LIFE

Second Life (dále jen „SL“) je trojrozměrný virtuální svět, který 23. června 2003 vznikl pod hlavičkou americké společnosti Linden Research, (nyní Linden Lab – dále jen „LL“). Cíl byl jasný, vytvořit ve všech ohledech převratné místo, kde budou lidé společně sdílet 3D prostory a budovat v nich nový svět. Svou vizi původně pojmenoval Linden World, nyní však projekt známe pod názvem Second Life.

3.1 Charakteristika virtuálního světa Second Life

Jedním z důvodů, proč je SL již mnoho let tolik úspěšný je skutečnost, že tento virtuální svět si vytvářejí sami uživatelé, nikoliv sama společnost LL. Ta sice zajišťuje technologické zázemí, ale podoba světa je jen na jeho obyvatelích. V současné době vyvíjí desítky tisíc tvůrců neustále nový 3D obsah a uplatňují své zkušenosti při dosahování zisku z prodeje svých milionů virtuálních předmětů na trhu.

Každý jeden uživatel má k dispozici modelovací nástroj z klientské aplikace, pomocí něhož může takřka neomezeně vytvářet objekty jako budovy, nábytek či ošacení. Takové předměty pak může uživatel ve hře využít k vlastnímu užitku, či následnému prodeji. Z počátku tento virtuální svět nedosahoval takových úspěchů. Vše se ale do jisté míry změnilo během roku 2006 a 2007, když se o jeho možnostech začala zajímat média a SL začal být objevován lidmi po celém světě. [22, 23]

3.2 Začlenění Second Life

Sami jeho tvůrci svět SL zařazují také mezi tzv. MMORPG a to ve smyslu, že potřebujete schopnosti k tomu, abyste získali práci. Ovšem na rozdíl od pravých MMORPG, zde rozhodují vaše reálné vlastnosti. Samotné označení SL jako typu MMORPG je ovšem nepřesné. Jak sám Philip Rosedale řekl: „Second Life není hra“. Principem tohoto prostředí tedy není dosažení nějakého cíle, vytvoření armády, bojování s nepřítelem či záchrana světa. Jde především o to, zkusit si žít svůj jiný život, pobavit se, najít přátele nebo zkusit vydělat peníze. Obyvatelé mohou komunikovat s ostatními obyvateli, navazovat nové vztahy, ať už přátelské či milenecké, mohou cestovat po různých regionech a komunikovat s lidmi po celém světě, kupovat pozemky, stavět domy, nakupovat různé věci, podnikat, ale i bavit se navštěvováním diskoték či posloucháním rádia, účastnit se soutěží nebo jen tak relaxovat a

pozorovat dění kolem sebe. V současné době zde obyvatelé mají mnoho možností, jak se vzdělávat, mohou navštěvovat kurzy, účastnit se přednášek a konferencí či různých setkání.

Vstup do světa SL je zadarmo. Uživatel si vytvoří účet a trojrozměrnou postavu avatara, která jej bude ve virtuálním světě zastupovat. Avatary v prostředí SL se dají různě upravovat, podle uživatelovy nálady, která vyjadřuje, jak si přeje vypadat. Společnost LL nabízí i prémiové účty; ty již ale nejsou zadarmo a uživatel musí za jejich provoz platit reálnými penězi. Tyto prémiové účty nabízí jejich vlastníkům především možnost koupit si vlastní pozemek.

3.3 Ekonomický aspekt

Do tohoto virtuálního prostředí nechodí jen lidé, kteří se chtějí pobavit či vyzkoušet něco nového, ale také lidé, kteří chtějí skrze SL vydělat reálné peníze. Ve světě SL totiž funguje plně integrovaný ekonomický systém, který umožňuje lidem vydělávat peníze, tzv. lindenské dolary (L$) které jsou volně směnitelné za americké dolary. [24]

Obyvatelé mohou vydělávat různým způsobem, stejně jako v reálném životě. Mohou se nechat zaměstnat nebo samostatně podnikat, například výrobou a prodejem různých výrobků, či vést nějaký podnik a podobně. Ekonomika je postavená tak, aby odměňovala zručnost, inovace nebo podstoupené riziko.

3.3.1 Vlastnická práva

SL poskytuje svým obyvatelům tu výhodu, že ponechává veškerá vlastnická práva autorům vytvořeného digitálního obsahu. Cokoliv obyvatel vytvoří, to je jeho a záleží jen na něm, jak s tím naloží.

3.3.2 Zastoupení reálných firem

Do světa SL ale nevstupují jen jednotlivci; reálné zastoupení zde mají i firmy, které tímto našly další způsob propagace a zviditelnění se, ale také rozšíření pole své působnosti. Tento virtuální svět totiž vytváří podmínky pro jakékoliv podnikání. Firmy tak mohou prezentovat nejen služby a produkty, ale také provádět výzkumy mezi obyvateli, získávat od nich zpětnou vazbu, pořádat virtuální mítinky, organizovat (nejen) placené e-learningové kurzy pro zájemce o vzdělání nebo nabírat nové zaměstnance. Mezi firmami a organizacemi, které této možnosti využívají, můžeme nalézt světoznámé značky, jako jsou IBM, Adidas,

Philips, Dell, Nike či Toyota. Zastoupení zde mají i univerzity z celého světa, například Harvardská univerzita, Rotterdamská univerzita, univerzita v Miláně, New Yorská univerzita a mnoho dalších. [13]

Obrázek 4: Titulní strana virtuálního světa Second Life. Zdroj: [25]

3.4 Second Life jako bezpečnostní hrozba

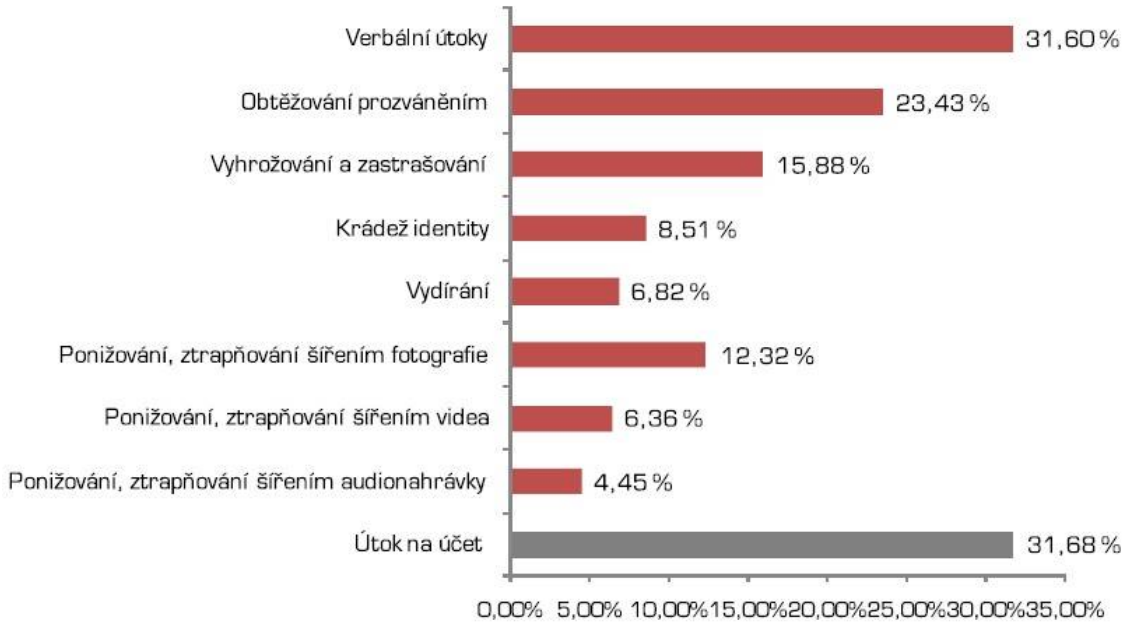
Americký Federální úřad pro vyšetřování (FBI) považuje on-line svět SL za bezpečnostní hrozbu. Jak uvádí zpráva agentury, hra slouží v mnoha případech ilegálním gangům k náboru nováčků a ke koordinaci kriminálních akcí. „Uživatelé komunikují přes textový chat v reálném čase. SL prokazuje víceúčelové anonymní prostředí a umožňuje bezpečnou komunikaci. Díky tomu členové gangu mohou potenciálně užívat SL k rekrutování, propagandě a dalším kriminálním aktivitám včetně pašování drog a tréninku pro zločiny v reálném životě," tvrdí zpráva FBI.

SL se objevil ve vyšetřování FBI už v minulosti, když v roce 2009 zkoumala virtuální hazard v jeho herních kasinech. Mimo to sama FBI využívala prostředí hry jak ke kontaktu s lidmi ohlašujícími zločiny, tak i k "vylepování" plakátů deseti nejhledanějších zločinců v USA. [26]

4 KYBERŠIKANA

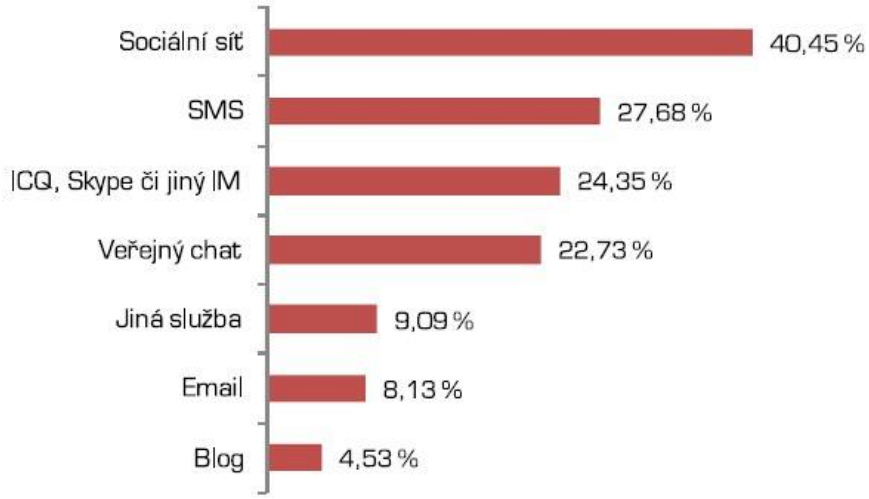
Jakmile jsou na internet jednou vloženy informace, je jen velmi těžké je posléze odstranit. Za určitých okolností může jít o výhodu, protože nelze snadno odstranit informace o problémech nebo trestných činech. Na druhé straně může být tato skutečnost nebezpečnou zbraní, kterou mohou ostatní využít v takovém rozsahu, že cílové osoby potřebují psychologickou pomoc. Ač se to nezdá, kybernetická šikana rozhodně není okrajovým jevem. Podle výzkumu v roce 2014 mezi 28 tisíci mladistvými, který zorganizovala Pedagogická fakulta Univerzity Palackého v Olomouci ve spolupráci se společností Seznam.cz a Google, má s kyberšikanou už zkušenost 51 % českých dětí.

Následující graf na obrázku 5 je z podobného výzkumu, který Univerzita Palackého v Olomouci podnikla roku 2012. Tehdy se výzkumu zúčastnilo bez mála 11 tisíc dětí v rozmezí 11-17 let. Nutno dodat, že procentuální výsledky nejčastějších forem kyberšikany, se v průzkumech roku 2012 a 2014 změnili jen minimálně. [27, 28]



Obrázek 5: Nejčastější formy kyberšikany u českých dětí. Zdroj: [29]

Pokud se zaměříme na platformy, prostřednictvím kterých došlo ke kyberšikaně, vedou jednoznačně sociální sítě. Je však nutné si zároveň uvědomit, že řada útoků probíhá souběžně ve více komunikačních prostředcích. [29]



Obrázek 6: Komunikační platformy kyberšikany. Zdroj: [29]

4.1 Ponížení na pracovišti

Kyberšikana ale není pouze problémem dospívajících. Podle studie Digitální život v práci, kterou připravila společnost AVG, už jí v práci zažilo přibližně 12 % Čechů. Za zásadní problém a klíčový rozdíl mezi konvenční a virtuální šikanou považují experti množství lidí, kteří ji mohou sledovat. Zatímco dříve se jednalo o lokální záležitost a problému bylo možné uniknout změnou zaměstnání, nyní může jít o globální problém. Jakmile se vaše citlivá nebo kompromitující data objeví na internetu, může na ně narazit kdokoliv, včetně vašeho budoucího zaměstnavatele. [27]

4.2 Následky kyberšikany

Důsledky těchto útoků provázejí oběti do konce života, následky mohou být různá psychická traumata, v některých případech i smrt oběti. Nejčastějšími prostředky používanými ke kyberšikaně jsou sociální sítě, chaty, e-maily či SMS a MMS zprávy atd. [30]

Ze života - typický příklad kyberšikany se odehrál roku 2014 v sousedním Německu. *Mladá dívka se na Facebooku seznámila s chlapcem, se kterým zpočátku pouze flirtovala. Postupně mu ale začala více věřit a svěřovat se mu s osobními záležitostmi, přičemž rozhovory mezi nimi se postupně začaly stávat více intimními. Přibližně po dvou měsících virtuálního vztahu, kdy spolu začali hovořit o prvním sexu, se měli setkat ve skutečnosti. Bohužel se ale ukázalo, že za mladého muže se vydávaly dívky z její třídy, které se o intimní informace dívky dělily i s ostatními spolužáky. Dívka přestala chodit do školy, žila*

v neustálém stresu, kde všude se mohou objevit informace o ní, a celá situace vygradovala jejím pokusem o sebevraždu a hospitalizací v psychiatrické léčebně. [27]

4.3 Kybergrooming

Tento termín označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, výrobě dětské pornografie apod. Kybergrooming je tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií.

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je závislá na důvěřivosti oběti a na způsobu manipulace s ní. Oběťmi jsou většinou děti a mladiství, nejčastěji ve věku 11 – 17 let. Častěji se oběťmi stávají dívky než chlapci.

4.4 Stalking

Obecně můžeme stalking chápat jako úmyslné pronásledování a obtěžování jedné osoby jinou, což oběti snižuje kvalitu jejího života a vyvolává u ní strach o bezpečí svoje nebo svých blízkých. Pachatel může oběť obtěžovat nejen přímým fyzickým kontaktem a sledováním, ale i zasíláním SMS, e-mailů, zpráv na sociálních a jiných sítích, zasíláním dárků, telefonáty apod. Tyto pokusy o kontakt pachatele s obětí nemusí zpočátku vykazovat prvky násilí či zastrašování, ale velmi snadno a rychle k nim sklouznou. Ze zpráv vyznávajících lásku a zasílání květin a dárků se mohou časem stát zprávy vyhrožující oběti či poškozování majetku oběti pachatelem, což u oběti v obou případech vyvolává důvodnou obavu. Tato obava působí velkou psychickou zátěž, která pak může vyústit v duševní i fyzické onemocnění oběti. [28]

Zákonná úprava: Zákon 40/2009 Sb. zavedl v lednu 2010 paragraf §354 týkající se stalkingu. Podle tohoto paragrafu může policie zakročit již v počátku problému, aby se zabránilo tomu, že pronásledování přeroste ve fyzické násilí. Od roku 2010 tak za nebezpečné pronásledování (a to i prostřednictvím mobilu, e-mailu, či např. Facebooku) hrozí trest v délce až 3 roky vězení.

5 ZÁKLADNÍ METODY STANOVENÍ RIZIK

V současnosti je k dispozici značné množství metod analýzy rizika, vyvinutých pro nejrůznější účely, takže výběr vhodné metody může představovat náročný problém. V následujícím textu je uveden příklad a stručná charakteristika vybraných metodických postupů.

Preliminary Hazard Analysis – PHA (předběžná analýza nebezpečí) vyhledává nebezpečné stavy či nouzové situace, jejich příčiny, dopady a řadí je do kategorií dle předem stanovených kritérií. Koncept PHA vlastně představuje soubor různých technik, vhodných pro posouzení rizika.

Checklist Analysis – CLA (analýza kontrolním seznamem) důsledně kontroluje plnění předem stanovených podmínek a opatření. Struktura seznamů se může měnit od jednoduchého až po složitý formulář.

What-If Analysis (analýza toho, co se stane když) je metoda založená na principu brainstormingu[9], klade volně strukturované otázky, nebo vyslovuje úvahy. Hledají se možné dopady vybraných provozních situací.

Safety Review (bezpečnostní prohlídka) se zaměřuje na systematickou identifikaci nebezpečí, s následným návrhem opatření vedoucím ke zvýšení bezpečnosti.

Hazard Operation Process - HAZOP (analýza nebezpečí a provozuschopnosti) je metoda založená na pravděpodobnostním hodnocení ohrožení a z nich plynoucích rizik. Hlavní cíl analýzy je identifikace scénářů potencionálního rizika, nejčastěji formou brainstormingu.

Failure Mode and Effect Analysis – FMEA (analýza chyb a jejich důsledků) je metoda založená na rozboru způsobů selhání a jejich důsledků. Využívá se především pro vážná rizika a zdůvodněné případy.

Relative Ranking – RR (relativní klasifikace) je spíše analytická strategie, která analytikům umožňuje porovnat vlastnosti několika procesů nebo činností a určit, zda mají natolik nebezpečné charakteristiky, že to analytiky opravňuje k další podrobnější studii.

---

[9] Brainstorming – metoda spontánní diskuze, sloužící ke generování množství nápadů na dané téma. Funguje většinou skupinově, ale zvládne ji i jednotlivec.

Process Quantitative Risk Analysis – QRA (analýza kvantitativních rizik procesu) jde o důsledný a komplexní přístup pro predikci odhadu četnosti a dopadů nehod pro zařízení nebo provoz systému. Vyžaduje náročnou databázi a počítačovou podporu.

Event Tree Analysis – ETA (analýza stromu událostí) dohlíží na průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou variant – příznivé a nepříznivé.

Fault Tree Analysis – FTA (analýza stromu poruch) je metoda založená na důsledném zpětném rozboru událostí pomocí řetězce příčin, které mohou vést k vybrané vrcholové události.

Human Reliability Analysis – HRA (analýza lidské spolehlivosti) je metoda využívaná k posouzení vlivu lidského faktoru na výskyt živelných pohrom, nehod, havárií, útoků apod., či jejich dopadů. Má těsnou vazbu na aktuální předpisy z hlediska bezpečnosti práce.

Fuzzy Set and Verbal Verdict Method (metoda mlhavé logiky verbálních výroků) je to multikriteriální metoda rozhodovací analýzy z kategorie měkkého a mlhavého typu. Umožňuje aplikaci jednotlivcem i kolektivu.

Causes and Consequences Analysis – CCA (analýza příčin a dopadů) vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod.

Probablistic Safety Assessment – PSA (metoda pravděpodobnostního hodnocení) určuje příspěvky jednotlivých zranitelných částí k celkové zranitelnosti systému. Technologii můžeme použít například k modelování scénářů jaderných havárií.

Z předešlých odstavců vyplývá, že nasazení technologií virtuální reality do metod identifikace rizik je v mnoha případech opodstatněné. Při vhodném způsobu použití umožní docílit kvalitativně hodnotnějších výstupů z analýz rizik. [31, 32]

PRAKTICKÁ ČÁST

6 BEZPEČNOST VE VIRTUÁLNÍM PROSTŘEDÍ

6.1 Internetová bezpečnost

75% evropských dětí používá internet, přičemž někteří lidé pějí chválu na jejich odborné znalosti v takto mladém věku, zatímco jiní se obávají, že jsou náchylnější k novým formám ohrožení. V současné době je důležité porozumět komplexní problematice online rizik, neboť použití internetu se stává stále více běžnou součástí života dětí a rodičů. Mezi rozšířené typy rizik, kterými jsou dnešní děti ohroženy, patří vystavení nevhodnému obsahu (např. pornografii, násilí, rasismu), nežádoucí kontakt (např. flirtování, sexuální obtěžování, zastrašování, zneužití osobních údajů, narušování soukromí) a nevhodné chování, kterého se dopouštějí samotné děti (např. zastrašování, šikana).

Je potřeba zavést opatření založená na faktech, díky nimž by nastala rovnováha mezi cíly maximalizovat příležitosti a zároveň minimalizovat rizika. Pojďme si tedy zmíněné příležitosti a rizika představit ve formě tabulky. [33]

Tabulka 3: Klasifikace online příležitostí a rizik pro děti. Zdroj: [34]

		Obsah: Dítě jako adresát	**Kontakt: Dítě jako účastník**	**Chování: Dítě jako aktér**
PŘÍLEŽITOSTI	**Vzdělání, studium a digitální gramotnost**	Vzdělávací zdroje	Kontakt s ostatními, kteří sdílí zájmy konkrétního dítěte	Samostatně iniciované nebo kolaborativní učení
	Participace a občanská angažovanost	Globální informace	Výměna v rámci zájmových skupin	Konkrétní formy občanské angažovanosti
	Kreativní a sebevyjádření	Rozmanitost zdrojů	Dítě je vyzváno/inspirováno aby něco vytvořilo, nebo se na něčem podílelo	Vytváření obsahu uživatelem
	Identita a sociální zapojení	Rada (osobní/ohledně zdraví/sexu, atd.)	Sociální sítě, sdílení zkušeností s ostatními	Vyjádření identity
RIZIKA	**Komerční**	Reklama, spam, sponzorování	Vyhledávání/sběr osobních informací („harvesting“)	Hazardní hry, nelegální stahování, hackerství
	Agresivní	Násilný/hrůzný/ nenávistný obsah	Šikanování, harassment (obtěžování), nebo stalking (nebezpečné pronásledování)	Šikanování nebo obtěžování jiných
	Sexuální	Pornografický/škodlivý sexuální obsah	Setkávání se s cizími lidmi, lákání na schůzku	Tvoření/přenášení pornografického materiálu do počítače/na internet
	Hodnotová	Rasistické, zkreslené informace/rady (např. ohledně drog)	Sebepoškozování, nežádoucí přesvědčování	Poskytování rad např. ohledně sebevraždy/proanorektických

6.1.1 Rizika veřejných Wi-Fi sítí

Prakticky ihned po připojení našeho přístroje k síti musíme počítat s hrozícími nebezpečími. Na nejvyšší úrovni je lze rozdělit na nebezpečí, která hrozí přenášeným datům a nebezpečí, která hrozí připojeným zařízením. [35]

Nebývalý rozmach, který v poslední době zažívají bezplatné veřejné Wi-Fi sítě, je pro všechny, kteří k práci potřebují internet, skutečným požehnáním. Jelikož jsou tyto bezplatné přístupové body k dispozici v restauracích, hotelích, knihkupectvích, na letištích a dokonce v některých maloobchodech, od přístupu k vaší síti a pracovním záležitostem vás obvykle dělí jen pár kroků. Používání otevřených Wi-fi sítí na veřejných místech ale rozhodně není bezpečné. Vlastnosti, díky nimž jsou přístupové body bezplatných Wi-Fi sítí lákavé pro spotřebitele, jsou lákavé i pro hackery – především fakt, že pro navázání spojení nevyžadují žádné ověření. Nedostatečné zabezpečení Wi-fi může snadno vést k tomu, že budou vyzrazena vaše citlivá data, která po internetu odesíláte. Největším rizikem zabezpečení bezplatných Wi-Fi sítí je to, že útočník se může dostat mezi vás a přístupový bod. Místo komunikace přímo s přístupovým bodem pak své informace posíláte hackerovi, který je předává dál. Proto není rozumné používat na Wi-fi v kavárně či třeba na nádraží internetové bankovnictví nebo se například přihlašovat k e-mailové schránce. [36, 37]

6.1.2 Osvětou proti nástrahám internetu

Dle nového průzkumu společnosti AVG Technologies většina dnešních českých dětí ve věku deseti let už se svými rodiči mluvila o sexu. To je až o pět let dříve, než měla stejnou rozmluvu generace jejich rodičů, přičemž většina z nich (v ČR dokonce až 53 %) si nepamatuje, že by takovou diskuzi vůbec kdy vedla.

Internet byl označen jako nejčastější „spouštěč“ rozhovorů s dětmi o věcech jako je porno, sex nebo puberta. Co se týče dětského surfování na internetu, největší starostí českých rodičů je, že děti netráví dost času venku (52 %) a také to, jak snadné pro ně je se na internetu dostat k nevhodnému obsahu (48 %).

Aby alespoň zčásti pomohla s řešením těchto problémů, vytvořila společnost AVG sérii interaktivních digitálních knih pro děti různého věku nazvanou Magda a Mo. Ta je věnována především problematice internetové bezpečnosti, kterou dětem vysvětluje zábavnou a přístupnou formou. Knihy jsou tvořeny ve spolupráci s dobročinnou organizací Childnet

International a jsou vydávány v několika jazycích. Průzkum AVG poukázal na zmatek rodičů v tom, jak nejlépe ochránit své děti na internetu. [38]

6.1.3 EU Kids Online

Jde o mezinárodní studie zaměřené na zkoumání problematiky online rizik a bezpečnosti na Internetu u dětí a rodičů v Evropských státech. Projekt koordinuje London School of Economics and Political Science (LSE). V České republice je projekt realizován pod vedením doc. PhDr. Davida Šmahela, Ph.D. na Institutu výzkumu dětí, mládeže a rodiny na Fakultě sociálních studií Masarykovy univerzity.

EU Kids Online zkoumá praxi dětí i rodičů v souvislosti s používáním Internetu. Projekt vychází z kritického srovnávacího přístupu a klade důraz na zachycení širšího kontextu celé problematiky. Hlavním cílem projektu je sestavení a realizace mezinárodního kvantitativního průzkumu zaměřeného na dětskou zkušenost s online riziky a porovnání pohledu dětí s vnímáním rizik a bezpečnostních postupů u rodičů.

Výzkumné týmy, které se zapojily do výzkumu, pocházely ze zemí:

Rakouska, Belgie, Bulharska, Kypru, České republiky, Dánska, Estonska, Finska, Francie, Německa, Řecka, Maďarska, Irska, Itálie, Litvy, Nizozemí, Norska, Polska, Portugalska, Rumunska, Slovinska, Španělska, Švédska, Turecka a Velké Británie.

Zástupci českého výzkumného týmu:

David Šmahel, Štěpán Konečný, Lukáš Blinka, Anna Ševčíková, Petra Vondráčková, Alena Černá, Hana Macháčková, Věra Kontríková a Lenka Dědková. [34]

Klíčová zjištění průzkumů EU Kids online

- Čím více děti používají internet, tím více získávají digitálních dovedností a tím větší šance mají z hlediska online příležitostí a získání benefitů.
- Šance dětí získat díky používání internetu výhodu a přidanou hodnotu, záleží na jejich věku, pohlaví, socio-demografickém statusu, způsobu, jak jim v této oblasti pomáhají rodiče a na množství a kvalitě stránek s pozitivním obsahem, které jsou pro ně k dispozici.

- Využívání internetu dětmi, jejich znalosti, vědomosti i online příležitosti také přímo souvisí s online riziky. Čím více zkušeností s internetem děti mají, tím více jsou vystaveny riziku.
- Potenciální riziko rozrušení anebo ohrožení online obsahem je u dětí částečně závislé na jejich věku, pohlaví, sociálně-ekonomickém statusu, a také na jejich odolnosti a zdrojích, které jsou k dispozici ke zvládnutí všech (škodlivých) událostí v prostředí internetu.
- Důležitá je role rodičů, školy a vrstevníků, ale také provádění regulace na národní úrovni, poskytování obsahu, kulturní hodnoty a systém vzdělávání.
- Nejvíce děti v oblasti online znepokojuje pornografie.
- Násilí, agresivita, krutost a brutalita jsou v těsném závěsu, i když násilí má méně obecné pozornosti než sexuální materiály.
- Co děti mimořádně znepokojuje je realita (nebo realističnost), a to více než fiktivní násilí, a násilí páchané na dětech a zvířatech.
- Obavy dětí z online rizik výrazně rostou ve věku od devíti do dvanácti let. Mladší děti se více obávají rizik souvisejících s obsahem, čím jsou starší, tím více se obávají rizik kontaktu a projevů chování na internetu.
- Děti vnímají stránky zaměřené na sdílení videí jako nejvíce rizikové z hlediska výskytu pornografie, násilí a dalších forem škodlivého obsahu [33]

7 UŽITÉ METODY ANALÝZY RIZIK

Při analýze rizik bezpečnosti ve virtuálním prostředí jsem aplikoval dvě metody WHAT-IF a CHECK LIST.

7.1 WHAT-IF (Co se stane když)

Analýza toho, co se stane když, je metoda na hledání možných dopadů vybraných provozních situací. Prakticky se jedná o spontánní diskusi a hledání nápadů, ve které skupina zkušených lidí dobře obeznámených s procesem, klade otázky nebo vyslovuje úvahy o možných nehodách či rizicích. Nejedná se o vnitřně strukturovanou techniku, jako některé jiné (např. HAZOP a FMEA). Namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept šetření určitému účelu. [39]

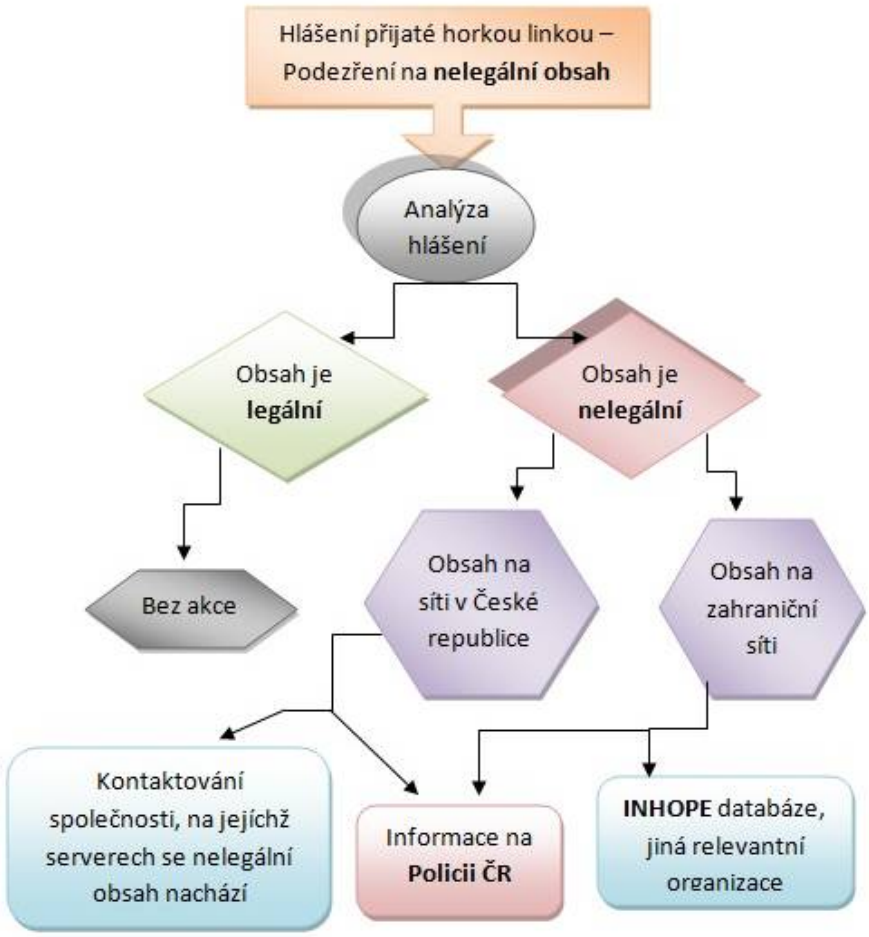
Na obrázcích 7 a 8 můžeme vidět metodu What-If ve dvou grafických znázorněních.

Obrázek 7: *Nahlášení nelegálního obsahu na síti* - za zdroj rizika můžeme v tomto případě považovat jakýkoliv obsah nelegálního charakteru, tj. takového, který je v rozporu se zákonem (např. dětská pornografie.). Graf na obrázku znázorňuje koloběh událostí, který se po nahlášení podezřelého obsahu roztočí. Přijatá zpráva se zkušenými odborníky horkých linek vyhodnotí (analyzuje) a po té se postupuje dle vykreslené metody.

Vysvětlivky pojmů použitých v obrázku 7:

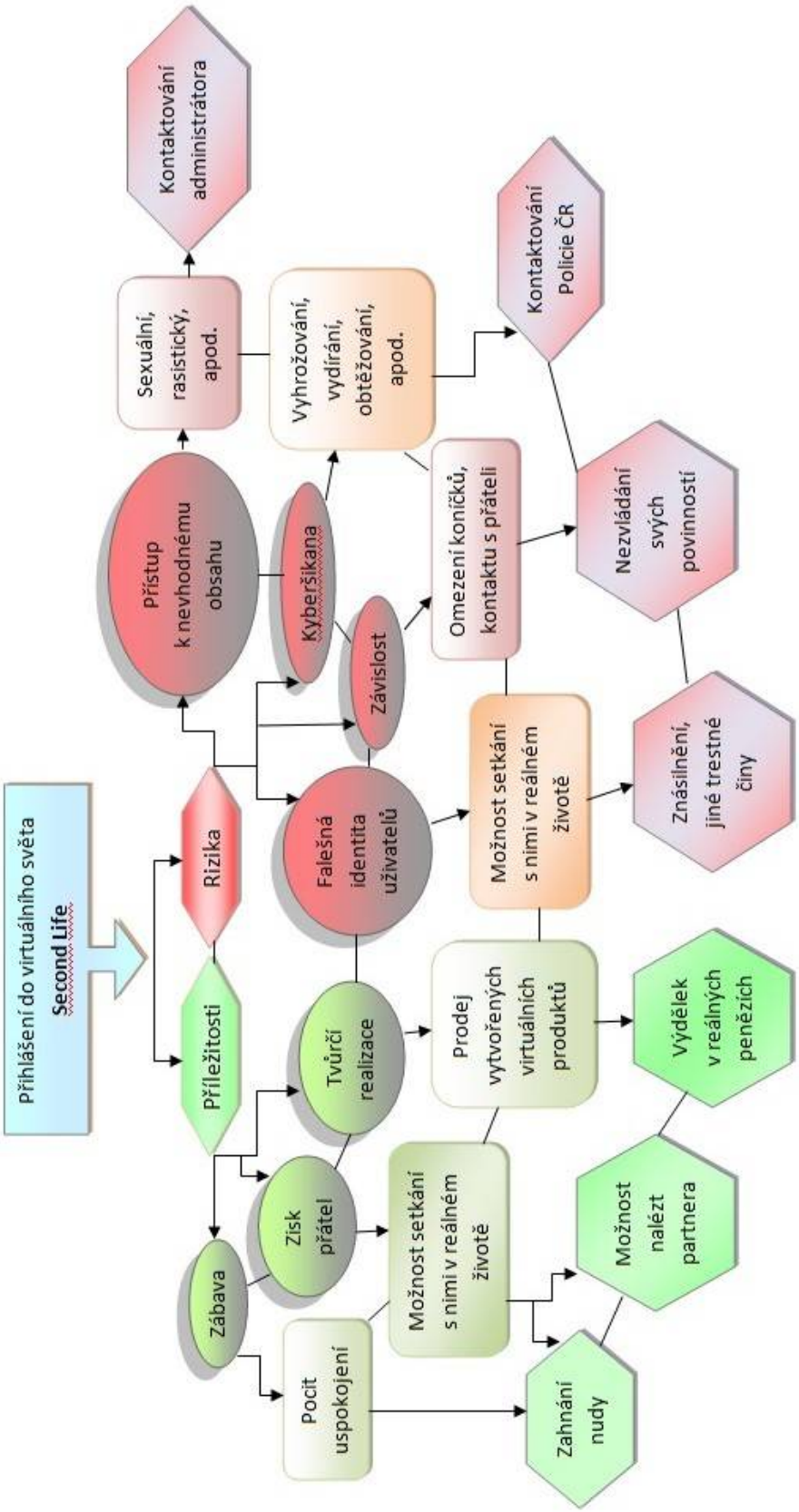
Horká linka – nízkoprahové kontaktní centrum pro příjem hlášení týkajícího se nezákonného obsahu na internetu, zejména dětské pornografie a kyberšikany páchané na dětech.

INHOPE - mezinárodní síť horkých linek. [40]



Obrázek 7: Metoda What-If. Nahlášení nelegálního obsahu na síti. Zdroj: [18]

Obrázek 8: *Koloběh událostí po vstupu do SL* – zdrojem rizika, je zde už samotný vstup do virtuálního světa, (chcete-li hry) Second Life. Ten nám samozřejmě kromě zmíněných rizik, přináší i řadu příležitostí. „Co se stane když“ do SL vstoupíme, nám tedy podrobně znázorňuje následující obrázek. Kromě analýzy rizik vykresluje i následná doporučení, jak nenadálé situace řešit.



Obrázek 8: Metoda What-If. Koloběh událostí po vstupu do SL. Zdroj: Vlastní.

7.2 CHECK LIST (kontrolní seznam)

Kontrolní seznam je postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek jsou zpravidla generovány na základě seznamu charakteristik sledovaného systému nebo činností, které souvisejí se systémem a potencionálními dopady, selháním prvků systému a vznikem škod. Jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout různou relativní důležitost parametru (váhu) v rámci daného souboru. [39]

RIZIKO NAPADENÍ DÍTĚTE PEDOFILEM		HODNOCENÍ	
Riziko	**Otázka**	**Ano**	**Ne**
Nepravdivé a zavádějící informace	Jsou získané informace dostatečně prověřeny?		x
Zneužití osobních údajů.	Je ochrana soukromí na dostatečné úrovni?		x
Přílišná důvěra k neznámým osobám	Je dítě naučeno nedůvěřovat neznámým lidem?		x
Zasílání materiálů intimního charakteru	Jsou dítěti vysvětlena rizika takového počínání?		x
Falešná identita uživatele	Je prověření identity neznámé osoby dostatečné?		x

Tabulka 4: Check list – Zdroj: Vlastní.

Kontrolní seznam v tabulce 4, nám zobrazuje rizika spojená s navazováním kontaktu s cizím člověkem. Tato modelová situace nám navozuje scénář, kdy se dítě ocitne v hledáčku osoby s pedofilními sklony. V tabulce 4 v sekci „Hodnocení“, byla vybrána v každém z pěti případů varianta „Ne“. Tak byly navozeny sice málo pravděpodobné, zároveň však nejpříhodnější podmínky pro navázání kontaktu pachatele s obětí. Tabulka tak odkazuje na odstavec 4.3 – Kybergrooming.

7.2.1 Výpočet míry rizika

Analýza rizik je první krok v procesu řízení rizik. Jedná se o proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich

závažnosti. Cílem je minimalizace možných škod a snaha vyhnout se ztrátám. K tomu jsou ale potřeba patřičné informace, které je nutno na základě analýzy vytvořit a získat tak podklady pro ovládání rizika a pro rozhodování o možném riziku. [41]

Pravděpodobnost vzniku rizika - P		Počet bodů
Velmi nízká	Mizivá hrozba	1
Nízká	Málo pravděpodobná hrozba	2
Střední	Reálná hrozba	3
Vysoká	Vysoká hrozba	4
Velmi vysoká	Neúměrně vysoká hrozba	5

Tabulka 5: Pravděpodobnost míry rizika. Zdroj: Vlastní.

Tabulka 5 určuje pravděpodobnost vzniku rizika. Analyzuje a vytipovává hrozby, které mohou připadat v úvahu. Při identifikaci hrozeb vycházíme z vlastních zkušeností, metod brainstormingu, literatury či dřívějších analýz.

7.2.2 Závažnost následků rizika

Nalezená nebezpečí a jejich možné následky charakterizuje tabulka 6.

Závažnost následků rizika - N		Počet bodů
Navázání kontaktu s neznámou osobou	Riziko, že neznámou osobou bude osoba s pedofilními sklony.	1
Zvětšující se intenzita psaní textových zpráv	Zvětšující se posedlost potencionálního pachatele.	2
Přeposlání vlastních intimních fotografií či videí	Riziko zneužití – vydírání, vyhrožování.	3
Přijmutí darů	Pachatel cítí větší sebedůvěru, ví, že oběť k němu chová sympatie.	4
Přijmutí nabídky ke schůzce	Vražda, znásilnění, jiné formy fyz. napadení.	5

Tabulka 6: Závažnost následků rizika. Zdroj: Vlastní.

7.2.3 Výsledná míra rizika

V tabulce 7 můžeme vidět výslednou míru rizika, která se vypočte jako součin pravděpodobnosti rizika a závažnosti možných následků (R = P x N). Míra rizika je konkrétním výstupem rizikové analýzy, na jehož základě jsou následně stanovena příslušná bezpečnostní opatření a určena jejich priorita.

R = P x N		**Závažnost následků - N**				
		a = 1	b = 2	c = 3	d = 4	e = 5
Pravděpodobnost vzniku rizika - P	Velmi nízká	1	2	3	4	5
	Nízká	2	4	6	8	10
	Střední	3	6	9	12	15
	Vysoká	4	8	12	16	20
	Velmi vysoká	5	10	15	20	25

Tabulka 7: Výsledná míra rizika. Zdroj: Vlastní.

7.2.4 Shrnutí metody Check List

Míra rizika 1 – 4: Riziko je přijatelné, je potřeba minimálních bezpečnostních opatření. Tato rizika však nesmíme bagatelizovat.

Míra rizika 5 – 11: Rizika musíme dále sledovat v rámci správy rizik a přijmout příslušná opatření.

Míra rizika 12 – 25: Nutnost přijetí okamžité nápravy, jedná se o nejvyšší prioritu. Dopady mohou mít tragické a nezvratné následky. [42]

7.3 Metodika závěrečné práce

Při tvorbě bakalářské práce jsem užil těchto metod:

Syntéza (z řec. syn-thesis, skládání) jde o myšlenkové spojení poznatků získaných analytickými metodami v celek. Syntéza je sumarizací poznatků vedoucí k získání nových poznatků, vztahů a zákonitostí ve kvalitativně vyšší úrovni – objasňuje nové nebo dříve nedefinované vztahy a zákonitosti.

Indukce (z lat. inductio – uvádění) je vyvozování obecného (teoretického) závěru na základě poznatků o jednotlivostech. Závěry induktivních myšlenkových pochodů jsou vždy ovlivněny subjektivními postoji (zkušenostmi, znalostmi) a mají proto omezenou platnost. Východiskem indukce je statistické zpracování a vyhodnocení údajů, na jejichž základě formulujeme obecnější závěry platné pro zkoumanou oblast.

Dedukce (lat. deductio – odvození) jde o proces, ve kterém testujeme, zda vyslovená hypotéza je schopna vysvětlit zkoumaný fakt. Indukce a dedukce spolu úzce souvisí, indukcí dospíváme k teoretickým zobecněním na základě zkoumání jednotlivých jevů z praxe, a naopak si můžeme teoretické závěry dedukcí ověřit v praxi.

Sběr dat je shromažďování informací k určitému tématu z nejrůznějších zdrojů, které jsou následně centralizovány, přenášeny či zpracovány. Skládá se především z činností indikace prvotní informace, vytvoření sdružené informace, přenos a příprava ke zpracování.

Dotazování můžeme rozčlenit na ústní (rozhovory), písemné (dotazníkové šetření) a elektronické či telefonické. Všem druhům dotazování je společný vysoký význam volby typu a formulace otázek, které mohou ovlivnit celkovou kvalitu i výsledky provedeného výzkumu. [43]

8 PRŮZKUM VEŘEJNÉHO MÍNĚNÍ

8.1 Výhody a nevýhody dotazníkového šetření

Jedním z druhů získávání informací je písemné dotazování – dotazník či anketa (dle adresnosti dotazování). Mezi hlavní výhody lze uvést finanční nenáročnost, rychlost, ale i odstranění případného nežádoucího vlivu tazatele na respondenta. Hlavními nevýhodami jsou zejména nemožnost kontroly podmínek vyplnění (kdo byl skutečně respondentem, vnější rušivé vlivy apod.) a celkově nižší návratnost tohoto nástroje. Vzhledem k rozšířenosti těchto technologií je tento přístup využíván i k zajištění reprezentativních výzkumů. [43]

8.2 Cíle dotazníku

Cílem je získat poznatky ohledně zkušeností široké veřejnosti všech věkových kategorií s online technologiemi a zjistit tak jejich povědomí o rizicích a bezpečnosti ve virtuálním prostředí. Dále se zaměřuji na hry typu MMORPG, konkrétně na virtuální svět Second Life a na rizika spojená s užíváním internetu. Obecně vzato, zda jsou si lidé vědomi reálných hrozeb a rizik, která na ně a hlavně na dospívající generaci ve virtuálním světě číhají.

8.3 Sběr a vyhodnocení dat

Dotazník se skládá z 24 otázek, z nichž u otázky č. 10 *„Jakou činností trávíte na počítači (tabletu) nejvíce času?“* měl respondent možnost uvést vlastní odpověď, pokud si nevybral ze stanovených možností. Další otázkou, která se svou formou odlišovala od ostatních, bylo č. 20. *„Pokud ano, jaké konkrétně?“*. Šlo o nepovinnou otázku, která disponovala možností zatrhnout větší množství odpovědí v případě, že respondent odpověděl v předchozím dotazu kladně. Konkrétně bylo jejím úkolem doplnit otázku č. 19 *„Byl(a) jste někdy sám(a) obětí kyberšikany?* Rozšíření otázky č. 20 o možnost označení více odpovědí, bylo záměrné s ohledem na fakt, že útoky formou kyberšikany jsou proti obětem často vedeny několika způsoby současně a navzájem se doplňují. Např. publikování ponižujících fotografií je v mnoha případech doprovázeno vyhrožováním či zastrašováním. Všech zbylých 22 otázek v dotazníku, bylo koncipováno do jasné formy vymezených odpovědí, kdy bylo možno vybrat vždy jen jednu z 2-6 variant, v návaznosti na typu otázky. Z důvodu úspory místa, jsem u otázek s jednoznačnými odpověďmi „Ano“ a „Ne“, neaplikoval vý-

sledky do prstencových grafů. Ty byly použity pouze pro lepší přehlednost u otázek s větším množstvím odpovědí.

Dotazník vytvořený v programu MS Word, jsem poté vložil na portál **survio.com**, který se tvorbou dotazníků zabývá a přišel mi svou formou nejpřehlednější a uživatelsky nejpřívětivější. Dotazník jsem šířil pomocí přímého odkazu a to zprvu u rodinných příslušníků a přátel, následně pak prostřednictvím facebookových skupin „Týdeník policie“ a „Co mě štve i těší v Uherském Hradišti“. Od prvního do posledního vyplnění dotazníku uběhlo 7 dnů, za tuto dobu stihlo formulář vyplnit na 820 respondentů z celého území ČR. Doba pro vyplnění dotazníku se nejčastěji pohybovala v rozmezí 2-5 minut, jak je patrno z tabulky 6. Po dosáhnutí dostatečného množství odpovědí, jsem nasbíraná data analyzoval a převedl do finálních grafů pomocí programu MS Excel. Takto zpracované statistiky ve formě prstencových grafů, pak už jen stačilo zanést přímo do bakalářské práce. Zde jsem mohl pomocí filtrů jednotlivé výsledky dále rozvádět a poskytnout tak čtenáři podstatně širší úhel pohledu na řešenou problematiku.

Čas vyplňování	**Počet respondentů**
Méně jak **1** min.	0 (**0 %**)
1–2 min.	28 (**3,3 %**)
2-5 min.	614 (**75 %**)
5-10 min.	135 (**16,5 %**)
10-30 min.	27 (**3,2 %**)
30-60 min.	7 (**0,9 %**)
Více jak **60** min.	9 (**1,1 %**)

Tabulka 8: Čas potřebný k vyplnění dotazníku. Zdroj: Vlastní.

Týdeník policie – Zpravodajská skupina založená roku 2012 na sociální síti Facebook. Jedná se o žurnalistickou stránku, prezentující práci složek IZS. Je provozována civilními osobami a nespadá nijak pod Polici ČR. V roce 2014 skupina obsadila 7. Místo v anketě Křišťálová lupa v kategorii Zpravodajství (Cena českého internetu oceňující nejob-

líbenější a nejzajímavější projekty a služby českého internetu za uplynulý rok). Jakožto příslušníkovi bezpečnostních sborů, mi bylo administrátorem skupiny nabídnuto sdílení mého dotazníku na hlavním panelu týdeníku s mým komentářem: *„Ahojte, jsem momentálně na ZOPce v Holešově a po odpolednech dopisuji bakalářku. Do praktické části jsem pak vytvořil dotazník ..kdyby jste si našli 5 minut a vyplnili jej, byl bych vám vděčný. Díky všem, co pomůžou!“*

Čtenář týdeníku Brenyx Bob k mému dotazníku např. napsal: *„konečně dotazník, který nebyl jako od mého zaměstnavatele“*.

Co mě štve i těší v Uherském Hradišti – Jedná se o uzavřenou skupinu (komunitu) lidí, která ve městě Uherské Hradiště (dále jen UH) žije, nebo se o něj nějakým způsobem zajímají. Uživatelé zde např. diskutují o tom, co je v jejich městě těší, s čím jsou naopak nespokojeni, nebo sdílejí různé informace a dotazy týkající se UH. Dotazník jsem zde sdílel se slovy: *„Hezký den všem, rád bych vás touto cestou poprosil o vyplnění dotazníku, zahrnutého v praktické části mé bakalářky. Je to skutečně jen na pár minut. Studuji v UH na UTB-FLKŘ, obor Ovládání rizik. Díky za váš čas.“*

Barevné složení prstenců je ve všech případech dle stejného klíče. Odpověď, která získala největší počet procentních bodů, je vždy označena červenou barvou, následována barvou modrou. Třetí nejfrekventovanější odpověď je označena zeleně, čtvrtá pak žlutě. Pátá, tedy jedna z možností s nejmenším počtem hlasů má růžové zbarvení, paletu barev následně uzavírá šestá, šedá.

8.4 Výsledky zjištěné dotazníkovým šetřením

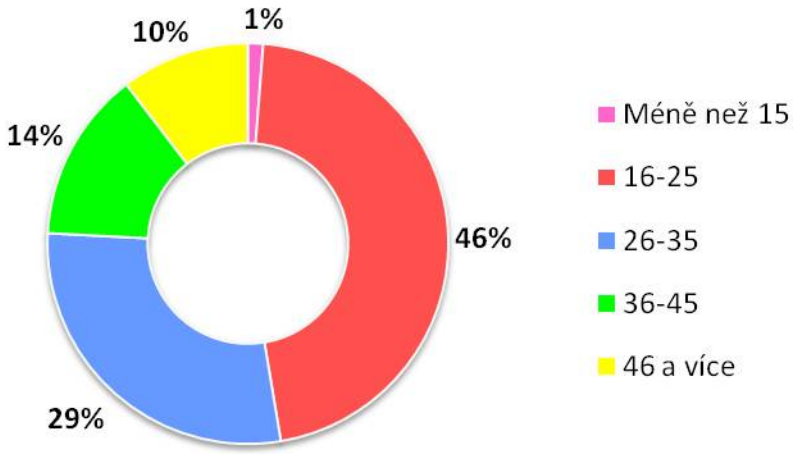
Jak jsem již zmínil o několik odstavců výše, výzkumného šetření se zúčastnilo 820 respondentů, kteří odpovídali na 24 otázek. První čtyři otázky se přímo netýkaly bezpečnosti ve virtuálním prostředí, ale měly za úkol zjistit pohlaví, věk, vzdělání a společenské postavení dotazovaných.

Otázka č. 1 – Respondentem je:

Z celkového čísla dotazovaných, je zastoupení žen a mužů takřka vyrovnané, tedy 433 žen (52,8 %) ku 387 mužům (47,2 %). Díky tomu mají získaná data nepoměrně vyšší vypovídající hodnotu, než by tomu bylo v případě nerovnoměrného zastoupení obou pohlaví.

Otázka č. 2 – Do jaké věkové skupiny patříte?

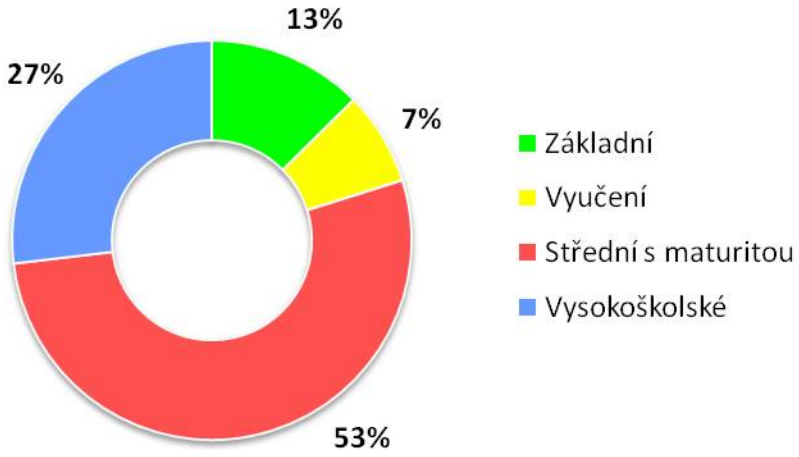
Nejpočetnější věkovou skupinu dotazovaných 16-25 let (46,1 %) nám znázorňuje obrázek 9.



Obrázek 9: Věkové rozhraní. Zdroj: Vlastní.

Otázka č. 3 – Nejvyšší dosažené vzdělání (řádně ukončené):

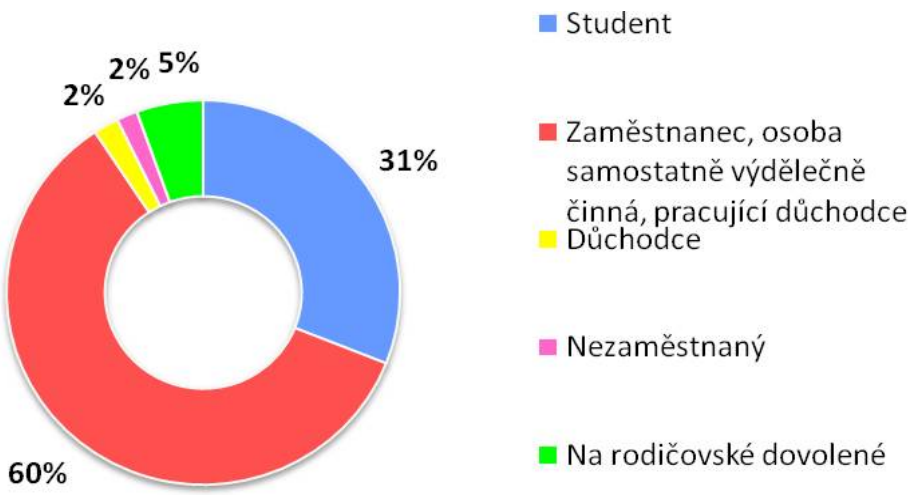
Z obrázku 10 se můžeme dozvědět, že nejčastěji zastoupenou kategorií v oblasti vzdělání, jsou lidé se střední školou s maturitou (52,9 %), následováni vysokoškolsky vzdělanou populací (26,8 %).



Obrázek 10: Nejvyšší dosažené vzdělání. Zdroj: Vlastní.

Otázka č. 4 – Nynější společenské postavení:

Na obrázku 11 je průkazné, že majoritní skupinou respondentů jsou lidé zaměstnaní, OSVČ – Osoby samostatně výdělečně činné, či pracující důchodci (59,8 %). Spolu se studenty pak tvoří 90,8 % všech dotazovaných.



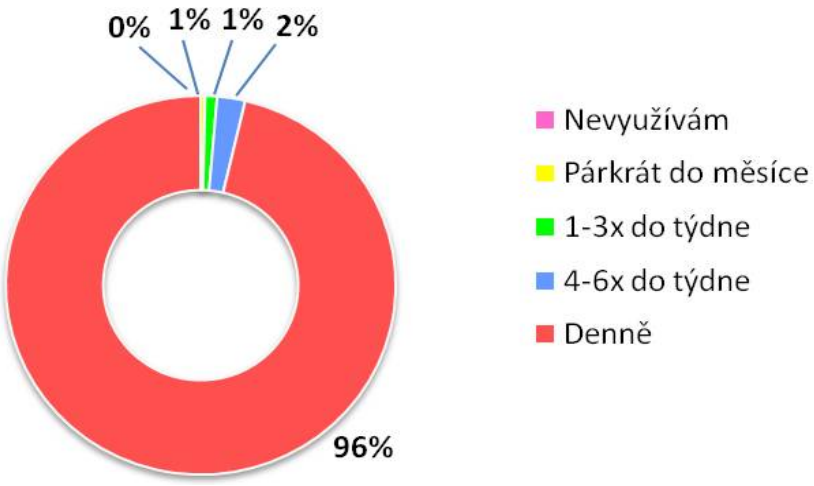
Obrázek 11: Společenské postavení. Zdroj: Vlastní.

Od následující otázky se dotazník začal fakticky zaobírat bezpečností ve virtuální realitě. Zpočátku je zaměřen na prostředí internetu a Wi-Fi sítí, poté se dále dotýká témat, rozebíraných v bakalářské práci.

Otázka č. 5 – Jak často využíváte internet?

V dnešní době už není tolik velkým překvapením, že dle statistik ročenky 2015 rozsáhlého průzkumu NetMonitor, je ve věkové kategorii 10-24 let na internetu 96 % lidí. S rostoucím věkem pak podíl na internetu klesá. Pouze 42 % lidí starších 55 let využívá internet. [44]

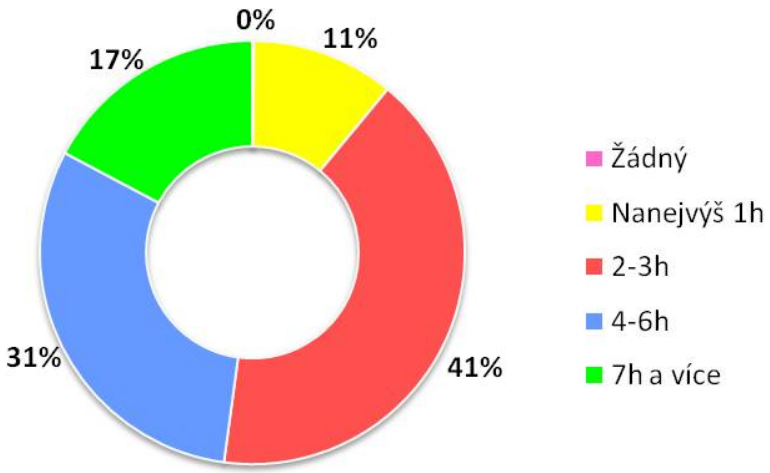
Jak můžeme vidět na obrázku 12, až 96, 3 % (790 z 820 respondentů) užívá internet denně, což je vzhledem k různorodému věkovému složení poměrně úctyhodné číslo, které dokazuje, jak důležitou roli internet v našem každodenním životě zastupuje.



Obrázek 12: Četnost využívání internetu. Zdroj: Vlastní.

Otázka č. 6 – Kolik času denně strávíte na internetu?

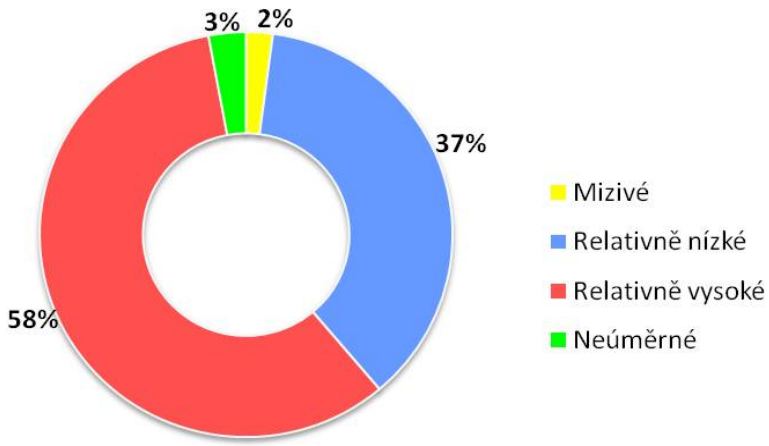
Dle výsledků by se dalo říci, že lidé nejčastěji tráví na internetu 2-3h času denně, což by nebylo nijak šokující zjištění. Pokud se ale podíváme na graf pozorněji, zjistíme, že až 48% populace tráví denně v prostředí internetu nejméně 4h, často však ještě mnohem více. Trend dnešní doby je jasný, čas takto strávený se stále prodlužuje a nemalou měrou k tomu nepochybně přispívá i rozmach tzv. „smartphonů“, tedy chytrých telefonů, často vybavených připojením k internetu. Není pak překvapením, že v kategorii 16-25 let jsou lidé 4h a více připojeni už skoro v 57 % případů. U respondentů ve věku 46 let a více, pak tato míra klesá na „pouhých“ 33 %.



Obrázek 13: Čas strávený na internetu za den. Zdroj: Vlastní.

Otázka č. 7 – Jak hodnotíte riziko spojené s užíváním internetu?

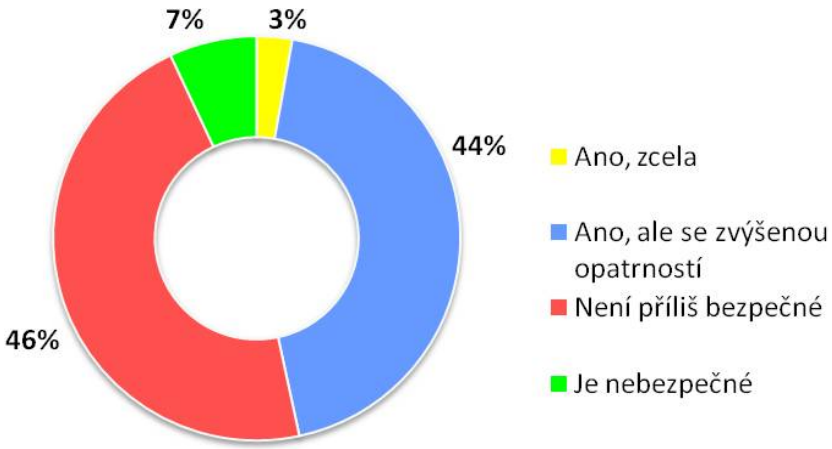
Grafické znázornění nám ukazuje, že větší část dotazovaných považuje riziko spojené s užíváním internetu za relativně vysoké (58 %), další 3% pak za neúměrné. Z analýzy získaných dat mimo jiné vyplynulo, že riziko spojené s užíváním internetu, považuje za relativně vysoké, či neúměrné mnohem více žen (70,9 %), než mužů (50,1 %).



Obrázek 14: Hodnocení rizika spojeného s užíváním internetu. Zdroj: Vlastní.

Otázka č. 8 – Myslíte si, že je užívání veřejných Wi-Fi sítí bezpečné?

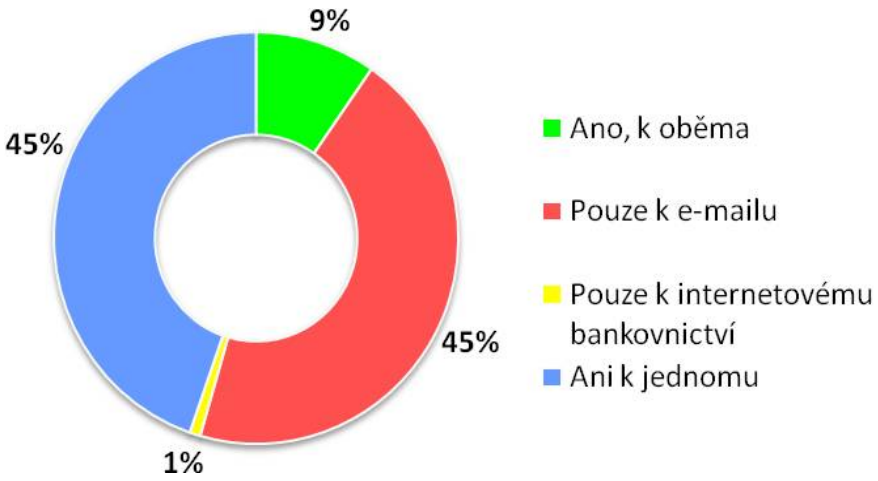
Souhrnný výsledek ukazuje, že 47 % dotazovaných, považuje veřejné Wi-Fi sítě za bezpečné se zvýšenou opatrností, popř. za zcela bezpečné. Naproti tomu, 53 % je vnímá jako ne příliš bezpečné, či dokonce nebezpečné. Vzniká nám tedy zajímavá situace, kdy se respondenti v návaznosti na bezpečnost veřejných Wi-Fi sítí dělí na dva tábory. Pozitivní stránkou věci je, že lidé si jsou možných rizik vědomi. Přinejmenším jsou na veřejných Wi-Fi sítích obezřetní.



Obrázek 15: Bezpečnost veřejných Wi-Fi sítí. Zdroj: Vlastní.

Otázka č. 9 – Přihlašujete se někdy na veřejných Wi-Fi sítích k e-mailu či internetovému bankovnictví?

V návaznosti na předchozí graf, je u lidí patrná jistá míra uvědomělosti. Pouhé 1 % z nich, se totiž na veřejných Wi-Fi sítích připojuje k internetovému bankovnictví. Přitom je průkazné, že obliba této služby v ČR stále roste. Podle výzkumu Eurostatu (statistický úřad Evropské unie), využívalo internetové bankovnictví v roce 2014 na 46 % obyvatel ČR. V celé Evropské unii (EU 28) činil ve stejném roce tento podíl 44 %, přičemž nejvíce mají severské státy (Island 91 %, Norsko 89 %, Finsko 86 %) a nejméně Rumunsko (4 %) a Bulharsko (5 %). [45]

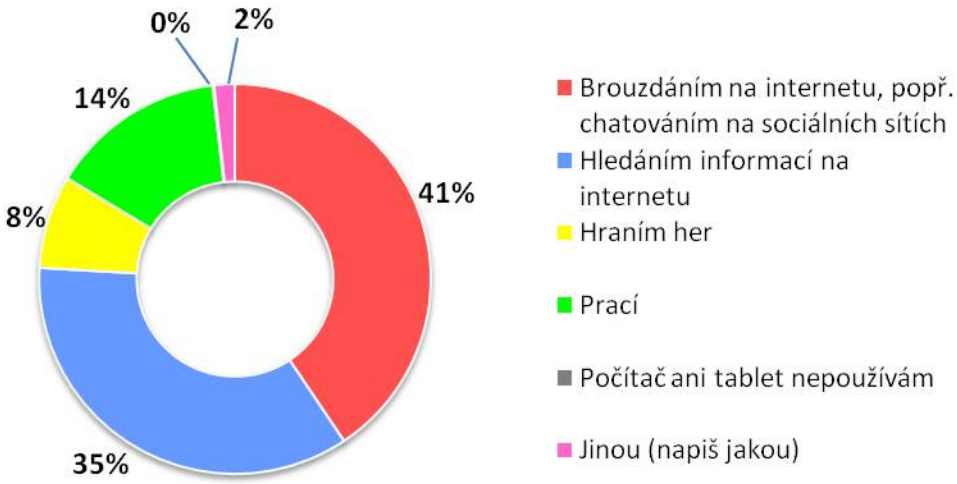


Obrázek 16: Veřejné Wi-Fi sítě, e-mail a internetové bankovnictví. Zdroj: Vlastní.

Otázka č. 10 – Jakou činností trávíte na počítači (tabletu) nejvíce času?

Z tohoto grafu je patrné, že nejvyšší procento dotázaných na svém pc či tabletu vyplňuje svůj čas brouzdáním na internetu, popř. chatováním na sociálních sítích (Facebook, Twitter, Instagram, Myspace atd.). Je však nadmíru jasné, že druh vykonávané činnosti se podstatně mění ve vztahu k věku respondentů či faktu, zda jsou lidé v práci, doma apod. Pokud tedy vyfiltrujeme získaná data podle věku, zjistíme, že např. čas strávený brouzdáním či chatováním se s přibývajícím věkem postupně snižuje: 16-25 let (51,6 %); 26-35 let (33,9 %); 36-45 let (29,8 %); 46 a více let (20 %).

Přesně opačnou tendenci má u dotazovaných činnost „Hledání informací na internetu“. Ta má s přibývajícím věkem naopak vzrůstající tendenci: 16-25 let (23 %); 26-35 let (39,1 %); 36-45 let (48,2 %); 46 a více let (55,3 %).



Obrázek 17: Nejčastější činnost na pc a tabletu. Zdroj: Vlastní.

Pod možností „Jinou“ respondenti nejčastěji odpovídali (seřazeno dle četnosti odpovědí):

- Studiem
- Sledováním videí, filmů či seriálů
- Sledováním pornografických materiálů
- Posloucháním hudby
- Kontrolou e-mailu
- Zálohováním videí a fotografií
- Kombinací zadaných variant

Otázka č. 11 - Omezil(a) jste někdy kvůli času strávenému ve virtuálním prostředí (internet, hry apod.) některé své zájmy (kulturní, sportovní, rekreační)?

V 72,4 % odpovědí respondenti uvedli, že své zájmy neomezili. Kladně na tuto otázku odpovědělo pouze 27,6 % z nich, z čehož bylo procentuálně nepatrně více mužů, než žen. Je tedy zřejmé, že ačkoliv lidé tráví ve virtuálním prostředí stále více času, neděje se tak příliš na úkor jejich volnočasových aktivit.

Pokud se podíváme na výše zmíněná procenta ve vztahu k otázce č. 6: „Kolik času denně strávíte na internetu?“, zjistíme, že mezi hodnotami je přímá úměra. Tedy čím více času člověk stráví denně na internetu, tím více má tendence omezovat své volnočasové zájmy. K lepší přehlednosti nám poslouží vytvořená tabulka.

Čas strávený respondenty denně na internetu	**Lidé, kteří omezili své zájmy, kvůli času strávenému ve VR**
Nanejvýš 1h	8/89 (9 %)
2-3h	79/337 (23,4 %)
4-6h	85/251 (33,9 %)
7h a více	54/142 (38 %)

Tabulka 9: Statistika přímé úměry. Zdroj: Vlastní.

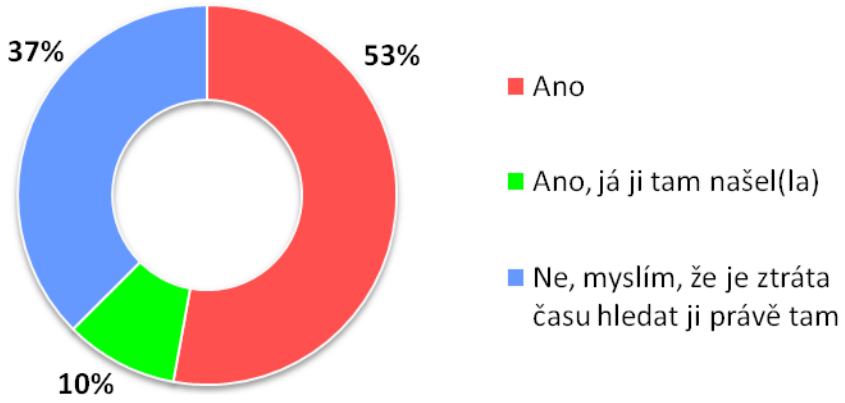
Otázka č. 12 - Zkoušel(a) jste někdy ve virtuálním prostředí (seznamky, online hry apod.) nalézt partnera(ku)?

Z výsledků vyplývá, že ve virtuálním prostředí se pokoušelo nalézt partnera či partnerku 40,6 % dotazovaných. 59,4 % se o to dosud nepokusilo. Je jasné, že údaj není zcela průkazný, ve smyslu naleznutí partnera ve virtuálním prostředí. Řada lidí se totiž ve VR neseznámila jen kvůli záměru naleznout vhodného partnera. Jejich vztah mohl vznikat postupně, např. díky alianční komunikaci v online hře apod.

Pokud nás však zajímá jen údaj, kolik respondentů se ve VR pokoušelo nalézt partnera, pak je vypovídající hodnota zcela průkazná. Nikoho pak nepřekvapí fakt, že usilovnějšími „hledači“ jsou muži (45 %), než ženy (36,7 %). Nejčastěji jsou to lidé ve věkové skupině 26-35 let (50,2 %).

Otázka č. 13 - Myslíte si, že se dá ve virtuálním prostředí najít životní láska?

K uvedeným datům lze snad jen dodat, že životní lásku by ve virtuálním prostředí hledalo zhruba o 9 % více mužů, než žen. Věk respondentů tentokrát nehrál při rozhodování příliš významnou roli, snad jen věková kategorie 46 a více let, byla v této otázce mírně skeptičtější, než mladší lidé.



Obrázek 18: Životní láska ve virtuálním prostředí. Zdroj: Vlastní.

Otázka č. 14 - Měl(a) jste někdy podezření, že osoba, se kterou si píšete (na chatu, ve hře, emailem, formou sms), není tím, za koho se vydává?

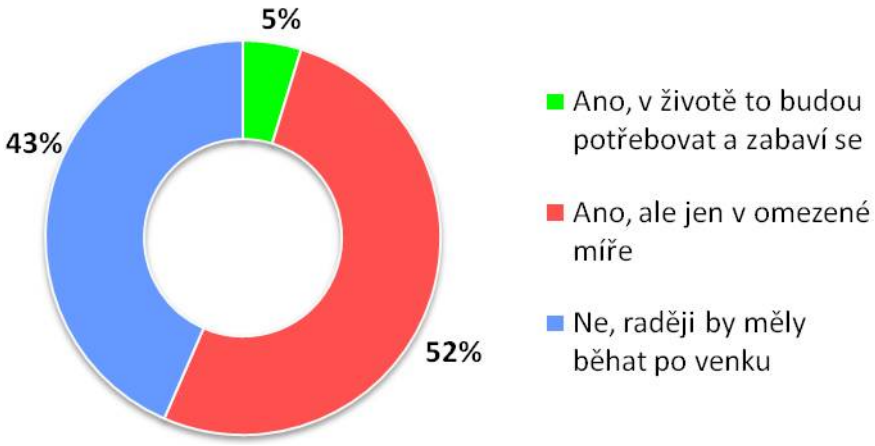
Ano – 438 respondentů (53,4 %); **Ne** – 382 respondentů (46,6 %)

V tomto případě hraje věk respondentů opět důležitou roli. Čím jsou lidé starší, tím méně mají zkušeností s podezřením na falešnou identitu. 16-25 let (58,7 %); 26-35 let (55,4 %); 36-45 let (43,9 %); 46 a více let (37,6 %). Výsledná data si můžeme vysvětlit tak, že s přibývajícím věkem už lidé provozují hraní online her, nebo chatování v podstatně menší míře, než je tomu u mladší populace. Tím se logicky snižuje rozsah míst pro setkání s falešnou identitou.

Otázka č. 15 - Je dle Vás správné, aby už od útlého věku děti pracovaly s počítačem, smartphonem či tabletem?

Z uvedeného prstence vyplývá, že jen minimum lidí, by od útlého věku dalo dítěti do rukou počítač, tablet, či chytrý telefon tak, aby se zabavilo a stalo se při práci s ním zručnější. Větší část dotazovaných, by tak svolilo jen v omezené míře.

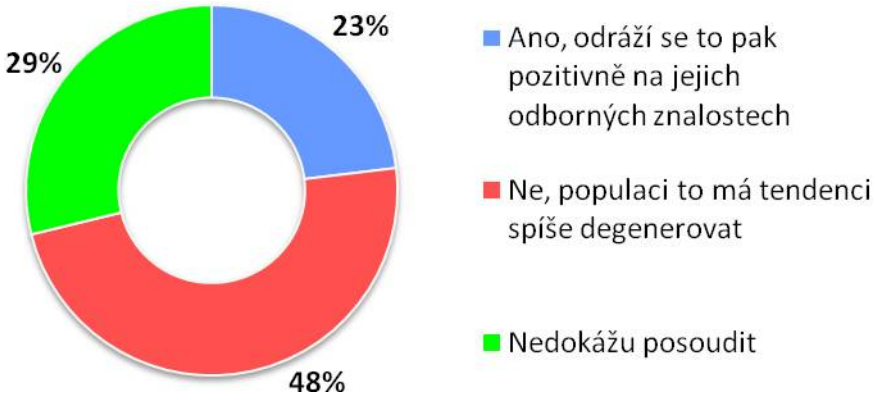
Z filtrovaných dat jsem dále zjistil, že muži by nechali děti běhat po venku pouze ve 36,7 %, kdežto ženy ve 49,7 %. O poznání vícekrát, také muži označili první možnost, že takto nabité zkušenosti budou děti v životě potřebovat a zabaví se (34 respondentů - 8,8 %), oproti ženám (5 respondentek - 1,2 %). Tyto statistiky dle mého částečně svědčí o tom, že muži mají k technice blíže. Proto by tímto směrem častěji vedli i své ratolesti.



Obrázek 19: Práce dětí s pc, tabletem a smartphonem. Zdroj: Vlastní.

Otázka č. 16 - Myslíte si, že v dnešní době moderních technologií, je pro dospívající přínosem čas strávený na internetu?

Z procentuálního vyjádření následujícího grafu je zřejmé, že téměř polovina respondentů si myslí, že internet dospívající populaci spíše degeneruje. Pouhých 23 % dotazovaných má opačný názor a 29 % situaci nedokáže posoudit.

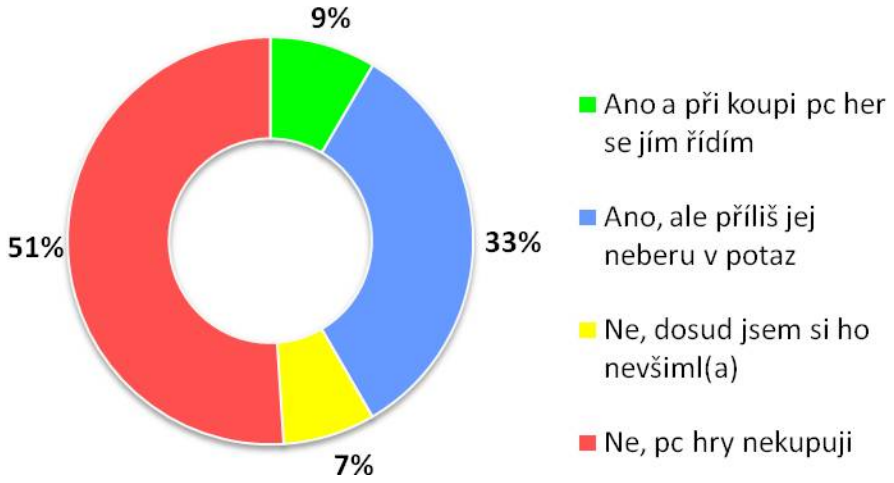


Obrázek 20: Přínos času stráveného na internetu - dospívající. Zdroj: Vlastní.

Otázka č. 17 - Znáte systém PEGI? (*Obal pc hry je dle jejího obsahu označen příslušným piktogramem a číslem určující věk, od kterého je vhodné počítačovou hru hrát*)

Systém, který má podporu Evropské komise a je považován za model evropské harmonizace na poli ochrany dětí už v ČR tolik známý není. [20] Alespoň se to dá tvrdit dle výsledků dotazníkového šetření, ze kterého je zřejmé, že 58 % respondentů o něm dosud neslyšelo. Pouze 9 % lidí jej pak bere při nákupu v potaz.

Zajímavý je však značný rozdíl mezi odpověďmi žen a mužů. Zatímco u mužského zastoupení zná tento systém bez mála 66 % dotazovaných a 26,9 % z nich pc hry nekupuje, u žen zná systém PEGI pouhých 20,1 % respondentek a nákupy v tomto odvětví nepodniká 72,7 % z nich. Získaná data tedy potvrzují známý fakt, že prostředí pc her je mnohem větším lákadlem pro mužskou část populace.



Obrázek 21: Systém PEGI. Zdroj: Vlastní.

Otázka č. 18 - Byl(a) jste někdy ve svém okolí svědkem kyberšikany?

Svědky kyberšikany bylo dle výsledků 39,1 % dotazovaných. Zbylých 60,9 % jí ve svém okolí nezažilo. I když se jedná o menší část z celkového počtu respondentů, dá se říci, že hranice 40 % je velmi vysoké číslo. Nutno dodat, že kyberšikana je před našimi zraky většinou skryta, tím spíše je pak takto vysoké procento jejích svědků alarmující.

Otázka č. 19 - Byl(a) jste někdy sám(a) obětí kyberšikany?

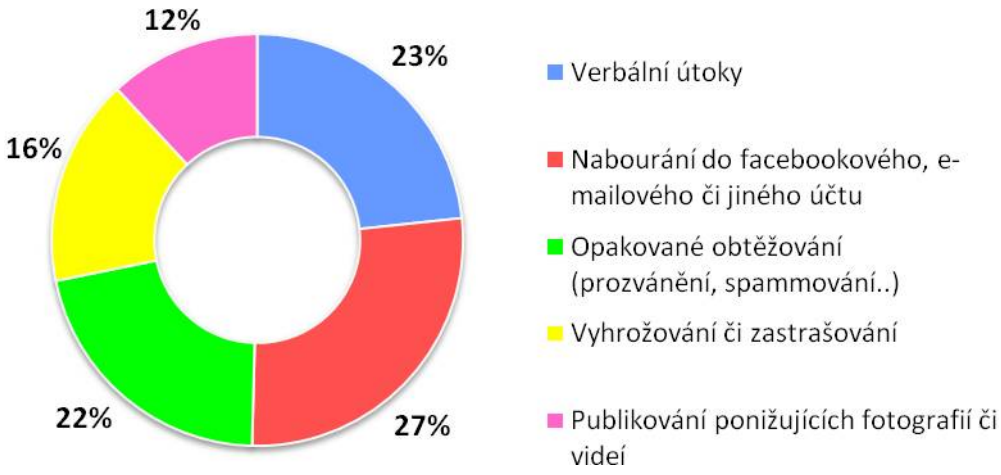
Z odpovědí jednotlivých respondentů vyplývá, že obětí kyberšikany se stalo 13,3 % z nich. Konkrétně 11,6 % mužů a 14,8 % z řad žen. Pokud se na tuto problematiku zaměříme z hlediska věku, zjistíme, že kyberšikana je problémem především mladší generace, tedy dětí. Dle šetření tohoto dotazníku, ji zažilo 7 z 10 dětí do 15 let (70 %); 14,8 % lidí ve věku 16-25 let; 12% lidí ve věku 26-35 let; 14% lidí v kategorii 36-45 let a 7,1 % respondentů ve věku 46 a více let.

Dalším zjištěním po filtraci dat je, že pokud respondenti odpověděli, že byli svědky kyberšikany, tak 26,5 % z nich bylo zároveň i její obětí. V opačném případě, kdy s kyberšikanou ve svém okolí lidé zkušenosti neměli, jich bylo současně jejími oběťmi „jen“ 4,8 % z nich.

Procentuální rozdíl mezi lidmi, kteří kyberšikanu viděli ve svém okolí a kteří ji skutečně zažili na vlastní kůži, si vysvětluji několika způsoby. Zejména skutečností, že v případě zveřejnění ponižujících fotografií, je má možnost vidět velké množství lidí, zatímco oběť je pouze jedna. Stejně tak urážení a ponižování oběti, může ve virtuálním prostředí přihlížet větší množství jinak nezúčastněných diváků.

Otázka č. 20 – Pokud ano, jaké konkrétně? (Je možno zatrhnout více odpovědí)

Jak již bylo psáno v úvodním popisu dotazníkového šetření, tato otázka byla jako jediná dobrovolná a reagovali na ni pouze respondenti, kteří v předchozí otázce odpověděli kladně. Tedy, že se v minulosti stali oběťmi kyberšikany. Ačkoliv v tomto průzkumu veřejného mínění odpovídali i děti, větší procento respondentů je z řad dospělých. Ani tato skutečnost však neměla výrazný vliv při hodnocení četnosti jednotlivých druhů kyberšikany. Lze proto říci, že následující graf (až na drobné odchylky) dává za pravdu statistice uvedené na obrázku 5.



Obrázek 22: Druhy kyberšikany dle jejich četnosti. Zdroj: Vlastní.

Otázka č. 21 - Lákala Vás někdy myšlenka, žít svůj druhý život ve virtuálním světě „neomezených možností“?

Jelikož může být pro mnohé z nás obtížné, něco si pod touto otázkou představit, pomůckou budiž americký snímek „Náhradníci“ (Surrogates) [46], ze kterého jsem při tvorbě otázky vycházel. Mnoho lidí si ale může představit pod pojmem virtuální svět např. MMORPG hru World of Warcraft, nebo Second Life. Člověk měl tedy v této otázce možnost zapojit svou fantazii.

Pokud se podíváme na výsledek dotazníkového šetření, jednoznačně nám z něj plyne, že pouze malou část respondentů (17,7 %) by lákala možnost žít druhý život ve virtuálním světě. Následným filtrováním výsledků jsem zjistil, že častěji by tato možnost lákala muže (25,1 %), než ženy (11,1 %). Velkou roli při rozhodování, má opět věk respondentů. Čím je člověk mladší, tím častěji na otázku č. 21 odpověděl kladně. Do 15 let (50 %); 16-25 let (23,5 %); 26-35 let (16,7 %); 36-45 let (8,8 %); 46 a více let (2,4 %).

Otázka č. 22 - Pohltil Vás někdy virtuální prostor natolik, že jste omezil(a) kontakty v reálném světě?

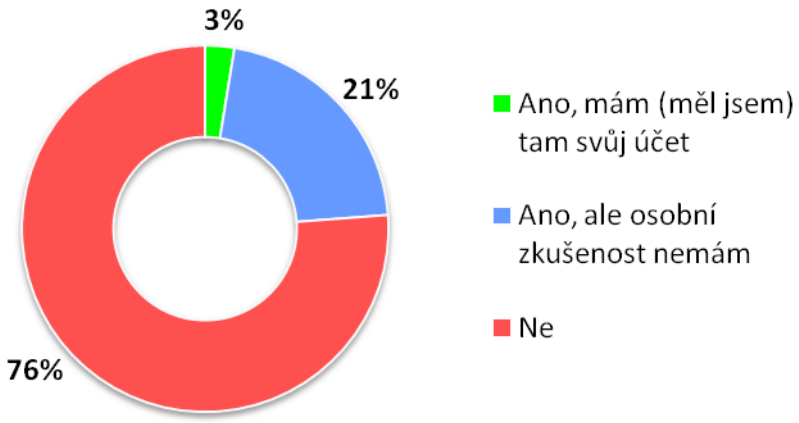
Na tento dotaz odpovědělo kladně 12,3 % respondentů a 87,7 % záporně. Po filtraci dat se už jako v jiných případech potvrdila přímá úměra. Čím více času člověk strávil denně na internetu, tím častěji byl schopen omezit kontakty v reálném světě. Pro lepší přehlednost nám opět poslouží vytvořená tabulka.

Čas strávený respondenty denně na internetu	**Lidé, kteří omezili kontakty, kvůli času strávenému ve VR**
Nanejvýš 1h	2/89 (2,2 %)
2-3h	27/337 (8 %)
4-6h	38/251 (15,1 %)
7h a více	34/142 (23,9 %)

Tabulka 10: Statistika přímé úměry. Zdroj: Vlastní.

Otázka č. 23 - Slyšel(a) jste už někdy o virtuálním světě (hře) „Second Life“?

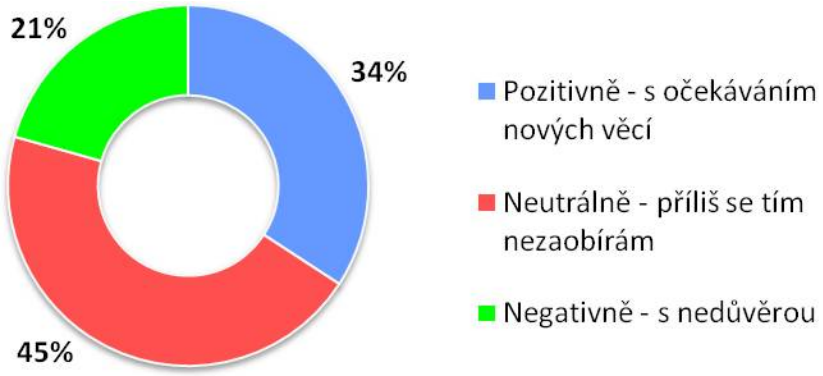
Úkolem této otázky bylo, zjistit povědomí dotazovaných o virtuálním světě SL. Výsledky ukazují, že jej zná 23,8 % respondentů, tedy bez mála čtvrtina všech dotázaných. Konkrétně 32,6 % mužů a 15,9 % žen. Rozdělení dle věkové kategorie v tomto případě nehrálo příliš velkou roli, jako tomu bylo u některých předchozích dotazů. Výsledky sice naznačují, že SL zná větší procento mladších lidí (méně než 15 let – 30 %), než starších (46 a více let – 16,5 %), ale toto pravidlo neplatí u všech daných věkových kategorií. Nabízí se zde jednoduché vysvětlení. Svět SL dokáže svými možnostmi nalákat skutečně široké spektrum hráčů všech věkových kategorií, z nichž si každý dokáže najít svůj vhodný objekt zájmu.



Obrázek 23: Povědomí o virtuálním světě Second Life. Zdroj: Vlastní.

Otázka č. 24 - Jak vnímáte technologický pokrok lidstva, tedy život stále více spjatý s elektronickými vymožeností?

Technologický pokrok provázel lidstvo od nepaměti a vždy jej kromě očekávání a nadšení provázela i skepse. Jinak tomu není ani v současné době. Více než kdy dřív dnes platí, že technologický pokrok lidstva stále zrychluje. Zvětšuje se rychlost i množství přenášených informací, narůstá míra stresu. Názory respondentů nám přibližuje obrázek 24.



Obrázek 24: Vnímání technologického pokroku lidstva. Zdroj: Vlastní.

Z dále selektovaných dat zjistíme, že muži vnímají současný technologický pokrok o poznání lépe než ženy. Pozitivně na něj nahlíží 49,4 % z nich, neutrálně 35,9 % a s nedůvěrou pouhých 14,7 %. U žen jsou data následující: Pozitivně - 20,6 %; neutrálně - 53,6 % a negativně 25,9 %.

9 NÁVRHY A DOPORUČENÍ

Na základě zjištěných informací, lze doporučit následující:

Utíkat a skrývat se před riziky virtuálního světa, je stejně špatný nápad, jako utíkat a skrývat se před problémy ve světě reálném. Ačkoliv se hrozby virtuálního světa nikdy nepodaří úplně vymýtit, můžeme se proti nim alespoň účinně bránit dodržováním několika málo zásad.

- Zabezpečit své soukromé údaje před zneužitím (např. účet na sociálních sítích)
- Nepracovat zbytečně na veřejných Wi-Fi sítích s citlivými daty
- Ověřovat si získané informace z více zdrojů
- Používat antivirové programy
- Vždy počítat s rizikem falešné identity osoby, se kterou jsme ve VR v kontaktu

9.1 Rady pro rodiče

Krokem k většímu bezpečí dětí v online světě, je v první řadě zvýšení povědomí rodičů. Pokud jsou děti příliš omezovány, nestanou se tak vůči rizikům odolnější, naopak ztratí možnost využívat příležitostí on-line světa. Namísto zákazu, by se právě rodiče měli o aktivity svých dětí ve virtuálním prostředí více zajímat. Nejlépe je tyto úkony provádět ještě před dosažením puberty dítěte. Čím dříve si dítě bezpečnostní pravidla vštípí, tím lépe se bude umět zachovat v situacích, kdy mu hrozí nebezpečí.

- Informujte se o výhodách i hrozbách, které s užíváním internetu souvisí a podporujte děti už od raného věku v objevování online světa
- Zaměřte se na to, aby vaše děti posilovaly své digitální dovednosti, a zvyšovaly tak svou odolnost vůči potencionálním rizikům
- Pravidelně hovořte s dětmi o tom, s čím se setkávají na internetu a co může být problematické
- Používat antivirové programy
- Stanovte jasná pravidla upravující chování dětí v online prostředí

ZÁVĚR

Cíl práce spočíval ve vymezení pojmu bezpečnosti ve virtuální realitě se zaměřením na Second Life. Právě Second Life (druhý život), však umožňoval dvojí pojetí dané problematiky. Jednak uvedení do virtuálního světa (hry) s MMORPG prvky, kde jsou lidé reprezentování prostřednictvím svých avatarů a současně šlo o přiblížení druhé života lidí ve virtuální realitě v obecném slova smyslu.

Vybrané téma bakalářské práce má tedy velmi široký záběr a nesčetnou škálu oblastí, jimiž se dá zabývat. Hledíc na omezenou kapacitu obsahu práce, jsem se tedy dotknul jen některých z mnoha aspektů bezpečnosti ve virtuálním prostředí. Čtenáři jsem se pokusil zprostředkovat zejména virtuální realitu z pohledu uživatelů internetu. Právě ti jsou riziky virtuálního prostředí dotčeni nejvíce, zejména dospívající část populace. Děti jsou v prostředí internetu velmi ohroženou skupinou. Jsou často otevřeny novým věcem, tráví v online světě nejvíce času a v neposlední řadě mají tendence být velmi důvěřivé. Nejdůležitější složkou prevence je tedy komunikace s rodiči, kteří by je měli poučit o možných rizicích virtuálního prostředí.

Internet je totiž velmi mocný nástroj, který využívají milióny uživatelů ze všech koutů světa. Slouží jim k vyhledávání informací, práci i zábavě, ke komunikaci a k navazování sociálních vztahů s dalšími lidmi. Skrývá však také řadu nebezpečí, kterým mohou být jeho uživatelé vystaveni. Nejrozšířenějšími hrozbami jsou kyberšikana, kybergrooming či stalking. Význam těchto pojmů byl rozveden v teoretické části práce a do jisté míry jej můžeme najít v otázkách dotazníkového šetření, jež bylo náplní praktické části. Právě získaná a vyhodnocená data z dotazníku, byla pro práci největším přínosem. Díky množství respondentů, kteří se dotazníkového šetření zúčastnili, mají výsledky vysokou vypovídající hodnotu a jsou tak zajímavé pro laickou i odbornou veřejnost.

Při výběru metod analýzy rizik, jež měly být další nedílnou součástí práce, jsem se rozhodl pro užití metody What-If (Co se stane když) a Check List (kontrolní seznam). Tvorbu grafů a tabulek jsem zaměřil na tématiku nahlášení nelegálního obsahu na síti, vstupu do virtuálního světa SL a nakonec rizika napadení dítěte osobou s pedofilními sklony. V poslední části práce, byla navrhnuta doporučení k zajištění větší bezpečnosti ve virtuálním prostředí. Těmito kroky jsem dle mého úsudku splnil zadání a vytyčené cíle bakalářské práce.

SEZNAM POUŽITÉ LITERATURY

[1] Žára, J.; Beneš, B.; Sochor, J.; Felkel, P.: Moderní počítačová grafika. Computer Press, a.s., Brno: 2004, ISBN 80-251-0454-0.

[2] AUKSTAKALNIS, Steve a David BLATNER. *Reálně o virtuální realitě: umění a věda virtuální reality*. Brno: Jota, 1994. Nové obzory (Jota). ISBN 80-856-1741-2.

[3] LÉVY, Pierre. *Kyberkultura: zpráva pro Radu Evropy v rámci projektu "Nové technologie: kulturní spolupráce a komunikace"*. Vyd. 1. V Praze: Karolinum, 2000. ISBN 80-246-0109-5.

[4] NOVOTNÝ, Tomáš. *Dizertační práce: Využití technologie virtuální reality v analýze rizik a bezpečnosti výrobních strojů* [online]. Brno, 2013 [cit. 2016-04-21]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=62617. Vysoké učení technické v Brně. Vedoucí práce Doc. Dr. Ing Radek Knoflíček.

[5] *Svět hardware: Přehled headsetů pro virtuální a rozšířenou realitu* [online]. Brno: oXy Online, 2016 [cit. 2016-04-21]. Dostupné z: http://www.svethardware.cz/prehled-headsetu-pro-virtualni-a-rozsirenou-realitu/40915

[6] BOWEN, David, ELLIOT, Joe (ed.). *Multimédia: podrobný průvodce : [virtuální realita, trojrozměrné hry, Internet, World Wide Web, CD-ROM a informační superdálnice*. 1. čes. vyd. Ilustrace Jay Coneyl. Praha: Albatros, 1997. ISBN 80-000-0528-X.

[7] *Oculus Rift* [online]. Irvine, California: Oculus, 2016 [cit. 2016-03-14]. Dostupné z: https://www.oculus.com/en-us/blog/oculus-rift-pre-orders-now-open-first-shipments-march-28/

[8] *Herní konzole* [online]. Liberec: Heureka Shopping, 2016 [cit. 2016-03-14]. Dostupné z: http://prislusenstvi-herni-konzole.heureka.cz/oculus-rift-xbox-one/specifikace/#section

[9] BÜSCHER, Barbara, Martin FLAŠAR, Jana HORÁKOVÁ a Petr MACEK. *Umění a nová média*. Vyd. 1. Brno: Masarykova univerzita, 2011. ISBN 978-80-210-5639-8.

[10] *Husova Praha: Maroldovo panorama* [online]. Praha: Prag City Tourism, 2016 [cit. 2016-04-21]. Dostupné z: http://www.husovapraha.cz/

[11] STEPHENSON, Neal. *Sníh*. Překlad Tomáš Hrách. Praha: Talpress, 2000. ISBN 80-719-7109-X.

[12] STROSS, Randall E. *Planeta Google: o troufalém plánu jedné firmy organizovat všechno, co známe*. Vyd. 1. Brno: Computer Press, 2009. ISBN 978-80-251-2412-3.

[13] *KUČÍRKOVÁ, Petra. Second Life: Motivace uživatelů ke vstupu a setrvání a jejich vnímání této virtuální komunity* [online]. Brno, 2009 [cit. 2016-04-24]. Dostupné z: http://is.muni.cz/th/216394/fss_b/?lang=en. Masarykova univerzita, Fakulta sociálních studií.

[14] TURKLE, Sherry. *Life on the screen: identity in the age of the Internet*. 1st Touchstone ed. New York: Touchstone Book, 1997. ISBN 06-848-3348-4.

[15] ŠMAHEL, David. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton, 2003. Psychologická setkávání. ISBN 80-725-4360-1.

[16] GACKENBACH, Jayne (ed.). *Psychology and the Internet: intrapersonal, interpersonal, and transpersonal implications*. San Diego: Academic Press, c1998. ISBN 01-227-1950-6.

[17] MACEK, Petr. *Adolescence: psychologické a sociální charakteristiky dospívajících*. Vyd. 1. Praha: Portál, 1999. ISBN 80-717-8348-X.

[18] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.

[19] *Národní centrum bezpečnějšího internetu* [online]. Praha: Saferinternet.cz, 2011 [cit. 2016-03-29]. Dostupné z: http://archiv.saferinternet.cz/pro-deti/hry

[20] *PEGI: Pan-European Game Information* [online]. Belgium - Brussels: ISFE, 2003 [cit. 2016-04-9]. Dostupné z: http://www.pegi.info/cs/index/

[21] PETRUŠKOVÁ, Kateřina. *Vztahy a sociální interakce v MMORPG World of Warcraft* [online]. Plzeň, 2011 [cit. 2016-04-22]. Dostupné z: https://otik.uk.zcu.cz/bitstream/handle/11025/3274/bakalarska_prace_Petruskova.pdf?sequence=1. Bakalářské práce. Fakulta filozofická Západočeské univerzity v Plzni.

[22] *Komunikace virtuálně* [online]. Brno: Havlena, 2009 [cit. 2016-04-22]. Dostupné z: http://www.havlena.net/ekonomie/komunikace-virtualne-masarykova-univerzita-a-second-life-sl/

[23] BRUNS, Axel. *Blogs, Wikipedia, Second life, and Beyond: from production to produsage*. New York: Peter Lang, c2008. Digital formations, vol. 45. ISBN 978-0-8204-8867-7.

[24] HÁJÍČEK, Martin a Lukáš VESELOVSKÝ. *Virtuální ekonomika v kontextu Evropské unie* [online]. Brno, 2011 [cit. 2016-04-22]. Dostupné z: https://www.law.muni.cz/sborniky/cofola2011/files/IT/eGovernment/Hajicek_Martin_6325.pdf

[25] *Second Life* [online]. MMOHuts, 2016 [cit. 2016-04-24]. Dostupné z: http://mmohuts.com/game/second-life

[26] *Bonusweb: Virtuální svět hry Second Life je podle FBI semeništěm zločinu* [online]. Praha: iDNES, 2011 [cit. 2016-04-24]. Dostupné z: http://bonusweb.idnes.cz/virtualni-svet-hry-second-life-je-podle-fbi-semenistem-zlocinu-p7t-/Magazin.aspx?c=A111110_111515_bw-magazin_lou

[27] Zapomeň na mě, Google. *CHIP*. 2014, (11), 3.

[28] *Národní centrum bezpečnějšího internetu: Kyberšikana* [online]. Praha: Saferinternet.cz, 2011 [cit. 2016-03-29]. Dostupné z: http://archiv.saferinternet.cz/

[29] *E-Bezpečí: Kyberšikana u českých dětí* [online]. Olomouc: Centrum PRVoK PdF, 2012 [cit. 2016-04-24]. Dostupné z: http://www.e-bezpeci.cz/index.php/component/docman/cat_view/27-vyzkumne-zpravy

[30] FLANDEROVÁ, Nikol. *Analýza vybraných aspektů kyberšikany na sociálních sítích pomocí metody klíčových slov* [online]. Praha, 2012 [cit. 2016-04-28]. Dostupné z: http://info.sks.cz/www/zavprace/soubory/81740.pdf. Bakalářská práce. Vedoucí práce Mgr. Ludmila Fonferová.

[31] ŠEFČÍK, Vladimír. *Analýza rizik*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.

[32] *Metodiky hodnocení rizik* [online]. Praha: BOZP, 2004 [cit. 2016-04-24]. Dostupné z: http://www.bozpinfo.cz/citarna/clanky/rizeni_bozp/hodnoceni_rizik040331.html

[33] *EU Kids online* [online]. London: LSE, 2009 [cit. 2016-04-24]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

[34] *EU Kids Online* [online]. Brno: LSE, 2009 [cit. 2016-04-24]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/NationalWebPages/Czech.aspx

[35] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[36] Bezpečné a anonymní surfování. *CHIP*. 2014, (11), 2.

[37] *Rizika použití veřejných wifi sítí* [online]. Praha: KASPERSKY LAB CZECH REPUBLIC [cit. 2016-04-01]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/internet-safety/public-wifi-risks

[38] Příprava dětí na nástrahy internetu. *CHIP*. 2014, (7), 1.

[39] *Rizika a hrozby: Metody analýzy rizik* [online]. Jindřichův Hradec: Public4u, 2014 [cit. 2016-05-01]. Dostupné z: http://www.jh.cz/cs/krizove-rizeni/rizika-a-hrozby/

[40] *Horkalinka* [online]. Praha: Národní centrum bezpečnějšího internetu, 2015 [cit. 2016-04-22]. Dostupné z: https://www.internet-hotline.cz/o-n%C3%A1s.html

[41] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[42] ĎULÍKOVÁ, Radka. *Likvidace následků výbuchu muničních skladů ve Vlachovicích - Vrběticích a prevence* [online]. Uherské Hradiště, 2015 [cit. 2016-05-04]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/34379/%C4%8Ful%C3%ADkov%C3%A1_2015_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce.

[43] *Závěrečná práce - metodika* [online]. Praha: Lorenc.info [cit. 2016-04-20]. Dostupné z: http://lorenc.info/zaverecne-prace/metodika.htm

[44] *NetMonitor: Trendy v návštěvnosti internetu* [online]. Sdružení pro internetový rozvoj, 2014 [cit. 2016-04-24]. Dostupné z: http://www.netmonitor.cz/sites/default/files/prilohy/IAC%202016%20-%20NetMonitor%20ro%C4%8Denka%202015.pdf

[45] *Eurostat: Individuals using the internet for internet banking* [online]. Lucemburk: Eurostat, 2014 [cit. 2016-04-25]. Dostupné z: http://ec.europa.eu/eurostat/tgm/table.do?tab=table&plugin=1&language=en&pcode=tin00099

[46] *Náhradníci* [film]. Režie: Jonathan Mostow. USA, Touchstone Pictures, 2009

[47] *About Linden Lab* [online]. San Francisco: Linden Lab [cit. 2016-04-24]. Dostupné z: http://www.lindenlab.com/

[48] SOBIESKÁ, Karolína. *Moderní internetové bankovnictví* [online]. Brno, 2015 [cit. 2016-04-25]. Dostupné z: http://is.muni.cz/th/405737/esf_b/Bakalarska_prace_Sobieska.pdf. Bakalářská práce. Vedoucí práce Prof. Ing. Jiří Dvořák, DrSc.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Překlad do českého jazyka je veden volnou formou, záměrně tedy není doslovný. Čtenář má díky tomu lepší představu o významu zkratky.

PC	Personal Computer *(Osobní počítač)*
VR	Virtual Reality *(Virtuální realita)*
AR	Augmented Reality *(Rozšiřující realita)*
SL	Second Life *(Druhý život – Virtuální svět s prvky MMORPG)*
LED	Light-Emitting Diode *(Dioda emitující světlo)*
OLED	Organic Light-Emitting Diode *(Organické elektroluminiscenční diody)*
RAM	Random Access Memory *(Libovolné paměťové místo)*
GB	Gigabyte *(Jednotka množství informace)*
HDMI	High-Definition Multimedia Interface (*Nekomprimovaný obrazový a zvukový signál v digitálním formátu)*
USB	Universal Seriál Bus *(Univerzální sériová sběrnice)*
MUD	Multi User Dungeon (*Textová počítačová hra na hrdiny pro více hráčů)*
MMO	Massive Multiplayer Online *(Online hra o velkém množství hráčů)*
RPG	Role Playing Game *(Hra na hrdiny)*
MMORPG	Massively Multiplayer Online Role-Playing Game *(Online hra o velkém množství hráčů s prvky RPG)*
FPS	First Person Shooter *(Střílečka z pohledu první osoby)*
GTA	Grand Theft Auto *(Série počítačových her)*
USA	United States of America *(Spojené státy americké)*
NHL	National Hockey League *(Národní hokejová liga USA a Kanady)*
NBA	National Basketball Association *(*Národní basketbalová liga USA)
PEGI	Pan European Game Information *(Evropský ratingový systém pc her)*
WoW	World of Warcraft *(Fantasy MMORPG počítačová hra)*
LL	Linden Lab *(Americká společnost provozující projekt SL)*
LSE	London School of Economics and Political Science *(Londýnská škola ekonomie a politických věd)*
FBI	Federal Bureau of Investigation (*Americký Federální úřad pro vyšetřování)*

SEZNAM OBRÁZKŮ

Obrázek 1: Složky systému virtuální reality ... 13
Obrázek 2: Přilba pro prostorové vidění ... 14
Obrázek 3: Piktogramy obsahu u pc her ... 22
Obrázek 4: Titulní strana virtuálního světa Second Life ... 26
Obrázek 5: Nejčastější formy kyberšikany u českých dětí ... 27
Obrázek 6: Komunikační platformy kyberšikany ... 28
Obrázek 7: Metoda What-If. Nahlášení nelegálního obsahu na síti ... 38
Obrázek 8: Metoda What-If. Koloběh událostí po vstupu do SL ... 39
Obrázek 9: Věkové rozhraní ... 47
Obrázek 10: Nejvyšší dosažené vzdělání ... 48
Obrázek 11: Společenské postavení ... 48
Obrázek 12: Četnost využívání internetu ... 49
Obrázek 13: Čas strávený na internetu za den ... 50
Obrázek 14: Hodnocení rizika spojeného s užíváním internetu ... 51
Obrázek 15: Bezpečnost veřejných Wi-Fi sítí ... 51
Obrázek 16: Veřejné Wi-Fi sítě, e-mail a internetové bankovnictví ... 52
Obrázek 17: Nejčastější činnost na pc a tabletu ... 53
Obrázek 18: Životní láska ve virtuálním prostředí ... 55
Obrázek 19: Práce dětí s pc, tabletem a smartphonem ... 56
Obrázek 20: Přínos času stráveného na internetu - dospívající ... 57
Obrázek 21: Systém PEGI ... 58
Obrázek 22: Druhy kyberšikany dle jejich četnosti ... 59
Obrázek 23: Povědomí o virtuálním světě Second Life ... 61
Obrázek 24: Vnímání technologického pokroku lidstva ... 62
Obrázek 25: Vývoj internetového bankovnictví v ČR ... 74
Obrázek 26: Procentuální podíl užívaní internetbankingu v zemích EU ... 74
Obrázek 27: Ukazatel celkového počtu respondentů ... 75

SEZNAM TABULEK

Tabulka 1: Významy slova virtuální, od nejslabšího po nejsilnější 12
Tabulka 2: Přehled žánrů pc her s příklady 21
Tabulka 3: Klasifikace online příležitostí a rizik pro děti 33
Tabulka 4: Check list 40
Tabulka 5: Pravděpodobnost míry rizika 41
Tabulka 6: Závažnost následků rizika 41
Tabulka 7: Výsledná míra rizika 42
Tabulka 8: Čas potřebný k vyplnění dotazníku 45
Tabulka 9: Statistika přímé úměry 54
Tabulka 10: Statistika přímé úměry 60

SEZNAM PŘÍLOH

Příloha P1: Společnost Linden Lab

Příloha P2: Vývoj internetového bankovnictví

Příloha P3: Ukazatel znázorňující celkový počet respondentů

Příloha P4: Dotazník (Bezpečnost ve virtuálním prostředí)

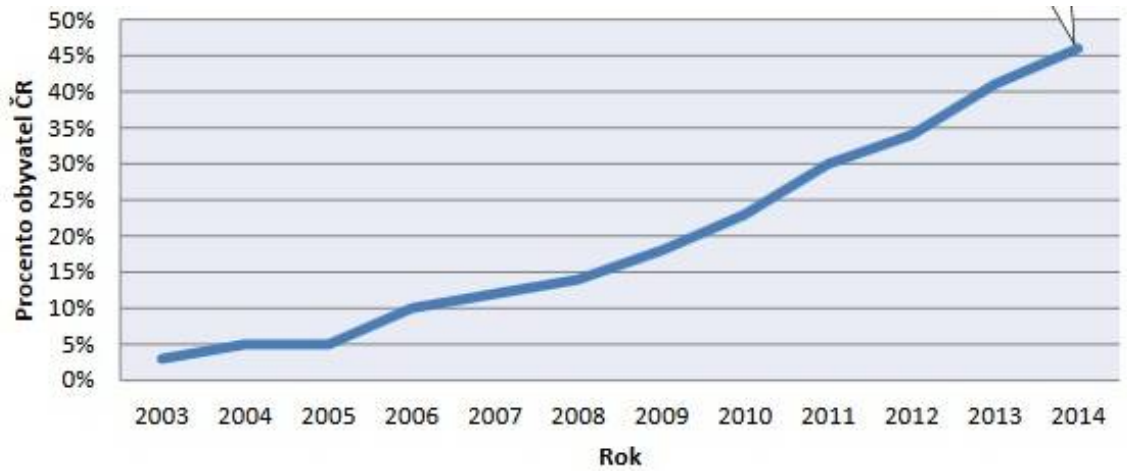
PŘÍLOHA P I: SPOLEČNOST LINDEN LAB

Americkou společnost v roce 1999 založil Philip Rosedal, známým též pod jménem Philip Linden.V roce 2003 byl spuštěn projekt SL, průkopnický virtuální svět, jehož uživatelé (hráči) se počítají na miliony a jejich transakce reálných peněz dosahují hodnot miliard dolarů.

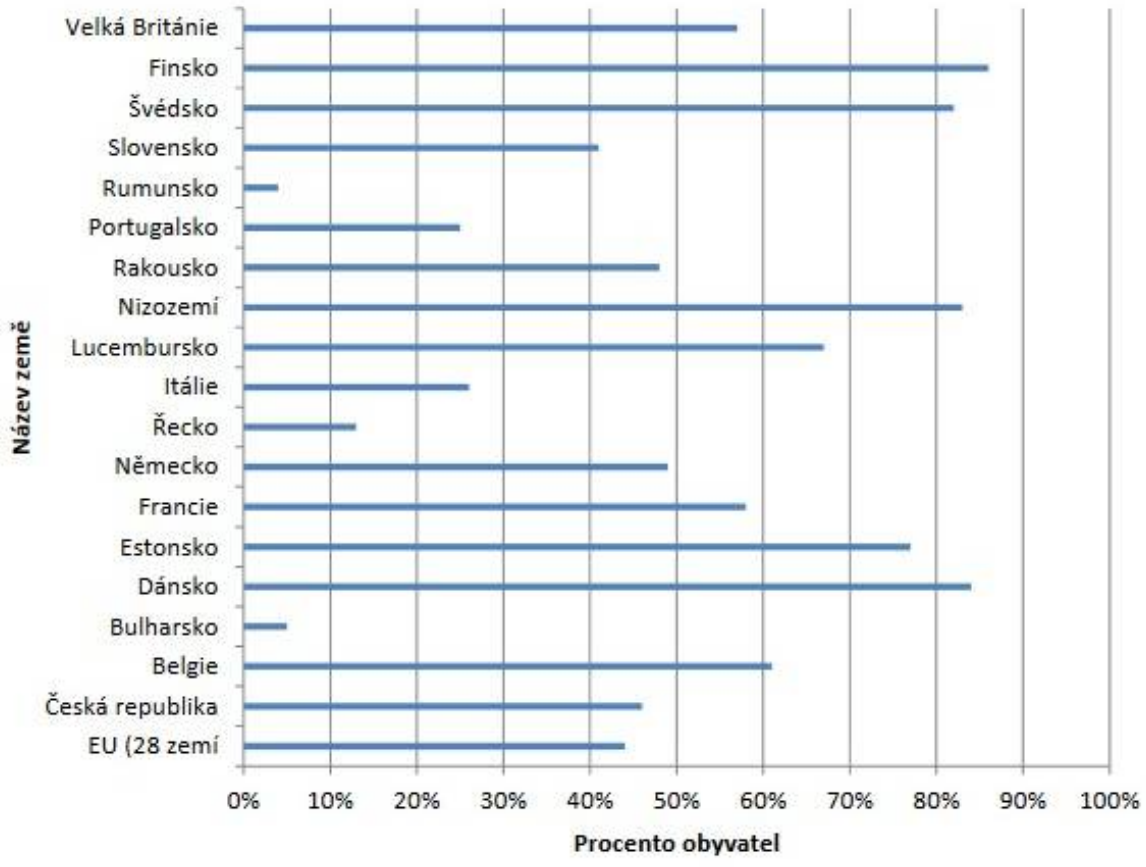
Společnost LL, tedy provozovatel aplikace SL, od počátku pracuje na vývoji nových, lepších verzí, které mají uživatelům umožnit více možností a větší seberealizaci. Protože je hlavní svět SL, tzv. MainGrid věkově omezen (od 18 let), vytvořila společnost LL v roce 2005 tzv. TeenGrid, který je určen pro zájemce od 13 do 17 let. Mezi těmito světy existují rozdílnosti například v ekonomii, v rozsahu obytné plochy, ve věkovém složení obyvatel či ověřování identity uživatele při registraci. [23]

V roce 2013, LL rozšířila své produktové portfolio o hru Blocksworld, veselý build-and-play systém na iPad pro děti i dospělé hráče. Společnost má sídlo v San Francisku a své pole působnosti rozšiřuje do Seattlu, Bostonu, Davis, a Charlottesville. [47]

PŘÍLOHA P II: VÝVOJ INTERNETOVÉHO BANKOVNICTVÍ



Obrázek 25: Vývoj internetového bankovnictví v ČR. Zdroj: [48]



Obrázek 26: Procentuální podíl užívaní internetbankingu v zemích EU. Zdroj: [48]

PŘÍLOHA P III: UKAZATEL ZNÁZORŇUJÍCÍ CELKOVÝ POČET RESPONDENTŮ

Obrázek 27: Ukazatel celkového počtu respondentů. Zdroj: Vlastní.

PŘÍLOHA P IV: DOTAZNÍK (BEZPEČNOST VE VIRTUÁLNÍM PROSTŘEDÍ)

Dotazník prosím vyplňte dle svého nejlepšího vědomí a svědomí, vše je anonymní a nezabere víc než pár minut.

1. Respondentem je:

a) Muž
b) Žena

2. Do jaké věkové skupiny patříte?

a) Méně než 15
b) 16-25
c) 26-35
d) 36-45
e) 46 a více

3. Nejvyšší dosažené vzdělání (řádně ukončené):

a) Základní
b) Vyučení
c) Střední s maturitou
d) Vysokoškolské

4. **Nynější společenské postavení:**

a) Student
b) Zaměstnanec, osoba samostatně výdělečně činná, pracující důchodce
c) Důchodce
d) Nezaměstnaný
e) Na rodičovské dovolené, v domácnosti

5. Jak často využíváte internet?

a) Nevyužívám
b) Párkrát do měsíce
c) 1-3x do týdne
d) 4-6x do týdne
e) Denně

6. Kolik času denně strávíte na internetu?

a) Zhruba 1h
b) 2-3h
c) 4-6h
d) 7h a více
e) Žádný

7. Jak hodnotíte riziko spojené s užíváním internetu?

a) Mizivé
b) Relativně nízké
c) Relativně vysoké
d) Neúměrné

8. Myslíte si, že je užívání veřejných Wi-Fi sítí bezpečné?

a) Ano, zcela
b) Ano, ale se zvýšenou opatrností
c) Není příliš bezpečné
d) Je nebezpečné

9. Přihlašujete se někdy na veřejných Wi-Fi sítích k e-mailu či internetovému bankovnictví?

a) Ano, k oběma
b) Pouze k e-mailu
c) Pouze k internetovému bankovnictví
d) Ani k jednomu

10. Jakou činností trávíte na počítači (tabletu) nejvíce času?

a) Hledáním informací na internetu
b) Hraním her
c) Prací
d) Jinou (napište jakou)

11. Omezil(a) jste někdy kvůli času strávenému ve virtuálním prostředí (internet, hry apod.) některé své zájmy (kulturní, sportovní, rekreační)?

a) Ano
b) Ne

12. Zkoušel(a) jste někdy ve virtuálním prostředí (seznamky, online hry apod.) nalézt partnera(ku)?

c) Ano
d) Ne

13. Myslíte si, že se dá ve virtuálním prostředí najít životní láska?

a) Ano
b) Ano, já ji tam našel(la)
c) Ne, myslím, že je ztráta času hledat ji právě tam

14. Měl(a) jste někdy podezření, že osoba, se kterou si píšete (na chatu, ve hře, emailem, formou sms), není tím, za koho se vydává?

a) Ano
b) Ne

15. Je dle Vás správné, aby už od útlého věku děti pracovaly s počítačem, smartphonem či tabletem?

a) Ano, v životě to budou potřebovat a zabaví se
b) Ano, ale jen v omezené míře
c) Ne, raději by měly běhat po venku

16. Myslíte si, že v dnešní době moderních technologií je pro dospívající čas strávený na internetu přínosem?

a) Ano, odráží se to pak pozitivně na jejich odborných znalostech
b) Ne, populaci to má tendenci spíše degenerovat
c) Nedokážu posoudit

17. Znáte systém PEGI? *(Obal pc hry je dle jejího obsahu označen příslušným piktogramem a číslem určující věk, od kterého je vhodné počítačovou hru hrát)*

a) Ano a při koupi pc her se jím řídím
b) Ano, ale příliš jej neberu v potaz
c) Ne, dosud jsem si ho nevšiml(a)
d) Ne, pc hry nekupuji

18. Byl(a) jste někdy ve svém okolí svědkem kyberšikany?

a) Ano
b) Ne

19. Byl(a) jste někdy sám(a) obětí kyberšikany?

a) Ano
b) Ne

20. Pokud ano, jaké konkrétně? *(Je možno zatrhnout více odpovědí)*

a) Verbální útoky
b) Nabourání do facebookového, e-mailového či jiného účtu
c) Opakované obtěžování (prozvánění, spammování..)
d) Vyhrožování či zastrašování
e) Publikování ponižujících fotografií či videí

21. Lákala Vás někdy myšlenka, žít svůj druhý život ve virtuálním světě „neomezených možností“?

a) Ano

b) Ne

22. Pohltil Vás někdy „virtuální prostor natolik, že jste omezil(a) kontakty v reálném světě?

a) Ano

b) Ne

23. Slyšel(a) jste už někdy o virtuálním světě (hře) „Second Life“?

c) Ano, mám (měl jsem) tam svůj účet

d) Ano, ale osobní zkušenost nemám

e) Ne

24. Jak vnímáte technologický pokrok lidstva, tedy život stále více spjatý s elektronickými vymoženostmi?

a) Pozitivně – s očekáváním nových věcí

b) Neutrálně – příliš se tím nezaobírám

c) Negativně – s nedůvěrou