

# Ochrana dětí na Internetu

Roman Haluza

---

Bakalářská práce  
2015



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2014/2015

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Roman HALUZA**  
Osobní číslo: **A10118**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Informační a řídicí technologie**  
Forma studia: **prezenční**

Téma práce: **Ochrana dětí na Internetu**  
Téma anglicky: **Child Safety Protection on the Internet**

Zásady pro vypracování:

1. Vypracujte literární rešerši na téma ochrany dětí z prostředí Internetu.
2. Definujte nejčastější nebezpečí a nástrahy Internetu týkající se dětí.
3. Prozkoumejte možnosti programového zabezpečení počítače oproti výše uvedeným hrozbám.
4. Sestavte sadu rad a doporučení pro děti a rodiče.
5. Zpracujte dotazník na téma ochrana dětí na Internetu a vyhodnoťte jej.

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**. 1. vyd. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.
2. KOPECKÝ, Kamil. **CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE PEDAGOGICKÉ FAKULTY UNIVERZITY PALACKÉHO V OLOMOUCI. Projekt E-bezpečí [online]**. 2008 - 2014 [cit. 2015-01-27]. Dostupné z: <http://www.e-bezpeci.cz/>
3. KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. **Nebezpečí internetové komunikace 3**. Olomouc, 2012. ISBN 978-80-244-3088-1. Dostupné z: [http://www.e-bezpeci.cz/index.php/ke-stazeni/doc\\_download/39-nebezpei-internetove-komunikace-3-2011-2012](http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012). Mogografie. Univerzita Palackého v Olomouci.
4. **NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. Národní centrum bezpečnějšího internetu [online]**. 2012 [cit. 2015-01-27]. Dostupné z: <http://www.ncbi.cz/>
5. **NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. Bezpecne-online.cz: safe-internet.cz [online]**. [2013] [cit. 2015-01-27]. Dostupné z: <http://www.bezpecne-online.cz/>

Vedoucí bakalářské práce:

**Ing. Jiří Vojtěšek, Ph.D.**

Ústav řízení procesů

Datum zadání bakalářské práce:

**6. března 2015**

Termín odevzdání bakalářské práce:

**22. května 2015**

Ve Zlíně dne 6. března 2015



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*

L.S.

prof. Ing. Vladimír Vašek, CSc.  
*ředitel ústavu*

### Prohlašuji, že


- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších 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 aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji 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 bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

20.5.2015

  
.....  
podpis diplomanta

## **ABSTRAKT**

Cílem práce je definovat nejčastější hrozby pro děti na Internetu a prozkoumat možnou ochranu proti těmto hrozbám. Pro zjištění povědomí veřejnosti byl sestaven dotazník, který byl vyhodnocen, a na základě výsledků bylo navrženo ochranné řešení. Tato práce teoreticky řeší postupné vzdělávání rodičů a dětí v oblasti Internetu a jejich hrozeb. V práci jsou ukázány konkrétní kroky, jak zabezpečit počítač, aby bylo dítě maximálně chráněno. Přínosem této práce je seznámení s hrozbami na Internetu a jejich řešením.

Klíčová slova: Internet, dítě, hrozba, ochrana, kyberšikana.

## **ABSTRACT**

The aim of this work is to define the most common threats to children on the internet and explore possible protection against them. A questionnaire was compiled to discover public awareness, it was evaluated and a protective solution was based on the results. This paper addresses theoretically progressive education of parents and children and their threats on the Internet. There are specific steps on how to secure your computer in order to protect the child. The contribution of this work is familiarization with the threats on the internet and their solution.

Keywords: Internet, child, threat, protection, cyberbullying.

Tímto bych chtěl vyjádřit hluboké poděkování za ochotu a trpělivost při vedení mé bakalářské práce panu Ing. Jiřímu Vojtěškovi, Ph.D., a také rodičům, sestře a přátelům, kteří mne při studiu a psaní této bakalářské práce podporovali.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 VÝVOJ A HISTORIE INTERNETU</b> .....	<b>11</b>
1.1 ARPA (DARPA) .....	11
1.2 ARPANET .....	11
1.3 VÝVOJ A HISTORIE INTERNETU V ČESKÉ REPUBLICE.....	11
1.4 CESNET (FESNET).....	12
1.5 WORLD WIDE WEB (WWW) .....	12
1.5.1 Web 1.0 .....	13
1.5.2 Web 2.0 .....	13
1.5.3 Web 3.0 .....	14
<b>2 KOMUNIKACE POMOCÍ SÍTĚ INTERNET</b> .....	<b>15</b>
2.1 E-MAIL .....	15
2.2 INSTANT MESSANGERY A SKYPE.....	16
2.3 SOCIÁLNÍ SÍTĚ .....	17
<b>3 KONKRÉTNÍ HROZBY NA INTERNETU</b> .....	<b>19</b>
3.1 KYBERŠIKANA.....	19
3.2 KYBERSTALKING.....	20
3.3 KYBERGROOMING .....	20
3.4 SEXTING .....	21
3.5 SOCIÁLNÍ SÍTĚ .....	21
3.6 SOCIOTECHNIKA (PHISHING, PHARMING).....	21
3.7 HOAX A JINÉ.....	22
3.8 STRÁNKY S NEVHODNÝM OBSAHEM .....	22
3.9 HRY.....	23
<b>II PRAKTICKÁ ČÁST</b> .....	<b>24</b>
<b>4 DOTAZNÍK K BAKALÁŘSKÉ PRÁCI</b> .....	<b>25</b>
4.1 VYHODNOCENÍ DOTAZNÍKU .....	25
4.2 ZHODNOCENÍ DOTAZNÍKU .....	41
4.3 OSOBNÍ ZHODNOCENÍ .....	42
<b>5 NÁVRH ŘEŠENÍ DLE VÝZKUMU Z DOTAZNÍKU</b> .....	<b>43</b>
5.1 VZDĚLÁNÍ RODIČŮ .....	43
5.1.1 Veřejné semináře.....	43
5.1.2 Kurzy a workshopy .....	43
5.2 VZDĚLÁNÍ DĚTÍ .....	45
5.2.1 Vzdělání v rámci hodin informatiky .....	45
5.2.2 Vzdělání s externím pracovníkem.....	45
<b>6 SOFTWAREVÉ ZABEZPEČENÍ POČÍTAČE</b> .....	<b>46</b>
6.1 VESTAVĚNÉ FUNKCE SYSTÉMU.....	46
6.1.1 Vytvoření standardního uživatelského účtu pro děti.....	46

6.1.2	Rodičovská kontrola.....	47
6.1.3	Zapnutí rodičovské ochrany .....	47
6.1.4	Časový limit .....	48
6.1.5	Hry.....	49
6.1.6	Blokování programů.....	53
6.1.7	Bezpečné vyhledávání na webu .....	53
6.2	DOPLŇUJÍCÍ SOFTWARE .....	54
6.2.1	Norton Security (Family) .....	54
6.2.2	Naomi 3.2.90.....	55
6.2.3	Manic Time .....	56
6.2.4	Kurupira – web filter .....	57
6.2.5	K9 Web Protection .....	59
6.2.6	HostsMan .....	60
6.3	SHRNUTÍ TESTOVÁNÍ DOPLŇUJÍCÍCH PROGRAMŮ .....	60
6.4	WEBOVÉ PROHLÍZEČE .....	61
6.4.1	Mozilla Firefox 37.0.1.....	61
6.4.2	Opera 28.0 .....	62
6.4.3	Google Chrome 41.0.2272.118 m.....	64
6.4.4	Internet Explorer 11 .....	64
6.4.5	AdBlock .....	64
6.4.6	Tablety, smartphony a aplikace v nich.....	65
6.4.7	Shrnutí .....	65
	<b>ZÁVĚR .....</b>	<b>66</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>67</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>71</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>72</b>
	<b>SEZNAM TABULEK.....</b>	<b>73</b>
	<b>SEZNAM GRAFŮ .....</b>	<b>74</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>75</b>

## ÚVOD

Cílem této práce bylo zjistit, jaké má veřejnost povědomí o hrozbách, které mohou číhat na děti na Internetu a následné ochraně dětí.

Postupem rozvíjejícího se Internetu přichází i hrozby, které mohou na děti čekat, proto je potřeba i s tímto faktem pracovat a předcházet událostem, které mohou mít i fatální následky. Díky tomu, že Internet není omezený, každý může na něj zavěsit v podstatě cokoliv. Je hodně stránek a serverů, které by děti neměly vidět. Od násilí, přes porno, až po nevhodné reklamy.

Díky nástrojům, které můžeme nalézt na internetu, můžeme alespoň část těchto hrozeb eliminovat. V praktické části této práce budou navržena softwarová řešení, jak předcházet tomu, aby se dítě dostalo do styku s nevhodným obsahem.

Pro zjištění povědomí veřejnosti o hrozbách a ochraně dětí na Internetu, byl vytvořen dotazník, kde respondenti odpovídali na 21 otázek, které se týkaly celkovému povědomí o hrozbách na Internetu, komunikaci pomocí Internetu, ochraně a osvětě dětí na Internetu.

Další částí, kterou se budu zabývat v této práci, budou konkrétní hrozby, které jsou na Internetu, nebo které mohou být díky Internetu vykonávány. Internet může být brán jako nástroj k nevhodnému chování a útokům vůči dětem. V následujícím textu se zaměřím také na tyto hrozby, jaké jsou kyberšikana, kybergrooming, či sociální techniky a také na následnou ochranu nebo prevenci před podobnými útoky.

Výstupem práce by měl být pocit, že čtenář ví, jaké jsou hrozby na Internetu. Ví, jak se proti nim bránit, případně jak své děti připravit na nástrahy na Internetu.

## **I. TEORETICKÁ ČÁST**

## 1 VÝVOJ A HISTORIE INTERNETU

Začátky počítačových sítí byly na principu propojování dvou počítačů, tedy bod-bod, což nebylo moc efektivní. Snahou bylo vytvořit síť počítačů, která by komunikovala mezi sebou. Ideálně, aby tato síť byla decentralizovaná. S náznaky Internetu přichází americký vědec Joseph Carl Robnett Licklider, který pro americkou armádu vymyslel projekt SAGE (Semi Automatic Ground Environment) Air Defence System a také byl součástí agentury ARPA. Tento projekt sloužil pro armádní účely a byl vytvořen za účelem sjednotit komunikaci a řízení v obranných, tak i útočných složkách armády. Síť nevyužívala jen jedno komunikační médium, ale fungovala na více komunikačních médiích. [1][2]

### 1.1 ARPA (DARPA)

ARPA (nyní DARPA) je agentura amerického ministerstva obrany, která má na starost vývoj nových pokročilých projektů a technologií. Byla založena v roce 1958 proto, aby si armáda Spojených států Amerických udržela technologický pokrok s tehdejšími Sovětským svazem, který v roce 1957 vypustil svoji první družici do vesmíru – Sputnik 1. Agentura ARPA se podílela na několika projektech, např. bezpilotní letoun Boeing X-45, projekt MAC a také projekt ARPANET.[3]

### 1.2 ARPANET

ARPANET byla síť, která vznikla v roce 1969 za účelem ozkoušení nového principu, a to přepojování paketů. Tento princip měl zvýšit robustnost a dostupnost k tehdejšími super počítačům, které byly na amerických univerzitách a zamezit zničení sítě tím, že by byl vyřazen nějaký přístupový bod, proto síť byla decentralizovaná. Síť tvořili čtyři americké univerzity – Univerzita v Los Angeles v Californii (UCLA), Univerzita Santa Barbara v Californii (UCSB), Univerzita Utah a Standfordský výzkumný ústav (SRI). První pokus o komunikaci přišel 29. října 1969. Od té doby vznikaly nové uzly na území Spojených států. Později se přidala i Evropa. Prvním státem připojeným do sítě ARPANET bylo Norsko v roce 1973 a následně Velká Británie.

ARPANET dal základ dnešnímu Internetu tak, jak ho známe.[4]

### 1.3 Vývoj a historie Internetu v České Republice

Počátek Internetu v ČR začíná v roce 1990, kdy se k propojení využívalo telefonní linky. První spojení proběhlo v roce 1991 s rakouským Lincem pomocí sítě EARN (European

Academic and Research Network). Avšak oficiální připojení ČR do Internetu bylo 13. 2. 1992 v Praze na ČVUT. Následně se uvažovalo o celorepublikové síti, která by spojovala jednotlivá města, což byla základní myšlenka pro vznik CESNET sítě. [5]

#### 1.4 CESNET (FESNET)

V brzkém začátku 90. let vznikla myšlenka dvou páteřních sítí, které by propojovali akademická centra, a následně by měl být Internet distribuován pomocí metropolitních sítí. Na české straně, tehdejšího Československa, vzniká síť FESNET (Federal Educational and Scientific NETwork), která se později přejmenuje na CESNET (Czech Educational and Scientific NETwork). Na Slovensku vzniká obdobná síť s názvem SANET (Slovak Academic NETwork).

Nejrychlejší propojení v roce 1995 bylo mezi Prahou a Amsterdamem, kdy rychlost byla 512 kbps. Dále pak mezi českými městy v rozmezí 124 kbps – 64 kbps. Avšak většina spojení fungovala na rychlosti 19,3 kbps.

Později Ministerstvo školství povolilo využívat CESNET i pro komerční účely, a tím si vydělávalo na svůj provoz. Díky tomuto uvolnění se CESNET stal součástí a poskytovatelem Internetu spolu s dalšími např. firmou COnet, která provozovala síť CZnet.[5]

#### 1.5 World Wide Web (WWW)

World Wide Web zkráceně WWW je celosvětová „pavučina“ (angl. web), která umožňuje uživatelům prohlížet, posílat, ukládat dokumenty mezi sebou prostřednictvím Internetu. Dokumenty jsou uloženy na serverech, a tyto dokumenty jsou mezi sebou propojeny hypertextovým odkazem. Prohlížení těchto dokumentů nám umožňují webové prohlížeče, např. Internet Explorer, Opera, Chrom aj. Původním cílem bylo vytvoření možnosti pro sdílení akademických projektů, ale postupem času se tento cíl překonal a dnes se využívá i na komerční účely. [6]

Služba WWW vznikla koncem 80. let v Cernu a jejím autorem je Tim Berners-Lee, který také navrhl značkovací jazyk HTML, nebo protokol http. Dnes působí jako ředitel W3C, což je organizace pro vytváření webových standardů.[7],[8]

WWW je složeno ze tří protokolů.

- HTTP – (Hypertext Transfer Protocol) protokol ke komunikaci klient – server.

- HTML – (Hypertext Markup Language) – základní značkovací jazyk pro tvorbu webových stránek.
- URL – (Uniform Resource Locator) – přesné umístění dokumentů na Internetu

### 1.5.1 Web 1.0

Obecně vzato k Webu 1.0 neexistuje přesná definice. Web 1.0 začíná v počátcích www, kdy první stránky byly převážně statické. Obsah stránek byl vytvářen převážně jeho vlastníkem, tudíž uživatel mohl informace pouze využívat, ale nemohl je ve většině případů měnit. [10]

Tab. 1 – Srovnání Web 1.0 a Web 2.0. [9]

	Web 1.0	Web 2.0
Obsah	obsah webu je vytvářen převážně jeho vlastníkem	návštěvníci se aktivně podílejí na tvorbě obsahu - vlastník je v roli moderátora
Interakce	interakce vytváří nároky na vlastníka, proto je jen v nezbytné míře	interakce je vítána, má formu diskuzí, chatu, propojení s messengery, sociálních profilů
Aktualizace	odpovídá možnostem vlastníka	web je živý organismus - tvůrců obsahu mohou být miliony
Komunita	neexistuje, návštěvník je pasivní příjemce informací bez interakcí	návštěvník je současně ten, "o kom web píše", jednotlivec je součástí rozsáhlé komunity
Personalizace	weby neumožňují implicitní personalizaci	umožňuje vytvářet a využívat sociální profily čtenářů.

### 1.5.2 Web 2.0

„Web 1.0 je o komerci, Web 2.0 je o lidech.“[11]

Je nutné podotknout, že k transformaci z Web 1.0 na Web 2.0 došlo postupně zvyšujícími se nároky na variabilitu webů, například na vyhledávání obsahu nebo celkově na úpravu dle uživatele (blogy, sociální sítě). Tato přeměna začala okolo roku 2004.[10]

Pojem Web 2.0 není oficiálním standardem, jde o všeobecný pojem a chápání tvorby webového obsahu. Dnes reprezentují Web 2.0 převážně sociální sítě, diskuzní fóra, blogy, seznamky, wiki aj. Dá se říct, že dnes většina webových stránek funguje na filozofii Web 2.0, kde uživatel má možnost ovlivnit obsah.[12]

### **1.5.3 Web 3.0**

Web 3.0 postupně navazuje na Web 2.0, avšak nemá přesnou definici ani počátek. Jedná se o typ webu, který používá sémantických prvků. Na takový web se můžete dostat i skrze tablet nebo mobilní telefon. Je kladen důraz na větší interakci s uživatelem, a také by měla být větší přizpůsobivost uživateli, aj. Web 3.0 není ještě úplně ucelen, avšak již dnes se spekuluje o Webu 4.0, jehož nástup se očekává v rozmezí 2020-2030. [13],[14]

## 2 KOMUNIKACE POMOCÍ SÍTĚ INTERNET

V počátcích sloužil Internet výhradně k akademickým, výzkumným a také vojenským účelům. Následně se Internet prosadil i v komerční sféře a s tím přišla potřeba komunikace. Jedním z nejnámějších a také nejstarších a nejrozšířenějších komunikačních kanálů jsou e-maily. S příchodem WWW se začínají rozšiřovat diskuzní fóra, kde uživatelé mezi sebou komunikují pomocí webových stránek. Vznikají také další možnosti, jako jsou Instant Messengery nebo volání pomocí Internetu přes aplikaci Skype.

### 2.1 E-mail

Začátek e-mailu se pojí se začátkem Internetu, tehdejšího ARPANETu. První zprávu sám sobě poslal vědec Ray Tomlinson. Ten si zpočátku ani neuvědomil, jakou revoluci v komunikaci po síti způsobil, protože o jeho úspěchu se nemluvilo. Tomlinson stál také u dnešní podoby e-mailových adres, kdy mezi jméno a počítač dal znak zavináče. Slovo e-mail vzniklo až o mnoho let později, přesně v roce 1982. [15]

Dle statistik v roce 2012 bylo odesláno v průměru 144 milionů e-mailů za den. [16]

Výhodou e-mailové komunikace je, že můžeme příjemci odeslat v podstatě cokoliv. Kromě samotné zprávy, můžeme příjemci poslat i menší datové soubory jako jsou: audiona-  
hrávky, videa, prezentace nebo fotky. Této možnosti využívají i útočníci, kteří e-mailem mohou posílat viry nebo poplašné zprávy tzv. hoaxy. Můžeme se setkat i s řetězovými zprávami, které chtějí po přečtení poslat tuto zprávu dalšímu počtu osob.

U e-mailů, které mají podezřelou přílohu, platí pravidlo. Čím si nejsme jistí, to neotevíráme.

V poslední době je rozšířená forma útoku v podobě e-mailu, který se tváří jako e-mail z banky nebo od exekutora, že jste nezaplatili pohledávku, proto máte poslat určitý obnos peněz na daný účet, jinak vám bude zabaven majetek. U takových e-mailů je třeba ověřit pravost. U e-mailů tvářících se jako příchozí z banky, je dobré do dané instituce zavolat. Mnohdy stačí pouze zkontrolovat e-mail odesílatele.

E-mailů využívají i různé sociální sítě jako své marketingové praktiky. Může vám přijít e-mail se zprávou, že váš známý vám zanechal na dané sociální síti zprávu. Po otevření odkazu se dostanete na stránky sociální sítě a ta vás žádá o registraci. Po registraci ale žádnou zprávu neobdržíte.

## 2.2 Instant Messangery a Skype

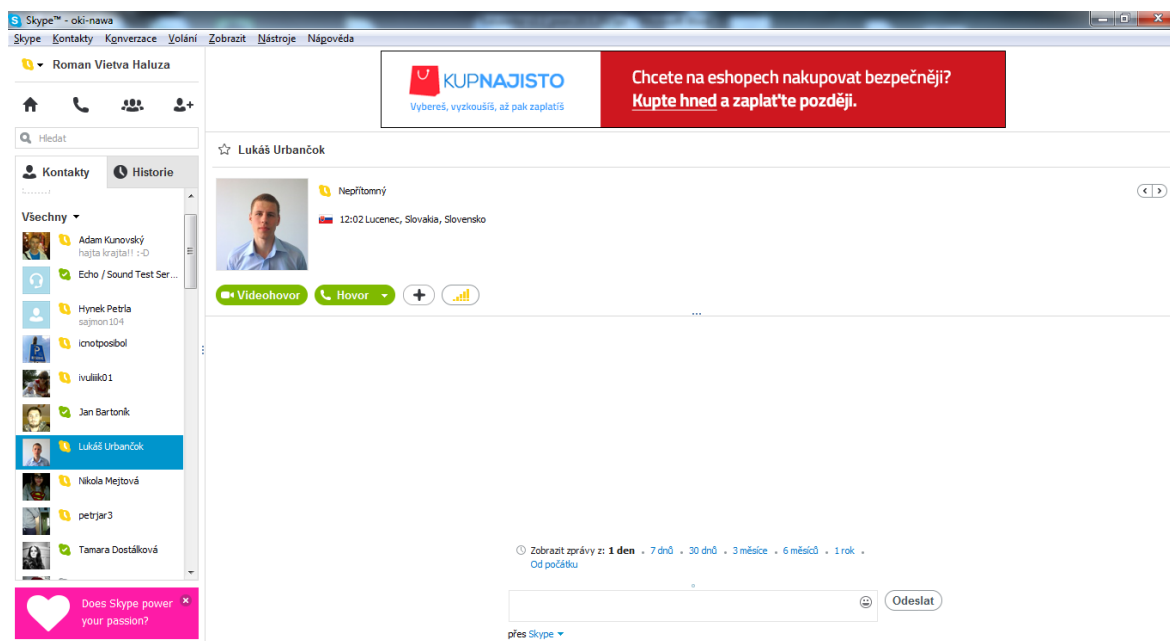
Historie Instant Messengerů (IM) začíná na konci 80. let 20. století. Největší rozmach této služby byl od roku 1996, kdy firma Mirabilis přišla s programem ICQ, který je velmi rozšířený dodnes, avšak s nástupem sociálních sítí už nezažívá takovou expanzi. Později byli vyvinuti další IM klienti jako například MSN Messenger, Yahoo aj. Nevýhodou bylo, že každý s klientů fungoval na odlišném protokolu, proto vznikli multi-protokoloví klienti, jako jsou Miranda, Trilian, Kopete a další.

Výhodou IM je komunikace s protější stranou v reálném čase. Tedy můžeme tzv. chatovat s uživatelem ihned a nemusíme čekat na odpověď. Výhodou oproti e-mailu je, že vidíme stav uživatele, tzn. jestli je online u počítače nebo je mimo počítač. Tento stav lze nastavit přímo v IM klientovi. Díky rozsáhlému používání mezi uživateli, se tento způsob komunikace rozšířil i do pracovního prostředí, kdy můžeme komunikovat s kolegy po celém světě ihned. Většina IM umožňuje posílat i soubory, proto musíme být obezřetní, od koho soubory dostáváme.

Nebezpečí může nastat v případě, že si do svých kontaktů přidáváme i neznámé lidi, proto platí, že bychom neměli sdělovat přes IM citlivé informace, například bydliště, telefonní číslo aj. Nejen, že to může protistrana využít proti nám, ale také komunikace může být odposlouchávána. [17]

Jelikož IM byl velmi oblíbený způsob komunikace, byl využíván i pro posílání zpráv, které obsahovali odkaz na podezřelou stránku nebo přímo soubor s podezřelým obsahem. Nejlepší obrana proti takovým útokům je nestahovat podezřelé soubory, byť od známých lidí (mohla jim být ukradena IM identita), a také používat kvalitní antivirový program. [18]

Skype je program, který se specifikuje na hlasové volání po Internetu. V rámci vašeho tarifu na Internet můžete telefonovat s kýmkoliv na světě. Výhodou je, pokud si předplatíte kredit, že můžete volat i na pevné linky. Avšak v dnešní době smartphonů si můžete nainstalovat Skype i do mobilního zařízení.



Obr. 1 – Prostředí Skype

Skype umožňuje také posílat zprávy, soubory jako IM. V dnešní době se Skype využívá i v pracovním prostředí na videokonference s obchodními partnery nebo na Internetové pohovory. U Skype platí stejná pravidla jako u IM. Musíme dávat pozor, s kým komunikujeme a jaké informace mu sdělujeme, protože naše komunikace může být nahrávána a archivována. Variantou ke Skype mohou být programy, které spíše používají hráči online her.

Teamspeak funguje na principu „Internetové vysílačky“, kdy mohou hráči jednotlivých týmů komunikovat mezi sebou a domlouvat si tím taktiku boje.

IM a Skype dnes běžně využíváme na stolních počítačích, ale také je můžeme využívat na mobilních telefonech a tabletech. Avšak s nástupem sociálních sítí tato forma komunikace upadá a využívají se tyto sítě.

### 2.3 Sociální sítě

Sociální sítě vznikly za účelem propojování lidí do skupin. Tyto skupiny mohou být zaměřené na určitý zájem nebo činnost. Například soc. síť Instagram je zaměřena na sdílení fotografií s lidmi po celém světě. Podobně je tomu u sítě Pinterest, která také slouží na sdílení obrázků, avšak tyto obrázky nemusí být naše vlastní. Mezi nejznámější sociální sítě můžeme zařadit Facebook, Twitter, Youtube, Pinterest, Instagram, YouTube, Google +, Tumblr a mnohé další. Odhaduje se, že sociálních sítí může být kolem 200 a tyto sítě využívá

cca 46% populace. [19] Mezi české sociální sítě můžeme zařadit seznamku Lidé, Líbímseti nebo dnes již překonaný Xchat.



Obr. 2 – Úvodní stránka soc. sítě Facebook

Vznikají i pracovní sociální sítě, například LinkedIn, nebo Business Animals. Zde si vytvoříte svůj profil a uvedete vaše pracovní dovednosti a zkušenosti. Můžete tu hledat i pracovní pozice, nebo naopak HR pracovníci mohou zde hledat spolupracovníky.

Cílem sociálních sítí je lidi sblížovat po Internetu, sdílet informace, dokumenty. Také, aby lidé mezi sebou komunikovali a sdíleli si zážitky. U sociálních sítí musíme být obezřetní, jaké informace sdílíme veřejně a kdo může vidět náš profil. Informace, které dáme na svůj profil na soc. síti, mohou být zneužity proti uživateli, například, může být ukradena celkově jeho identita uživatele, tzn., že útočník se vydává za uživatele. Nikdy neuvádějte na Internetu své telefonní číslo (pokud to není nutné), e-mail nebo rodné číslo a podobné citlivé informace.

Rizikem na soc. síti je anonymita a vysoká koncentrace cizích lidí. Této anonymity využívají útočníci, kteří se mohou vydávat za někoho jiného, než ve skutečnosti jsou a mohou po nás chtít citlivé informace nebo fotografie. [20]

### 3 KONKRÉTNÍ HROZBY NA INTERNETU

V této kapitole bude rozebráno, s jakými konkrétními hrozbami se můžete setkat. Budou zde i uvedeny konkrétní případy, které se ve světě staly, pro názornost kam až neřešení těchto hrozeb může dojít. Hodně útoků je spojených s reálným životem, jako je například kyberšikana.

#### 3.1 Kyberšikana

Kyberšikana je činnost na Internetu, která má za cíl psychicky ublížit své oběti. Kyberšikanou nazýváme útoky přímo na konkrétní osobu, například na diskuzních fórech, chatovacích serverech, ale útočníci využívají i sociální sítě. Zde si vytvářejí falešné profily a veřejně urážejí oběť. Útočníci využívají dalších možností, například e-mail, sms, ICQ a jiné. Tito lidé, kteří záměrně poškozují své oběti, vytváří také webové stránky, blogy za účelem veřejného zesměšnění.

Kyberšikana je další nástroj útočnicků, kteří svoji oběť většinou šikanují i v reálném životě. Kyberšikana stírá výhody klasické šikany, například sílu, nebo velikost útočníka. Za to může být více nepříjemná, a to z důvodu, že oběť nemůže odhadnout, kdy útočník zaútočí. Ve většině případů útočníci vystupují anonymně. Často mění identitu nebo e-mail, ze kterých odesílají zprávy. V některých případech se oběti stanou útočníky kyberšikany. [21] 39% šikanovaných dětí jsou ty, které využívají sociální sítě jako je Facebook, Líbímseti, MySpace aj. [22]

Kyberšikana může mít i tragické následky v podobě sebevražd. Například příběh třináctiletého chlapce z USA, který se jmenoval Patrick Ryan Halligan. Ten se oběsil v koupelně z důvodu zveřejnění intimních informací a také ho vrstevníci pomlouvali, že je homosexuál. [22]

Další případ se stal v Polsku, kdy mladá dívka si vzala v roce 2006 život. Spolužáci ji ve třídě sexuálně napadli a natočili to na video, které následně nahráli na Internet. Po tomto incidentu se dívka oběsila doma na švihadle. [22]

### 3.2 Kyberstalking

Stalking je opakované a stupňované obtěžování oběti, které je v České republice trestný čin. Ke kyberstalkingu většinou stalkeré (pronásledovatelé) používají mobilní telefony, sms zprávy, maily, zprávy na sociálních sítích, zasílání nechtěných dáreků, vzkazy na Skype nebo ICQ. Kyberstalkeré využívají také diskuzních fór, kde si vyhledávají oběti a informace o nich.

Oběťmi kyberstalkingu bývají ex-partneři, lidé, kteří neopětují city pronásledovatele nebo známé osobnosti. Stalker demonstruje svoji sílu pomocí výhrůžek, tím dává oběti najevo moc a sílu. Například může psát zprávy, ve kterých naznačuje, že ví, kde oběť je, co právě dělá apod.

Stalkeré mohou kombinovat klasický stalking s kyberstalkingem, kdy oběť pronásledují v reálném životě a zároveň oběť mohou sledovat pomocí Internetu. [23]

### 3.3 Kybergrooming

Kybergroomingem se nazývá technika, kterou využívají útočníci na seznamkách, sociálních sítích a jiných serverech, kde se setkává velké kvantum cizích lidí. Cílem útočníka je najít oběť, která může být v tíživé situaci, ze sociálně slabšího prostředí nebo nemá kamarády. Útočník zjišťuje u oběti situaci a následně se snaží vyvolat pocit důvěry. Tato fáze může trvat několik týdnů, kdy oběť začne důvěřovat útočníkovi. Svěřuje se mu s citlivými informacemi a toho útočník využívá. Prvotní krok útočníka je získat citlivé informace, jako jsou telefonní číslo, adresa, ICQ číslo aj. Aby si udržel sympatie oběti, tak jí dává různé dárky nebo jí může dobít telefon apod. Součástí kybergrooming může být i vydírání, kdy oběť může poslat útočníkovi intimní fotografie nebo mu může říct citlivé informace, které útočník použít proti oběti. Poté se útočník oběť snaží vylákat na osobní schůzku. Na schůzce dochází k zneužívání nebo fyzickému násilí. Nejlepší prevencí před kybergroomingem je komunikace rodičů s dětmi, aby si vytvořili dobrý vzájemný vztah. [24],[25]

Případ, který se stal u nás v České republice, byl v Praze. Vrátný Pavel Hovorka vyhledával mladé chlapce, po kterých chtěl intimní fotografie a následně je těmito fotografiemi vydíral. K vyhledávání využíval seznamky, chaty a po získání telefonního čísla i volal. Jeho první oběť nalákal na to, že vyhrála soutěž a poté ji pozval k sobě do vrátnice, kde ji pak sexuálně zneužil. Za zneužívání dětí dostal od soudu osmiletý trest.[26]

### 3.4 Sexting

Sexting je poměrně nová věc, která byla zdokumentována už v roce 2005. Jedná se o posílání zpráv, mailů, fotografií, videí se sexuální tematikou. Obvykle tyto dokumenty bývají uveřejňovány na sociálních sítích a serverech a stránkách se sexuálním obsahem.[27]

### 3.5 Sociální sítě

Sociální sítě slouží ke komunikaci a sdílení obsahu se známými i neznámými lidmi. (Facebook, Twitter, Líbímseti atd.)

U sociálních sítí nebo seznamek je potíž v tom, že nevíme, s kým si reálně píšeme. Sociální sítě jsou jako prostředník k páčání útoků v podobě kyberstalkingu i kybergroomingu a kyberšikany.

### 3.6 Sociotechnika (phishing, pharming)

Sociotechnika je způsob, kdy se útočník snaží oklamat oběť tím, že se vydává za někoho jiného. Cílem je získat od oběti citlivé informace jako jsou hesla, jména, adresy, telefonní čísla a jiné. Útočníci využívají především neznalosti, případně důvěřivosti obětí. [28],[29]

#### Phishing

Phishing je odvozený od slova fishing, což je v překladu rybaření. Oběť se chytá na návnadu v podobě smyšleného webu.

Phishing je technika, které má za cíl z obětí vylákat citlivé informace jako jsou hesla, kreditních a platebních karet. Principem je rozesílání emailů nebo zpráv na sociálních sítích, ve kterých jsou většinou odkazy na stránky, které se tváří jako známé weby. Například známé sociální sítě, bankovní služby, online platební portály, aukční weby. Na webech se přihlásíte a útočník se o vás dozví citlivé informace.

#### Pharming

Pharming je podobná technika phishingu. Cílem je také získat citlivé informace o uživateli. Tento útok je založený na napadení DNS a přepsání IP adresy. To poté způsobuje přesměrování na falešné stránky Internet bankingu. Tyto stránky bývají hodně podobné pravým stránkám, mnohdy nejsou k rozeznání.[30]

## **Pretexting**

Útočník má předem připravenou informaci o oběti, kterou použije většinou po telefonu za cílem zjistit další citlivé informace. Tím, že útočník ví předem nějakou informaci, kterou může zjistit například ze soc. sítě, vzbuzuje v oběti důvěru.[29]

## **3.7 Hoax a jiné**

Hoax jsou poplašné zprávy, které se nezakládají na reálném podkladu. Většina těchto zpráv je zcela smyšlených a jejich účelem pouze je, co nejvíce se rozšířit, případně vylákat z obětí peníze.

Většina zpráv hoax jsou poplašné zprávy o šířícím se neexistujícím viru nebo obsahují kreslené informace, které jsou buď zcela smyšlené nebo polopravdy. Na konci každé zprávy je informace o sdílení dalším osobám.[31]

Hoax znepríjemňuje život, protože uživatelům zbytečně zahlcují e-mailovou schránku. Rizikem u hromadného přeposílání hoax zpráv je, že dáváme k dispozici další adresy, které mohou útočníci využít buď na další útok nebo na rozesílání spamu.[32]

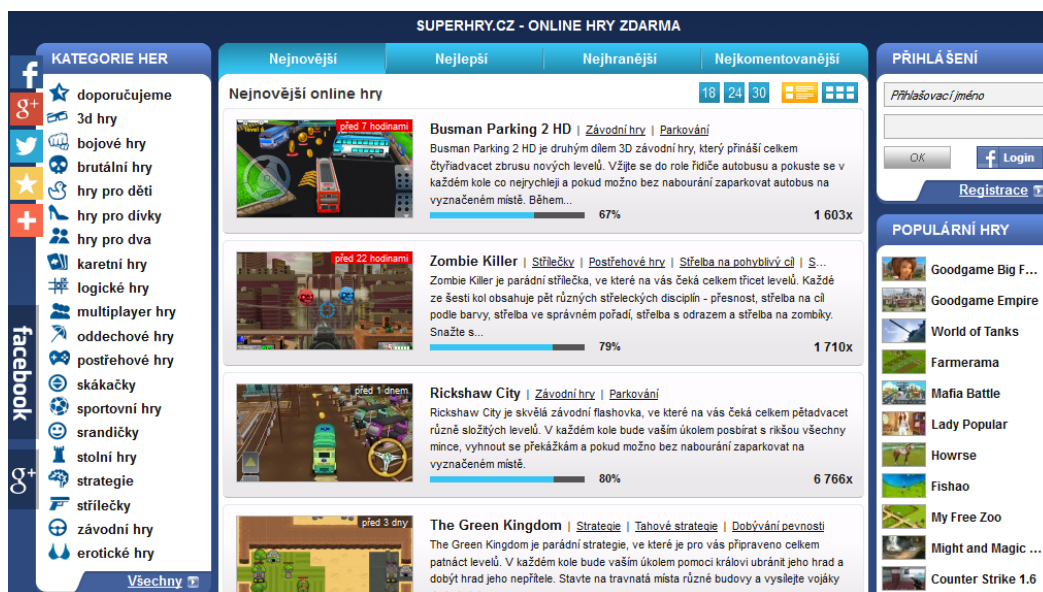
## **3.8 Stránky s nevhodným obsahem**

Stránek s nevhodným obsahem je na Internetu dost. Na těchto stránkách jsou většinou obrázky a videa s násilím nebo se sexuální tematikou. Při vstupu na tyto stránky je úvodní oznámení, kde musíte souhlasit s podmínkami vstupu.

Účinnou metodou, jak se takovým stránkám vyhnout, je používat doplňky do Internetového prohlížeče, které filtrují tento obsah a nedovolí vám navštívit takové stránky nebo software, který si nainstalujete do počítače.

### 3.9 Hry

Na Internetu se můžeme setkat s on-line hrami. Existují portály, které umožňují na jednom místě hrát různé hry, například server [www.superhry.cz](http://www.superhry.cz). Na těchto stránkách nalezneme nejen logické hry, ale i takové, které mohou obsahovat násilí.



Obr. 3 – Portál [superhry.cz](http://superhry.cz)

Populární jsou v dnešní době i on-line hry, které buď můžete hrát pomocí webového rozhraní, nebo po instalaci hry do počítače. Mezi nejznámější on-line hry patří World Of Warcraft, Travian nebo Minecraft.

## **II. PRAKTICKÁ ČÁST**

## 4 DOTAZNÍK K BAKALÁŘSKÉ PRÁCI

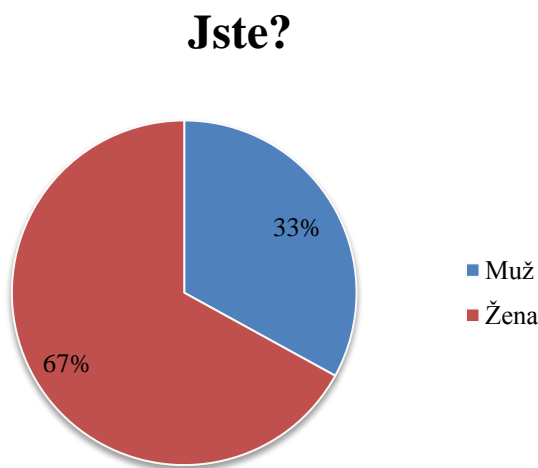
K bakalářské práci byl vytvořen dotazník k určení povědomí lidí o Internetu, sociálních sítích a také hrozbách, jaké na Internetu mohou být. Dotazník byl rozdělen do dvou částí podle toho, jestli respondent měl děti nebo ne. V dotazníku bylo uvedeno 21 otázek, na které museli respondenti odpovědět, aby mohli pokračovat dál. U některých otázek byly odpovědi z části nebo zcela volnou formou a bylo na respondentovi, jak chce odpovědět. Šetření probíhalo v rozmezí od 2. 1. 2014 do 19. 2. 2014. Zúčastnilo se ho 217 respondentů, kteří měli za úkol zodpovědět maximálně 21 otázek. Některé otázky se větvily dle odpovědi, proto respondent nemusel zodpovědět všech 21 otázek. Ke zpracování dotazníku byl použit portál vyplnto.cz. Tento portál byl využit z důvodu přehlednosti, rychlé a snadné úpravy otázek, a také snadného exportu do několika formátů, například xls, cs nebo pdf.

Dotazník byl šířen převážně přes Facebook a také přes e-mail. Cílem bylo oslovit co nejširší okruh lidí, kteří jsou ve věku 25-40 let, protože tato skupina lidí má větší potenciál mít děti.

Celé znění dotazníku naleznete v příloze P1.

### 4.1 Vyhodnocení dotazníku

1) Jaké je vaše pohlaví?



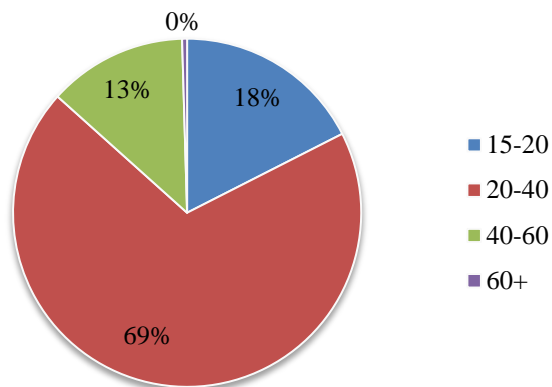
*Graf 1 – Pohlaví respondentů.*

*Tab. 2 – Pohlaví respondentů.*

Pohlaví	Počet odpovědí
Muž	72
Žena	145

Touto otázkou jsem se pokusil zjistit, zda je více respondentů mužského nebo ženského pohlaví, protože jak je známo, ženy bývají více empatické a starostlivé o své děti. Z grafu 1 a tabulky 2 vyplývá, že více respondentů byly ženy.

## 2) Kolik je Vám let?

**Kolik je Vám let?**

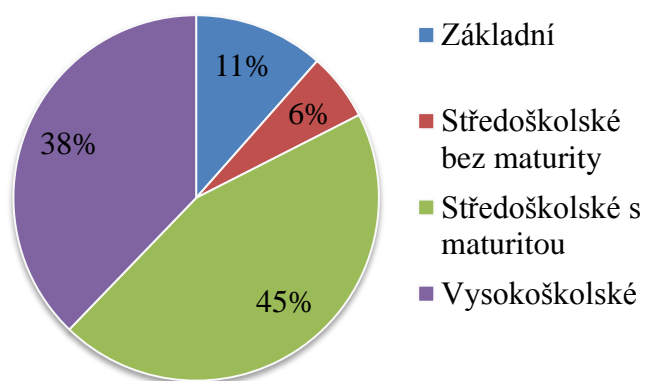
Graf 2 – Graf věku respondenta.

Tab. 3 – Tabulka věku respondentů.

Věk	Počet odpovědí
15-20	38
20-40	150
40-60	28
60+	1

Cílem této otázky bylo zjistit, v jakém věku jsou respondenti, kteří odpovídají na dotazník a jestli se podařilo zacílit na rodiče s dětmi. Jak lze vidět na grafu 2 nebo v tabulce 3, nejvíce dotázaných bylo ve věku 20-40 let. Z toho vyplývá, že se podařilo zacílit na skupinu lidí, která může mít malé děti.

## 3) Nejvyšší dosažené vzdělání?

**Nejvyšší dosažené vzdělání?**

Graf 3 – Graf vzdělání respondentů.

Tab. 4 – Nejvyšší vzdělání respondentů.

Vzdělání	Počet odpovědí
Základní	25
Středoškolské bez maturity	13
Středoškolské s maturitou	97
Vysokoškolské	82

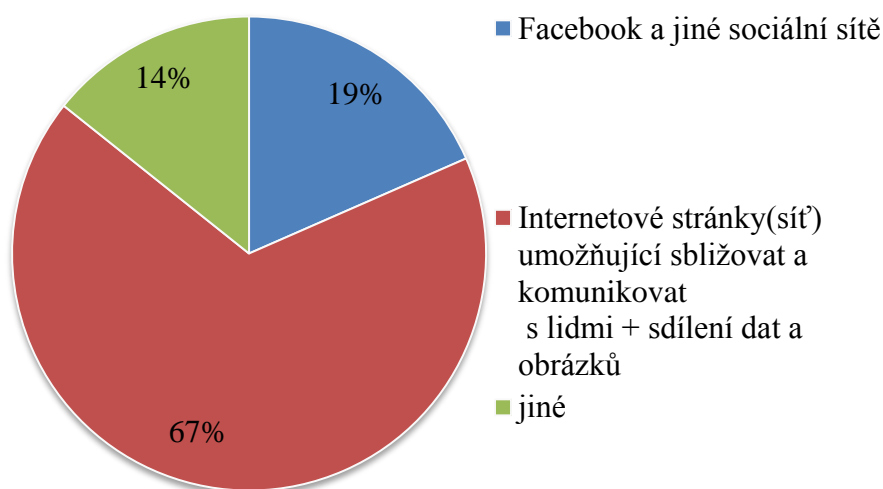
Touto otázkou bylo zjištěno, že 45% respondentů je středoškolského vzdělání s maturitou, jak vyplývá z grafu 3 a tabulky 4. Je to možná z důvodu, že lidem, kterým byl dotazník distribuován, jsou moji vrstevníci.

4) Co si představíte pod pojmem sociální síť?

Zkuste co nejpřesněji dle vlastního uvážení popsat, co to jsou sociální sítě.

Povinná otázka, respondent musel napsat odpověď vlastními slovy.

### Co si představíte pod pojmem sociální sítě?



Graf 4 – Graf povědomí o sociálních sítích.

Tab. 5 – Tabulka o povědomí sociálních sítí.

Odpověď	Počet názorů
Facebook a jiné sociální sítě	40
Internetové stránky (sítě) umožňující sblížit a komunikovat s lidmi + sdílení dat a obrázků	146
jiné	31

V dnešním světě se stále mluví o sociálních sítích, ale vědí lidé, co to sociální sítě jsou? To bylo cílem v této otázce zjistit. Z odpovědí vyplynulo, že převážná většina účastníků ví, co to sociální sítě jsou. 19% respondentů si za sociální síť doplní konkrétní stránky, například Facebook. Jak jde vidět z grafu 4 a tabulky 5, kdy 67% respondentů popsalo princip a popis sociálních stránek.

## 5) Využíváte sociální sítě?

Tab. 6 – Tabulka kolik respondentů využívá sociální sítě.

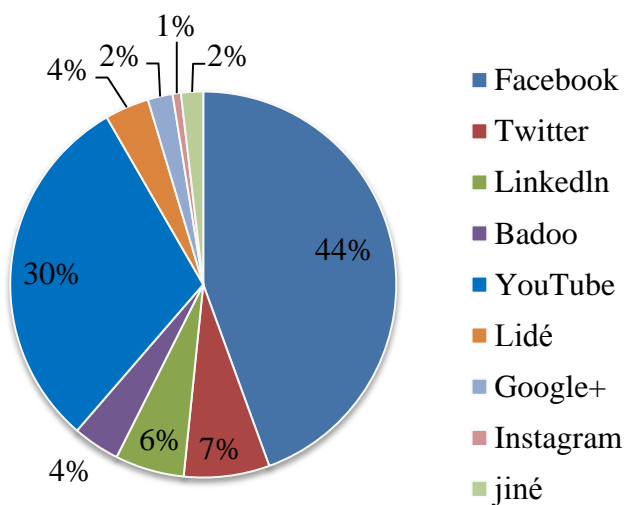
Odpověď	Počet odpovědí
Ano	197
Ne	20

Účastníci dotazníku používají sociální sítě ve velké míře. 197 odpovědělo, že sociální sítě používá a 20 respondentů ne, viz tabulka 6.

## 6) Jaké sociální sítě využíváte?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

### Jaké sociální sítě využíváte?



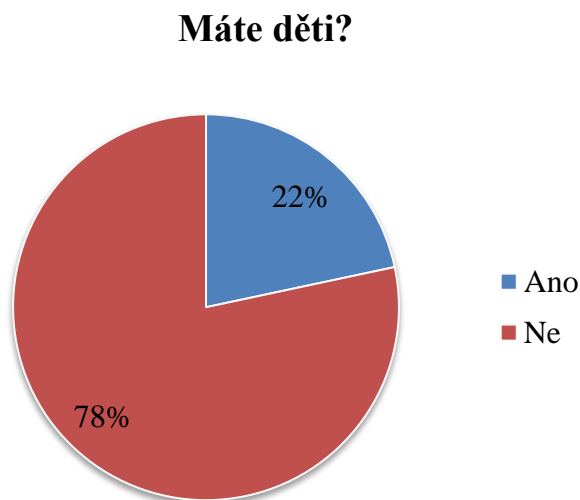
Tab. 7 – Přehled soc. sítí, které respondenti využívají.

Odpověď	Počet odpovědí
Facebook	192
Twitter	31
LinkedIn	25
Badoo	17
YouTube	131
Lidé	16
Google+	9
Instagram	3
jiné	8

Graf 5 – Přehled sociálních sítí, které využívají respondenti.

Podle předpokladů se dalo čekat, že nejvíce rozšířenou sociální sítí mezi respondenty je Facebook, následně využívají YouTube. V menší míře je rozšířený Twitter viz tabulka 7 a graf 5.

## 7) Máte děti?



*Graf 6 – Kolik respondentů má dítě.*

Touto otázkou byla snaha zjistit kolik respondentů má děti, což bylo klíčové pro další otázky v dotazníku. Jak lze vyčíst z grafu 7, tak pouze malá část respondentů má děti (22%). Většina respondentů děti nemá.

## 8) Věk Vašich dětí?

*Tab. 8 – Věk dětí.*

Věk	Počet odpovědí
0-6	15
6-10	7
10-15	13
15-18	12

Nejvíce respondentů má děti předškolního věku a ve věku dětí, které chodí na základní školu, jak vyplývá z tabulky 8. Cílem této otázky bylo zjistit, v jakém věku jsou jejich děti. Díky tomuto zjištění se můžeme připravit na prevenci, například na základních školách nebo ve školkách.

9) Dovolujete pracovat dítěti na počítači?

*Tab. 9 – Dovolujete pracovat  
dítěti na počítači.*

Odpověď	Počet odpovědí
Ano	40
Ne	9

Z tabulky 9 lze zjistit, že 40 respondentů, kteří mají děti, dovoluje dětem být na počítači. Důvod, proč rodiče nedovolují dětem být na počítači, bude rozebrán v následující otázce.

10) Proč?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

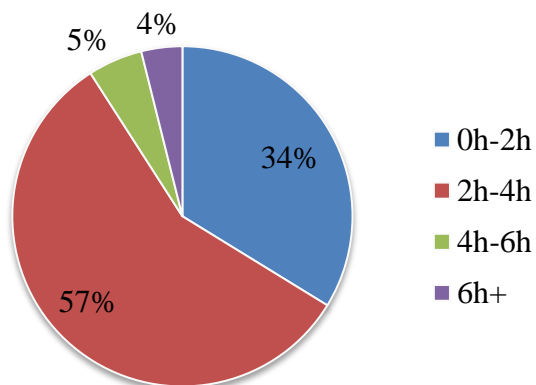
*Tab. 10 – Tabulka doplňujících odpovědí k otázce č. 9.*

Odpověď	Počet
Na počítač jsou ještě malé	7
Počítač využívám výhradně k práci	1
Chci je co nejvíce ochránit před negativním vlivem Internetu (pornografie, kyberšikana, nevhodné hry)	1

Touto otázkou bylo za cíl zjistit, proč rodiče nedovolují svým dětem být na počítači. Jak z tabulky 10 vyplývá, děti jsou na počítač ještě malé, což můžeme vyčíst i z tabulky 8, kdy 15 respondentů odpovědělo, že jejich děti jsou ve věku 0-6 let.

11) Kolik hodin tráví vaše děti na počítači?

### Kolik hodin tráví Vaše děti na počítači?



Tab. 11 – Tabulka počtu hodin, které dítě tráví na počítači.

Odpověď	Počet odpovědí
0h-2h	26
2h-4h	44
4h-6h	4
6h+	3

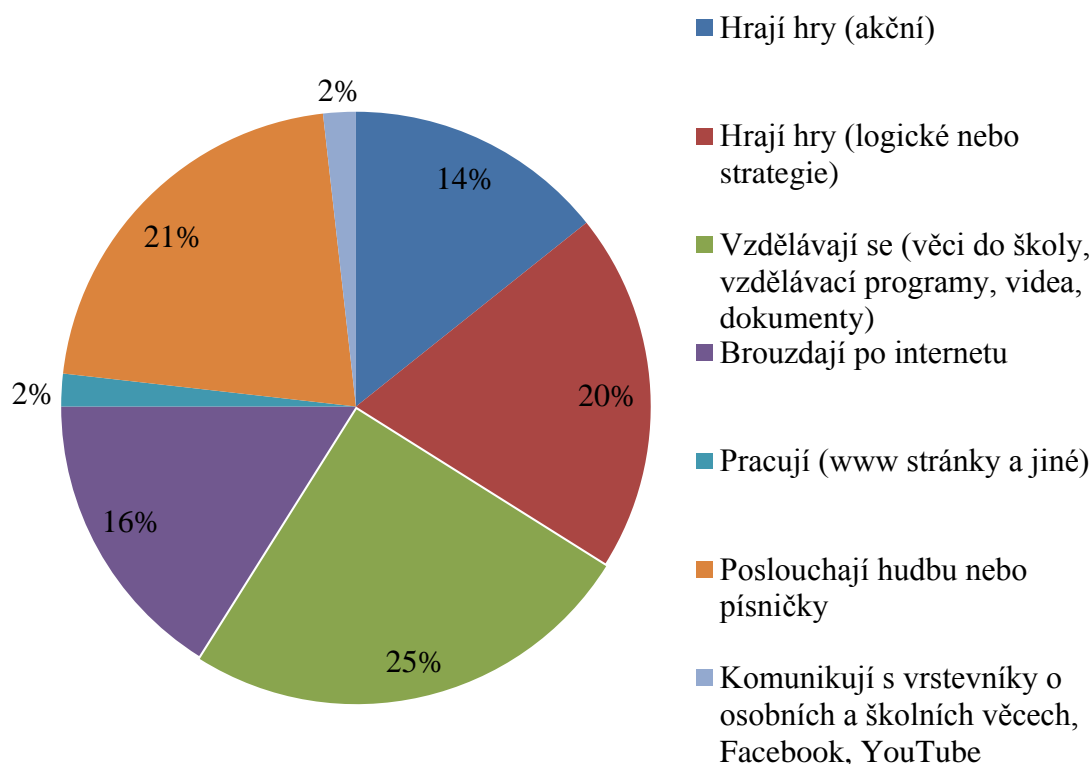
Graf 7 – Graf počtu hodin, které tráví děti na počítači.

Nejvíce času děti na počítači tráví od 2 až do 4 hodin, viz graf 8 nebo tabulka 11. Když bychom brali, že dítě přijde ze školy ve 14 hod., tak v podstatě většinu svého volného času tráví na počítači.

## 12) Co Vaše děti dělají na počítači?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

## Co Vaše děti dělají na počítači?



Graf 8 – Graf činností dětí na počítači.

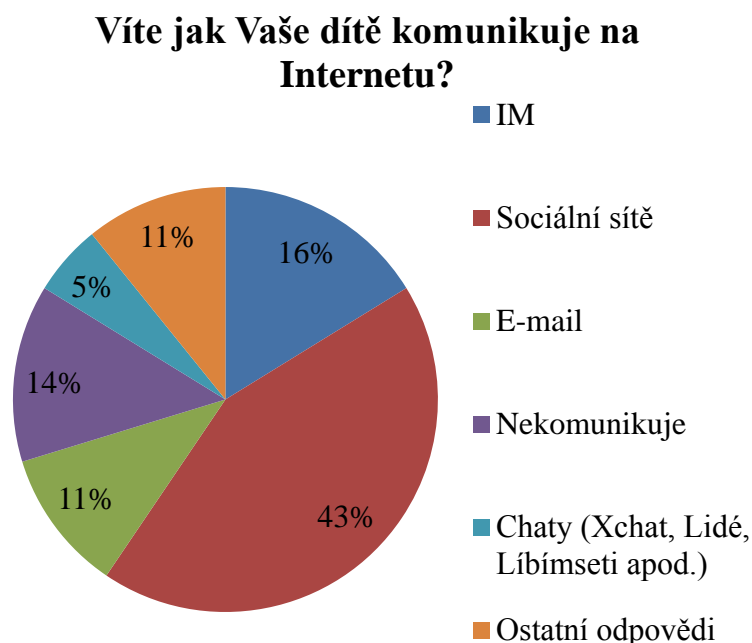
Tab. 12 – Tabulka činností dětí na počítači.

Odpověď	Počet odpovědí
Hrají hry (akční)	16
Hrají hry (logické nebo strategie)	22
Vzdělávají se (věci do školy, vzdělávací programy, videa, dokumenty)	28
Brouzdají po Internetu	18
Pracují (www stránky a jiné)	2
Poslouchají hudbu nebo písničky	24
Komunikují s vrstevníky o osobních a školních věcech, Facebook, YouTube	2

Podle respondentů jejich děti tráví čas na počítači učením, jak vyplývá z tabulky 12 nebo z grafu 9. Další nejčastější odpovědí bylo, že dítě tráví čas na počítači posloucháním hudby. Otázkou ovšem zůstává, jak často rodiče kontrolují děti v průběhu toho, co jsou na počítači.

### 13) Víte, jak Vaše dítě komunikuje na Internetu?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.



*Graf 9 – Graf komunikace dětí na Internetu.*

*Tab. 13 – Tabulka komunikace dětí na Internetu.*

Odpověď	Počet odpovědí
IM	6
Sociální síť	16
E-mail	4
Nekomunikuje	5
Chaty (Xchat, Lidé, Líbímseti apod.)	2
Ostatní odpovědi	4

Z grafu 10 i tabulky 13 je patrné, že nejoblíbenějším komunikačním nástrojem jsou sociální síť, což uvedlo 43% dotázaných respondentů.

14) Má Vaše dítě účet na sociální síti?

*Tab. 14 – Tabulka profilu*

*dítěte na sociální síti.*

Odpověď	Počet odpovědí
Ano	25
Ne	12

Z tabulky 14 se dá říct, že rodiče vědí, že jejich dítě má profil na soc. sítích, protože 25 dotázaných respondentů odpovědělo, že jejich dítě má profil na sociální síti.

15) Co děláte pro vzdělávání Vašich dětí, aby se mohl bezpečně pohybovat na Internetu?

Nepovinná otázka, respondent mohl zvolit více z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

*Tab. 15 – Tabulka opatření, aby se děti mohly pohybovat bezpečně na Internetu.*

Odpověď	Počet odpovědí
Mluvím s nimi o hrozbách (stalking, kyberšikana, pedofililové...)	27
Spoléhám se na to, co se dozví ve škole	8
Nic	4
Kontroluji a omezuji možnosti jejich PC	2
Učím je, co je to ochrana soukromí	2
Zatím jsou malé na Internet	2

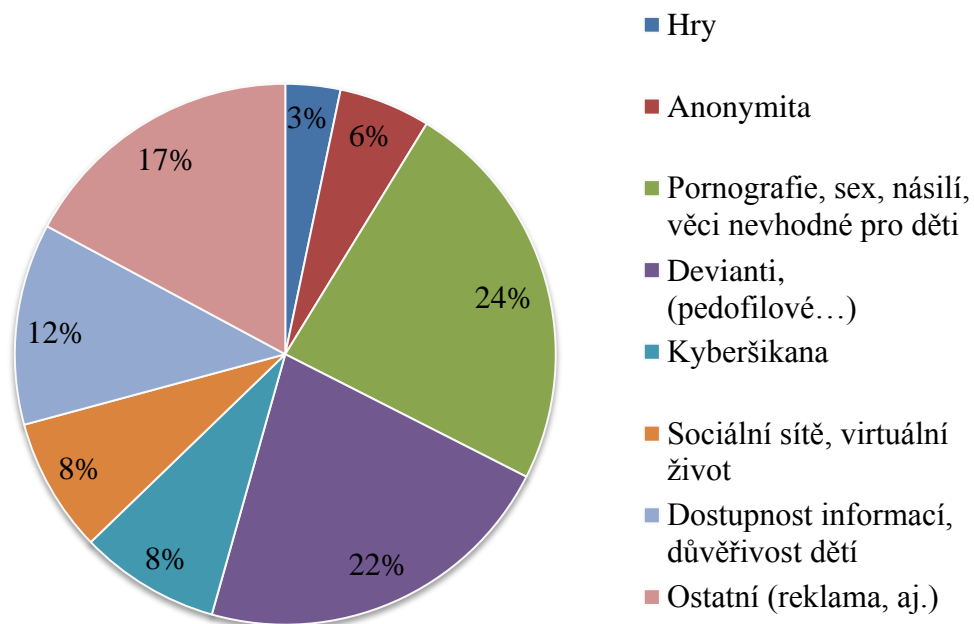
Respondenti se snaží se svými dětmi mluvit o hrozbách, které na ně mohou číhat na Internetu, jak vyplývá z tabulky 15. Považují to za nejúčinnější ochranu proti hrozbám na internetu.

16) Co je podle Vás největší hrozba na Internetu pro děti?

Co nejvíce ohrožuje děti na Internetu? Co může mít nejvíc negativní vliv?

Povinná otázka, respondent musel napsat odpověď vlastními slovy.

### Co je podle Vás největší hrozba na Internetu pro děti?



Graf 10 – Graf největších hrozeb na Internetu dle respondentů.

*Tab. 16 – Tabulka největších hrozeb Internetu dle respondentů.*

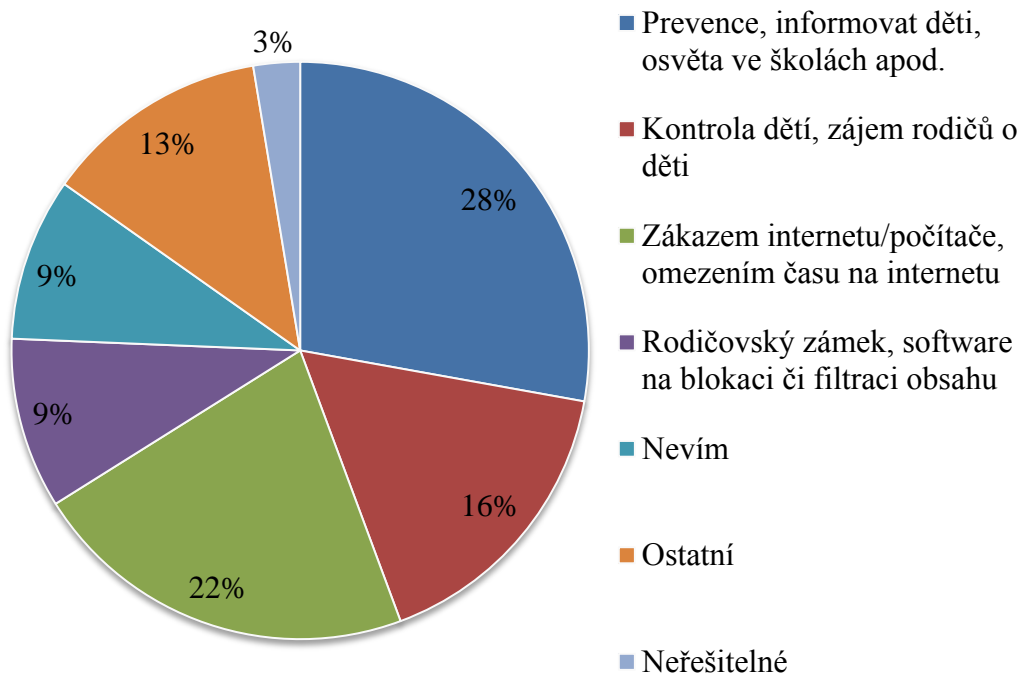
Odpověď	Počet odpovědí
Hry	9
Anonymita	15
Pornografie, sex, násilí, věci nevhodné pro děti	65
Devianti, (pedofilové...)	60
Kyberšikana	23
Sociální sítě, virtuální život	22
Dostupnost informací, důvěřivost dětí	33
Ostatní (reklama, aj.)	47

V této otázce se respondenti rozcházeli v odpovědích, přesto nejvíce odpovědí získala odpověď – porno, sex, násilí a věci nevhodné pro děti. Následně nejvíce hlasů získala odpověď – devianti, viz graf 11, nebo tabulka 16.

17) Jak byste tuto hrozbu řešili?

Povinná otázka, respondent musel napsat odpověď vlastními slovy.

### Jak byste tuto hrozbu řešili?



Graf 11 – Graf navrhovaných řešení hrozeb na Internetu dle respondentů.

Tab. 17 – Tabulka navrhovaných řešení hrozeb na Internetu dle respondentů.

Odpovědi	Počet odpovědí
Prevence, informovat děti, osvěta ve školách apod.	64
Kontrola dětí, zájem rodičů o děti	38
Zákazem Internetu/počítače, omezením času na Internetu	50
Rodičovský zámek, software na blokaci či filtraci obsahu	22
Nevím	21
Ostatní	29
Neřešitelné	6

Respondenti se ve většině odpovědí shodovali a odpovídali, že tato hrozba se dá řešit prevencí a celkovou osvětou o těchto hrozbách. Druhé řešení, dle respondentů, je velmi razantní. Buď by zakázali počítač úplně, nebo by omezili alespoň čas strávený na počítači, viz graf 12 a tabulka 17.

18) Od kolika let může být dítě zaregistrováno na Facebooku či Twitteru?

Bez hledání na Internetu víte, od kolika let může mít dítě vlastní facebookový nebo twitterový účet?

Nepovinná otázka, respondent mohl zvolit jednu z nabízených odpovědí.

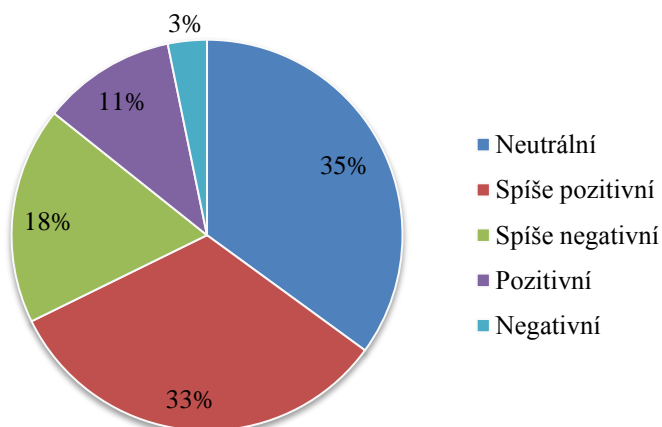
Tab. 18 – Tabulka věkové hranice pro registraci na Facebook a Twitter.

Věk	Počet
Věk není omezen	78
11	4
12	22
13	58
14	11
15	38

Z tabulky 18 lze vyčíst že, 78 respondentů si myslí, že věk na Facebook a Twitter není omezen. 58 respondentů si myslí, že věk je omezený na hranici 13 let. 38 respondentů odpovídalo, že věková hranice registrace na tyto servery je od 15 let.

19) Jaký máte postoj k sociálním sítím?

### Jaký máte postoj k sociálním sítím?



Tab. 19 – Tabulka postoj k sociálním sítím.

Odpověď	Počet odpovědí
Neutrální	76
Spíše pozitivní	71
Spíše negativní	39
Pozitivní	24
Negativní	7

Graf 12 – Graf postoje k sociálním sítím.

Otázkou bylo cíleno na to, jak respondenti nahlíží na sociální sítě. Jak lze posoudit z grafu 13 a tabulky 19, 33% respondentů má spíše pozitivní postoj k sociálním sítím. 35% má neutrální postoj.

20) Myslíte, že osvěta je v dnešní době dostačující?

*Tab. 20 – Tabulka dostačující*

*osvěty.*

Odpověď	Počet odpovědí
Ano	80
Ne	137

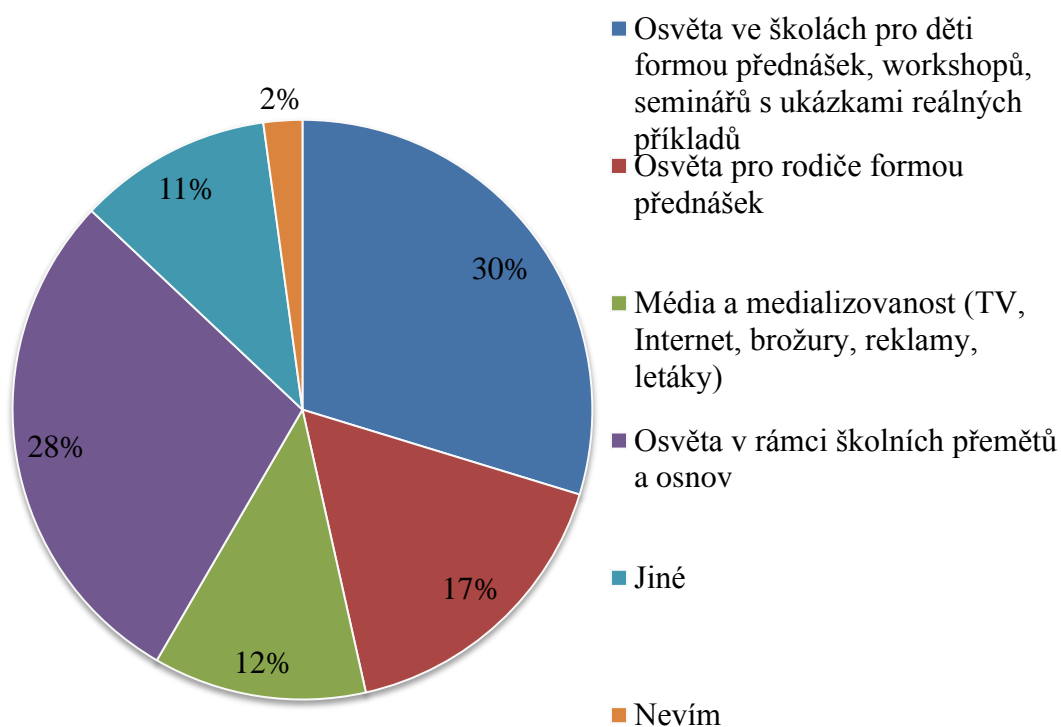
Většina respondentů podle tabulky 20 má názor, že osvěta není u nás dostačující.

21) Co byste udělal/a nebo zavedl/a, aby osvěta byla dostačující?

Zkuste popsat, co by podle Vás bylo dostačující, aby si děti uvědomovaly hrozby Internetu. Např. Více hodin ve školách zaměřených na toto téma, Semináře pro širokou veřejnost atd.

Povinná otázka, respondent musel napsat odpověď vlastními slovy.

### Co byste udělal/a nebo zavedl/a, aby osvěta byla dostačující?



Graf 13 – Graf návrhu řešení osvěty.

Tab. 21 – Tabulka návrhů od respondentů na zlepšení osvěty.

Odpověď	Počet odpovědí
Osvěta ve školách pro děti formou přednášek, workshopů, seminářů s ukázkami reálných příkladů	55
Osvěta pro rodiče formou přednášek	31
Média (TV, Internet, brožury, reklamy, letáky)	22
Osvěta v rámci školních předmětů a osnov	53
Jiné	20
Nevím	4

Otázka 21 navazuje z části na otázku 20. Respondenti v 30% by uvítali osvětu v rámci školy, formou workshopů a přednášek. 28% respondentů by chtělo zavést osvětu přímo do osnov ve školách.

## 4.2 Zhodnocení dotazníku

Na dotazník odpovídaly převážně ženy ve věku od 20 do 40 let a díky tomu jsem mohl posoudit, jak na ochranu dětí na internetu nahlíží skupina lidí, která má potenciál mít děti. V dotazníku převažovali respondenti se středoškolským vzděláním, které měli ukončené maturitní zkouškou a také vysokoškoláci.

Respondenti využívají sociální sítě. Nejvíce využívají Facebook, za kterým následuje YouTube. Facebook je všeobecně velmi populární sociální síť, kterou využívají všechny generace uživatelů Internetu. 78% respondentů je bezdětných, tudíž část dotazníku, který se zabývá konkrétně dětmi, vyplnilo 22% dotázaných. Věk dětí respondentů se pohybuje od 0-6 let (32% odpovědí), 6-10 let (15% odpovědí), 10-15 let (28% odpovědí), 15-18 let (26% odpovědí).

82% respondentů, kteří mají děti, dovoluje používat počítač dětem. Nejčastěji děti tráví 2-4 hodiny na počítači a jejich pracovní náplní je vypracovávání věcí do školy a poslouchání písniček nebo hrají logické a strategické hry.

Nejvíce děti respondentů komunikují pomocí sociálních sítí. Zdá se, že doba instant messangu je dávno pryč. 66 % respondentů uvedlo, že jejich dítě má profil na sociální síti. Respondenti se snaží s dětmi komunikovat a upozornit je na hrozby, které je mohou potkat na Internetu, protože dle výsledků dotazníku největší hrozby jsou pornografie, sex, násilí apod., dále pak různí devianti, pedofilové a jiné. Sami respondenti by tuto hrobu řešili osvětou ve školách nebo omezením doby dítěte na počítači či úplným zákazem počítače. 35,94 % dotázaných se domnívá, že Facebook či Twitter není omezený věkem, kdy se na tyto stránky může dítě registrovat. Pouze 27% respondentů odpovědělo správně, že věk je omezen na 13 let. Třetina respondentů má neutrální postoj k sociálním sítím a další třetina spíše pozitivní postoj.

63% dotázaných je přesvědčeno, že osvěta u nás není dostatečná. Respondenti by zavedli osvětu především do školních osnov a do předmětů (IT, Rodinná výchova apod.) Ocenili by taky osvětu ve školách formou přednášek, seminářů a různých workshopů, kde by byly i reálné příklady ze života. Hodně respondentů zmiňovalo nejen osvětu pro děti, ale i pro

rodiče, kteří s tímto novodobým fenoménem nemají žádné zkušenosti. Přínosné by bylo také, kdyby se média a reklama o této hrozbě více zmiňovala.

### 4.3 Osobní zhodnocení

Z dotazníku jsem zjistil, že rodiče se snaží s dětmi mluvit o hrozbách, ale uvítali by pomoc školy nebo pomoc formou přednášek a prezentací. Respondenti mají základní povědomí o hrozbách na Internetu, což mne velmi potěšilo, avšak stále mám dojem, že to není zcela dostačující.

Z dotazníku mi vyplynulo, že se rodiče snaží děti kontrolovat a hlídat. Tato metoda je v pořádku, bohužel nejen doma se děti dostanou k počítači, takže tento systém je účinný jen z části. Zákazy počítače jsou něco jako slovní spojení, že zakázané ovoce nejvíce chutná. Tento směr nevidím jako řešení, ba naopak důsledky mohou být daleko horší.

Jako jedinou cestu kterou vidím, je osvěta. Jak se říká, že rodina je základ, proto bych začal osvětou u rodičů. Pokud si rodiče budou vědomi toho, že na Internetu to může být velmi podobné jako na silnici, tak na své děti budou dávat větší pozor a dokážou jim jednoduše vysvětlit, že se přechází na zelenou.

Lékaři tvrdí, že nejlepší obranou je prevence. To platí i o bezpečnosti na Internetu. Pokud děti budou už od útlého věku vědět, že Internet není plný jen hezkých a užitečných věcí, ale že tam jsou i nebezpečí, které někdy končí velmi špatně, tak si na tyto věci budou dávat větší pozor. Budou na to připravené a budou vědět, o co se jedná, když je bude chtít někdo vylákat na schůzku do parku.

Avšak ani osvěta není 100% lék. Myslím si, že ani 100% lék neexistuje. I když to dítě ví, že se na červenou nechodí, někdy přes cestu přeběhne.

## 5 NÁVRH ŘEŠENÍ DLE VÝZKUMU Z DOTAZNÍKU

V této části práce se budu věnovat návrhu možného řešení, které mi vyplynulo z dotazníku. Mým cílem je, aby tyto návrhy nezůstaly jen na papíře, ale také aby byly převedeny do praxe. A o to se budu snažit.

### 5.1 Vzdělání rodičů

Důležitým faktorem jsou rodiče. Tak jako škola nemůže děti vychovávat k tomu, aby se slušně chovaly, tak nemůže zabezpečit 100% vzdělání ohledně chování na Internetu.

Důležité je, aby rodiče věděli, proč je pro ně osvěta a celkově vzdělání důležité. Dále musí vědět, jak ji aplikovat na své děti, aby byla co nejvíce efektivní. V neposlední řadě taky musí znát jaká opatření a co konkrétně pro děti udělat, aby co nejvíce minimalizovali ohrožení.

#### 5.1.1 Veřejné semináře

Veřejný seminář by měl pomáhat rodičům zorientovat se ve virtuálním světě, ve kterém se pohybují jak oni sami, tak hlavně jejich děti.

Setkání by měla být co nejvíce obecná, protože lidé, kteří jsou staršího věku, by měli vědět, jak funguje Internet, co to vlastně je a jak s ním pracovat.

Obecná osnova semináře

- Úvod – Cíl dnešního setkání
- Obecné informace pro rodiče
- Proč děti chránit
- Jaké jsou nejčastější nástrahy a jaké jsou možnosti ochrany
- Co konkrétně podniknout pro nejefektivnější ochranu dětí

Celý seminář by měl trvat dvě hodiny s možností otevřené diskuze. Pro oživení a přiblížení problematiky, by zde měly zaznít i reálné příběhy, které se opravdu staly. Více v příloze (příloha – prezentace seminář pro dospělé).

#### 5.1.2 Kurzy a workshopy

Kurzy a workshopy jsou jednodenní, či vícedenní setkání za účelem lepšího porozumění této problematiky. Měly by obsahovat praktické ukázky hrozeb a jejich ochrany před nimi. Od zabezpečení počítače po ukázky komunikace s dětmi.

## **Kurzy**

Kurzy by byly rozděleny na dva stupně – začátečníci a pokročilí. S tím, že postupem času bude více pokročilých.

Začátečníkem myslím rodiče, kteří nemají vztah k počítači, nebo mají pouze minimální povědomí o počítačích a Internetu.

Pokročilí jsou rodiče, kteří s počítačem pracují na denní bázi. Mají povědomí o výpočetní technice a Internetu.

### **Kurz pro rodiče začátečníky**

Tento kurz by byl postaven na týdenní bázi po dobu tří týdnů. Vždy by se setkávali lidé jeden den v týdnu, kde by probírali dané téma. Rodiče by měli týden na to, aby si dovednosti mohli vyzkoušet doma na svých zařízeních. Cílem vzdělávání je uvést rodiče do problematiky informačních technologií.

Témata:

První týden - Základem by bylo seznámit rodiče s fungováním počítače a jeho nastavením. S prací na Internetu, nastavením antiviru apod.

Druhý týden – Jaké jsou hrozby na Internetu. Co všechno může dětem hrozit.

Třetí týden – Jaké kroky podniknout a jak ty to kroky komunikovat směrem k dětem, aby to pochopily.

### **Kurz pro pokročilé**

Kurz pro pokročilé má výhodu, že do tohoto kurzu by se mohli přihlásit lidé, kteří buď prošli kurzem prvním nebo s počítačem mají zkušenost. Cílem tohoto vzdělání je hlouběji prozkoumat hrozby a jejich následné řešení a také prevenci.

První týden – detailní rozebrání hrozeb (pornografie, násilné hry, chatování s cizími lidmi, stalking apod.)

Druhý týden – prevence a řešení problémů z prvního týdne.

## **Workshop**

Jednodenní setkání s rodiči, kde by byla více probrána témata: Proč je důležitá ochrana dětí, nejvážnější hrozby, jak děti chránit a prevence před problémy.

## 5.2 Vzdělání dětí

Cílem vzdělání dětem vysvětlit proč jsou hrozby pro ně nebezpečné, jak se sami mohou chránit a bránit. Hodně záleží na přístupu k této problematice, proto je dobré rozdělit vzdělání pro základní školy a pro střední školy. Tuto část jsem rozdělil do dvou skupin.

### 5.2.1 Vzdělání v rámci hodin informatiky

V rámci výuky informatiky by měly být děti vzdělávané o povědomí hrozeb na Internetu, protože děti Internet využívají všude a v dnešní době nejen na počítači, ale i na tabletech a mobilních telefonech. Tráví na něm i několik hodin denně a jsou tak vystaveny daleko většímu riziku.

V prvé řadě by měli být vzděláni učitelé, protože se občas setkávám s tím, že ani učitelé přesně neví, co by děti mohlo ohrozit.

Pro děti, které chodí do základní školy, by toto téma měly dostat hravou formou, aby je bavilo, například hrou, příběhem.

Problémem mohou ovšem být osnovy školy, které nemusí umožňovat toto vzdělání.

### 5.2.2 Vzdělání s externím pracovníkem

Již v dnešní době se ve školách děti vzdělávají s externími pracovníky, se kterými si povídají o hrozbách na internetu. Například Policie ČR dělá přednášky na školách, kde si s dětmi povídají o hrozbách na internetu, jak se proti tomu bránit. Dávají dětem také různé materiály a letáky. Bohužel tato školení nebo workshopy nejsou moc časté.

Další alternativou mohou být neziskové organizace, které by pořádaly vzdělávání dětí, dospělých a také učitelů samotných. Takové organizace nebo projekty již existují, například soutěžní projekt Paragraf 11/55, který zastřešovala Aliance Zákon 18, kdy bylo za cíl zvýšit povědomí žáků základních škol a gymnázií o zákoně č. 37/1989 Sb., který pojednává o prodeji tabákových a alkoholických produktů. [33],[34]

## 6 SOFTWAREVÉ ZABEZPEČENÍ POČÍTAČE

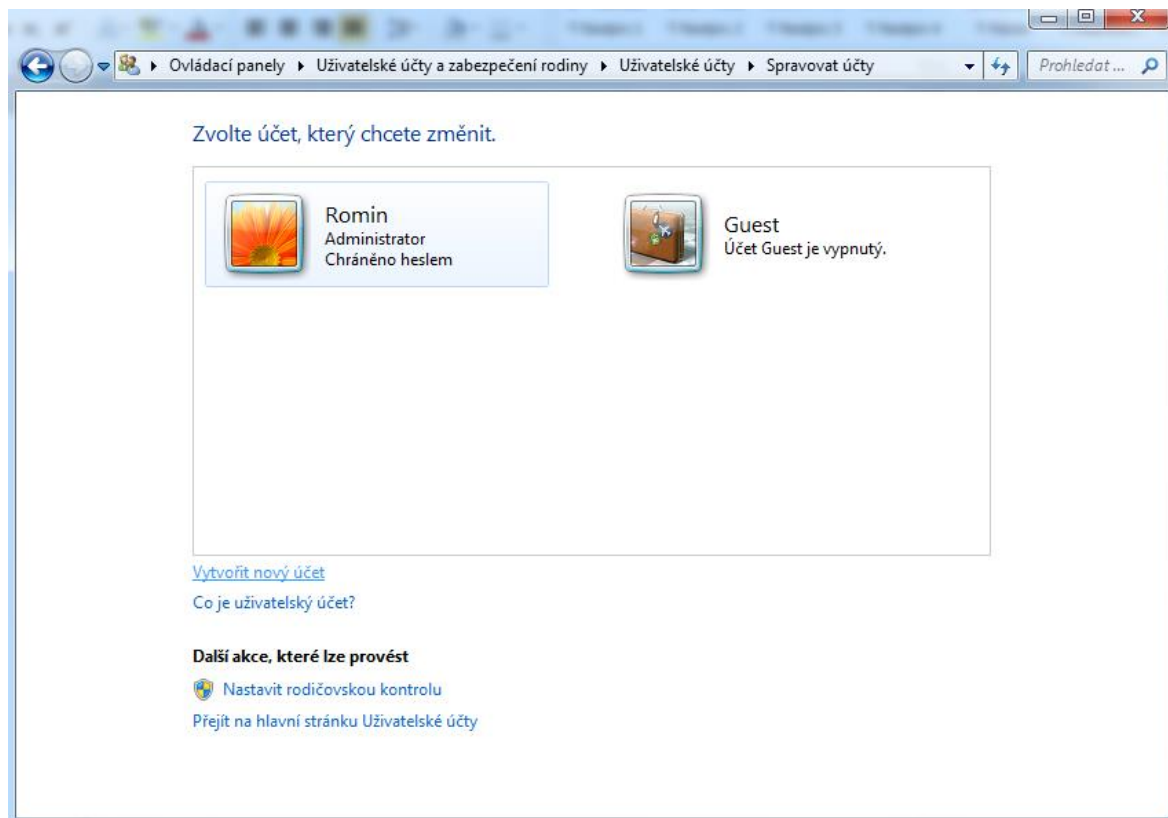
V této části se budu věnovat zabezpečení počítače z pohledu software. Existuje několik programů, které dokážou filtrovat a blokovat určité stránky nebo monitorovat práci na počítači. Nejrozšířenější operační systém, dle výzkumů, je Microsoft Windows 7, proto všechna nastavení byla řešena pomocí operačního systému Microsoft Windows 7 Home Premium. [35] Jednou z důležitých věcí je, aby dítě mělo svůj standardní uživatelský účet. Je to z několika důvodů. Můžeme na tento účet nastavit rozdílná práva. Dokonce pokud máme dětí víc, například jedno je o pár let starší a chtěli bychom mu nastavit rozdílná práva k používání počítače, tak je dobré, aby měl každý svůj účet s určitými právy.

### 6.1 Vestavěné funkce systému

Systém Windows 7 nabízí určité formy základního zabezpečení. V následujících kapitolách budou jednotlivé možnosti dopodrobna rozebrány.

#### 6.1.1 Vytvoření standardního uživatelského účtu pro děti

Abychom mohli nastavit rodičovskou ochranu, je třeba vytvořit nový standardní účet pro dítě, viz Obr 1. Klikneme na tlačítko Start, dále na Ovládací panely, následně Přidat nebo odebrat rodičovské účty. Zde jsou zobrazeny všechny vytvořené účty. Klikneme na Vytvořit nový účet. Zadáme název nového účtu např. Karlík a ponecháme zatrhnuto standardní uživatel. Dokončíme vytvoření účtu pomocí tlačítka vytvořit účet.



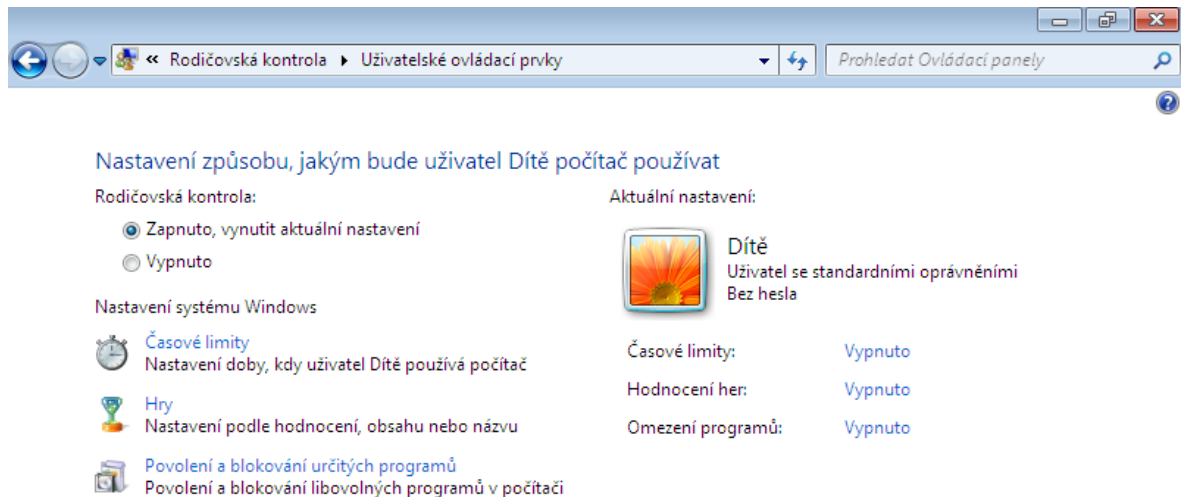
Obr. 4 – Vytvoření standardního uživatelského účtu.

### 6.1.2 Rodičovská kontrola

Rodičovská kontrola je jeden z nejzákladnějších nástrojů ochrany. Pomocí rodičovské ochrany můžeme ovlivňovat používání počítače dětmi. Pomocí rodičovské kontroly můžeme nastavit a spravovat tři hlavní okruhy zabezpečení. Nastavení časových limitů pro používání počítače dětmi, omezení her, které děti mohou hrát a také omezením konkrétních programů. Rodičovská kontrola s pomocí aplikace Windows Media Center umožňuje zablokovat přístup ke sporným televizním pořadům a filmům. Rodičovská kontrola je součástí systému Windows.

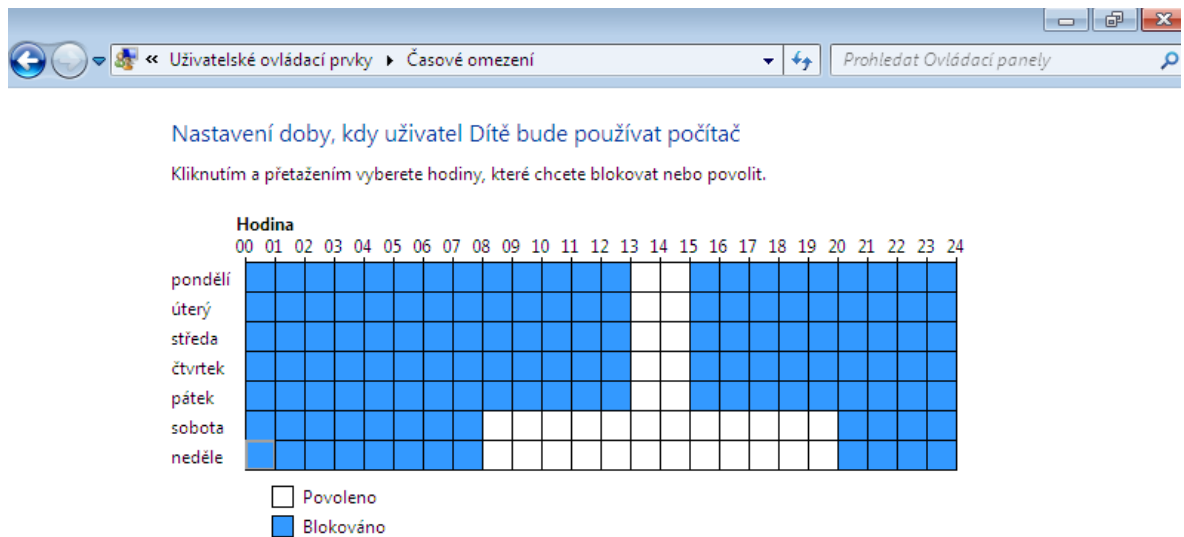
### 6.1.3 Zapnutí rodičovské ochrany

Rodičovskou kontrolu zapneme přes tlačítko Start, dále Ovládací panely, následně kliknout Uživatelské účty a zabezpečení rodiny, kde je položka Nastavit rodičovskou kontrolu pro všechny uživatele, viz Obr 2. Systém vás může vyzvat, abyste zadali heslo správce. V následujícím kroku vyberte profil, na který chcete aplikovat rodičovskou kontrolu. V položce Rodičovská kontrola zatrhněte Zapnuto, vynutit aktuální nastavení.



Obr. 5 – Nastavení rodičovské kontroly.

#### 6.1.4 Časový limit



Obr. 6 – Nastavení časového limitu

Na Obr. 3 vidíme, jak se dá nastavit časový limit. Čtverečky znázorňují hodiny. Bílé čtverečky je povolená doba, kdy dítě může být na počítači. A modré kdy je počítač blokován.

Je to jeden ze způsobů kontroly, kdy můžeme povolit dítěti být na počítači jen v tu dobu, kdy jsme doma.

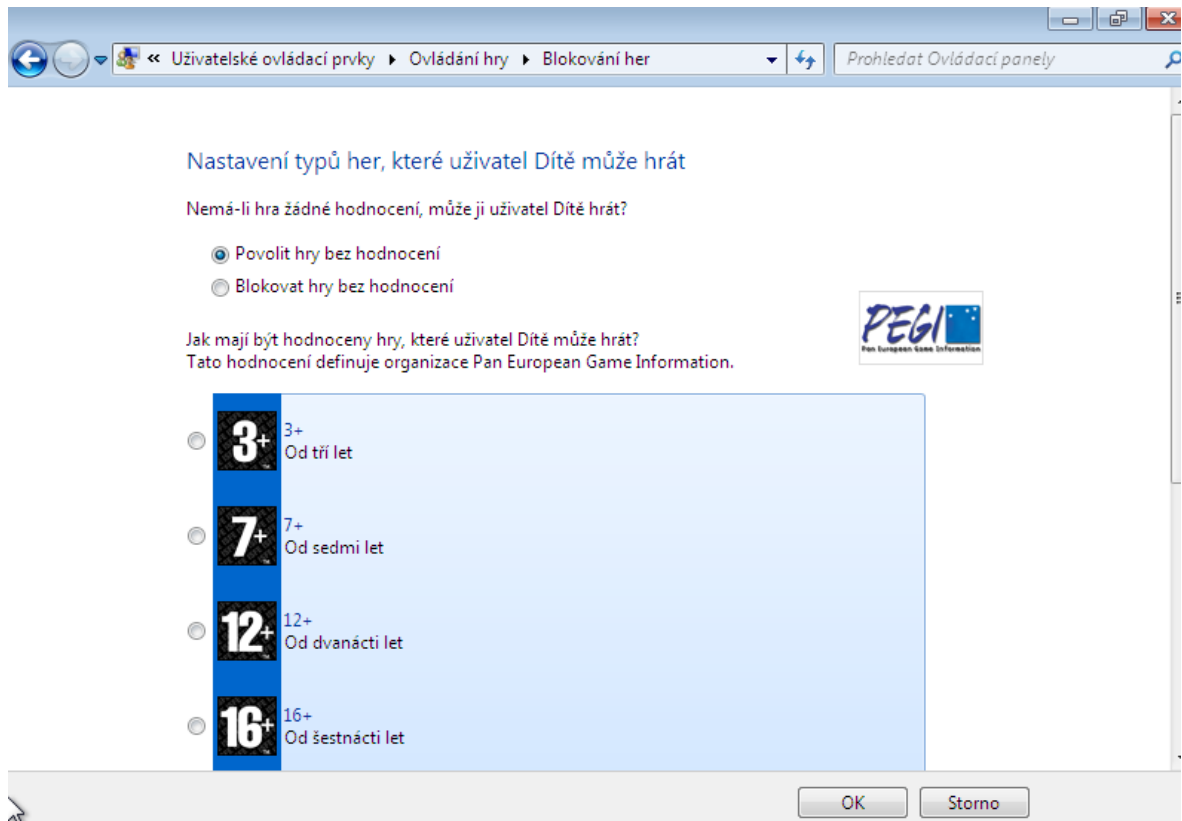
### 6.1.5 Hry

V této záložce můžeme na profil nastavit omezení hraní her. Hned na začátku můžeme nastavit pro daný profil, jestli může hrát hry. Další nastavení je podle hodnocení a typu obsahu, viz Obr 4. Toto hodnocení zastřešuje ratingová organizace Pan European Game Information, které hodnotí hry. PEGI je Evropský ratingový systém počítačových her pro lepší určení obsahu her. Hodnocení je zaznačeno nálepkou na obalu hry a tento systém značení zavedla federace Interactive Software Federation of Europe v roce 2003 na podporu rodičům, při výběru her pro děti. Nyní tento systém používá více jak 30 zemí světa a k jeho používání se vztahuje kodex chování, který musí vydavatelé dodržovat. [36]

Vždy se dá nastavit dle věku hráče, například 3+, 7+, 12+, 16+ a 18+.

Hlavní nálepkou, tudíž rozdělením je do věkových kategorií, ale jsou tu i doplňující nálepky, které určují doplňující popis hry.

- Vulgární mluva – hra obsahuje vulgární mluvu
- Diskriminace – hra obsahuje vylíčení nebo materiál, který může podpořit diskriminaci
- Drogy – Hra se vztahuje nebo popisuje užívání drog
- Strach – Hra může nahánět strach nebo děsit malé děti
- Gamblerství – Hra podporuje nebo učí gamblerství
- Sex – Hra ukazuje nahotu, sexuální chování nebo sexuální odkazy
- Násilí – Hra obsahuje prvky násilí
- Online – Hra může být hrána online



Obr. 7 – Nastavení typů her, které může dítě hrát.

Další možností blokování her je podle názvu hry. Pro určitou hru můžeme nastavit buď její povolení, blokování a také vidíme stav, tzn. jestli je daná hra blokována či nikoliv.

V USA a v Kanadě se ratingem her zabývá společnost ESRB ( Entertainment Software Ranting Broad), systém je podobný jako PEGI.

ESRB má tři části [37]

- Rating Categories – navrhovaný přiměřený věk
- Content Descriptors – popis obsahu, který může ovlivnit hodnocení
- Interactive Elements – interaktivní prvky, které určují interaktivnost, sdílet polohu s ostatními uživateli nebo sdílení osobních informacích třetím stranám.

Rating podle ESRB [37]

- Early Childhood (eC) – vhodné pro věk 3 a více
- Everyone (E) – 6 a více let
- Everyone 10+ (E10+) – 10 a více let
- Teen (T) – 13 a více let
- Mature (M) – 17 a více let

- Adults Only (AO) – 18 a více let

Více rozepsané druhy obsahu nalezneme v tabulce 22.

Tab. 22 – Druhy obsahu dle ESRB[37].

Název	Herní obsah	Hodnocení
Alcohol Reference	Odkazy a/nebo obrázky alkoholických nápojů	E10+, T, M
Animated Blood	Zabarvené a/nebo nereálné vyobrazení krve	E, E10+, T, M
Blood	Vyobrazení krve	T, M, AO
Blood and Gore	Vyobrazení krve a/nebo zmrzačení lidských končetin	T, M, AO
Cartoon Violence	Násilné akce zahrnující komiksově situace a charaktery. Může obsahovat násilí, kde postavy jsou po akci nezraněny	E, E10+, T
Comic Mischief	Vyobrazení nebo dialogu zahrnující groteskní nebo sugestivní humor	E, E10+, T
Drug Reference	Odkazy a/nebo obrázky nelegálních drog	T, M, AO
Fantasy Violence	Násilné činy fantasy povahy, týkající se postavy v situacích, snadno odlišitelných od reálného života	E, E10+, T
Intense Violence	Grafické a realisticky vypadající vyobrazení fyzického konfliktu. Může obsahovat extrémní a/nebo realistickou krev, zbraně a vyobrazení zranění a/nebo smrti	M, AO
Language	Mírná až středně závažná hanlivost	E10+, T, M
Lyrics	Mírné narážky v hudbě na sex, násilí, alkohol a/nebo drogy	E10+, T, M
Mature Humor	Vyobrazení nebo dialogy obsahující "humor pro dospělé", může obsahovat narážky na sex	M, AO
Nudity	Názorné a/nebo dlouhodobé vyobrazení nahoty	M, AO
Partial Nudity	Krátké a/nebo mírné vyobrazení nahoty	T, M (občas AO)
Real Gambling	Hráč může hrát hazardní hry obsahující sázky o skutečné peníze a/nebo měnu	M, AO
Sexual Content	Mírné vyobrazení sexuálního chování, může zahrnovat částečnou nahotu	(může T) M, AO,
Sexual Themes	Odkazy na sex nebo sexualitu	T, M (občas AO)
Sexual Violence	Vyobrazení znásilnění nebo jiného sexuálního násilí	AO
Simulated Gambling	Hráč může hrát hazardní hry neobsahující sázky o skutečné peníze a/nebo měnu	E, E10+, T, M
Strong Language	Explicitní a/nebo časté používání vulgarismů	(občas T,) M, AO
Strong Lyrics	Explicitní a/nebo časté narážky v hudbě na vulgárnost, sex, násilí, alkohol a/nebo drogy	(občas T,) M, AO
Strong Sexual Content	Explicitní a/nebo časté zobrazování sexuálního chování, může obsahovat nahotu	M, AO
Suggestive Themes	Mírně provokativní odkazy nebo materiály	E, E10+, T, M

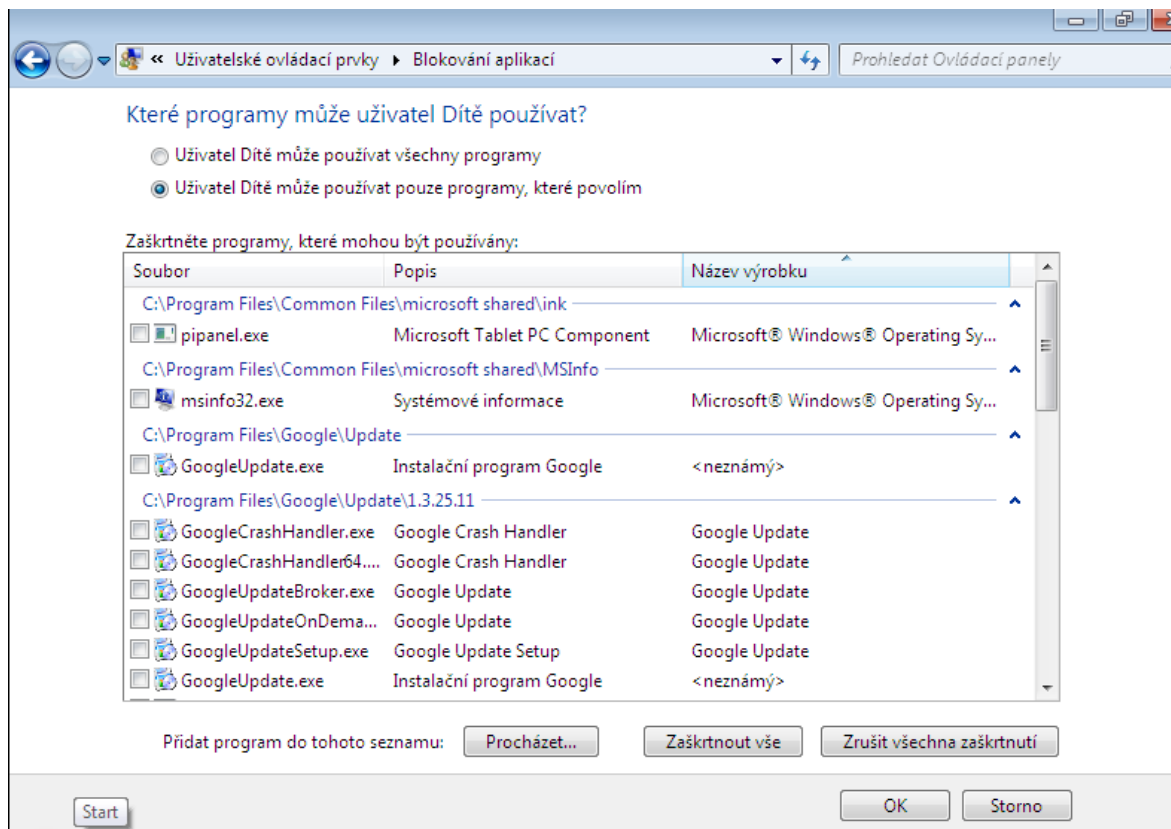
Tobacco Reference	Odkazy a/nebo vyobrazení tabákových výrobků	E10+, T, M
Use of Alcohol	Užívání alkoholických výrobků	E10+, T, M, AO
Use of Drugs	Užívání nelegálních drog	T, M, AO
Use of Tobacco	Užívání tabákových výrobků	T, M, AO
Violence	Scény obsahující agresivní konflikt	Všechny kromě Ec
Violent References	Odkazy na násilné chování	E10+, T,

Pro lepší názornost a hlavně pro porovnání s evropským ratingovým systémem má ESRB ekvivalenty hodnocení. [37]

- Early Childhood (EC) a Everyone (E) se dá přirovnat k PEGI 3
- Everyone 10+ (E10+) se dá přirovnat k PEGI 7
- Teen (T) se dá přirovnat k PEGI 12
- Mature (M) se dá přirovnat k PEGI 16
- Adults Only (AO) se dá přirovnat k PEGI 18

### 6.1.6 Blokování programů

Můžeme povolit programy, které dovolíme dítěti používat. Jednoduchým zatržením určíme, který program dítě bude moci používat, viz Obr 5.



Obr. 8 – Povolení používaných programů.

### 6.1.7 Bezpečné vyhledávání na webu

Jeden s pomocníků jak zabránit dětem chodit na nevhodné stránky může být nastavení bezpečného vyhledávání. Popis níže ukazuje, jak nastavit bezpečné vyhledávání pro prohlížeč Chrome.

Zobrazte si stránku Nastavení Vyhledávání. Poté vyhledejte sekci Filtry Bezpečného vyhledávání. Pokud je zaškrtnuté políčko Filtrovat explicitní výsledky, tak je filtrace obsahu zapnuta, neboli je nastaveno bezpečné vyhledávání. Pro zaznamenání změn, klikněte na tlačítko uložit.[38]

## 6.2 Doplnující software

### 6.2.1 Norton Security (Family)

Norton Security je komplexní řešení zabezpečení ochrany. Tento komplexní balíček obsahuje pokročilé možnosti ochrany a kontroly dětí na Internetu a také na počítači viz Obr 6. Umožňuje dohled nad webem, sociálními sítěmi, nebo také emailovou notifikaci pokud se dítě bude chtít dostat na zablokované stránky. NSF je dostupný i do mobilních telefonů a tabletů se systémy iOS a Android. Byla testována jen základní verze programu. Program lze pořídit ve verzi Premiér, kde je navíc dohled nad polohou, dohled na videem a jiné.

Funkce programu

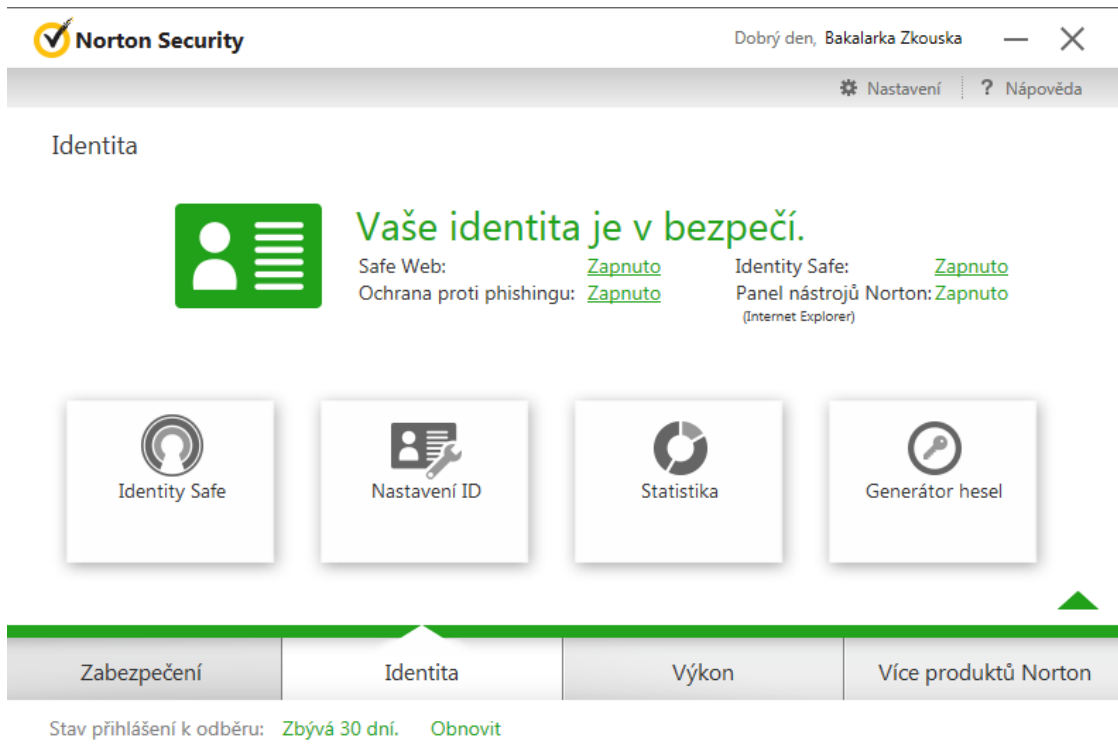
- Kontrola nad webem. Umožňuje rodičům kontrolovat stránky, které navštívilo dítě. Také umožňuje filtraci nevhodných webů tak, aby se na ně dítě nedostalo.
- Dohled nad sociálními sítěmi. Program dokáže poskytnout přehled, jak se dítě přihlašuje do soc. sítí.
- Kontrola nad vyhledáváním. NSF vám umožní zjistit, jaké výrazy hledá vaše dítě.
- Žádost o přístup. Vaše dítě vám může poslat poznámku se žádostí o výjimku pro daný blokový web.
- Individuální nastavení kontroly pro určitý profil.

Výhody

- Velké množství nastavení.
- Nastavení pro každý profil zvlášť.
- Komplexní řešení ochrany dětí na Internetu s nadstandardními možnostmi (žádosti o přístup, kontrola z mobilních zařízení aj.)

Nevýhody

- Program je spíše pro pokročilejší uživatele.
- Cena. V době psaní práce tento software stál 520Kč/rok.



Obr. 9 – Úvodní nabídka NS

Pokud máte nastavené profily, tak máte základní nastavení vytvořeno.

### 6.2.2 Naomi 3.2.90

Program Naomi podle popisu výrobce funguje tak, že ho nainstalujete a program sám podle daného slovníku blokuje nevhodné stránky. Umožňuje blokování P2P sítí. Náhled do programu Naomi nalezneme v Obr. 7.

Funkce programu

- Blokace stránek s nevhodným obsahem
- Blokování P2P

Výhody.

- Na první pohled velmi jednoduchý program.
- Primárně určen na filtraci nevhodného webu.

Nevýhody

- Program byl naposledy aktualizován 3. 4. 2006.
- Nefiltruje úplně ideálně nevhodné weby.
- Nesnadná odinstalace.



Obr. 10 – Rozhraní Naomi.

### 6.2.3 Manic Time

Program Manic Time se dá pořídit ve dvou verzích. Základní verze podporuje sledování činnosti počítače, čas spuštěných aplikací. Program umožňuje ukládání dat do databáze a tvorbu statistik. Program je primárně určen na zpětnou kontrolu.

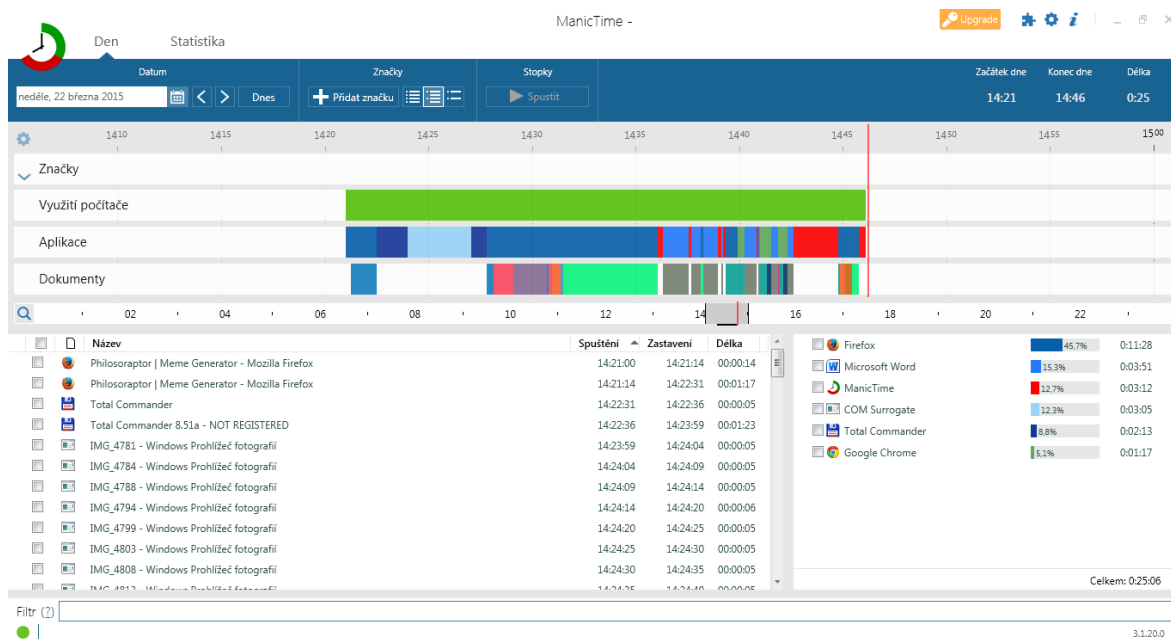
Při prvním spuštění si můžete vybrat 3 verze. Professional na 15 dní. Professional, kde musíte vložit jméno a klíč. Profesionální verze obsahuje navíc serverovou verzi, stopky kde si můžete měřit čas práce a jiné. Obr 8 ukazuje práci programu.

Výhody

- Jednoduchost instalace i programu
- Velké množství nástrojů na kontrolu a sledování dění na počítači.

Nevýhody

- Pouze sledování bez možnosti blokování.



Obr. 11 – Prostředí programu Manic Time.

## 6.2.4 Kurupira – web filter

Kurupira je komplexní balík ochrany dětí na Internetu. Slouží na filtrování nevhodného webu, nastavení času pro práci na počítači nebo také k blokování přístupu k vybraným aplikacím. Tento program je od brazilských vývojářů a je zdarma. Tato verze programu byla vydána 5. října 2014

### Funkce programu

- Filtrování webového obsahu, viz Obr. 9.
  - Stálá blokáce webových stránek dle vnitřní databáze programu (nemusí se dále nastavovat).
  - Filtrování přímo konkrétních adres.
  - Filtrování ve vymezeném čase – umožňuje filtraci stránek jen v předem uvedeném čase.
- Sledování stránek – nastavení, které pouze sleduje navštívené stránky, ale nejsou blokovány. K dispozici je podrobný report a historie.
- Blokování nevhodných programů - blokování aplikací podle zadaných klíčových slov (game, hra, Call of Duty a jiné).
- Blokování sociálních sítí – blokování Skypu, Facebooku, IM, a ostatních sociálních sítí.

- Seznam povolených programů – dle seznamu můžete povolit dětem určité aplikace. Tento způsob závisí na klíčových slovech v seznamu.
- Snímání obrazovky – program umožňuje dělat screenshoty, které program shromažďuje.
- Emailové notifikace – lze nastavit emailovou notifikaci kdykoliv, kdy dítě vyhledá blokovanou stránku anebo kdyby chtělo spustit nevhodný program.
- Změny ochráněny heslem

### Výhody

- Jednoduchý, flexibilní program. – dá se jednoduše nastavit filtrování a blokace.
- Ochrana programu heslem.
- Zdarma.

### Nevýhody

- Program není v češtině.
- Nelze nastavit pro konkrétní uživatelský účet.



Obr. 12 – Nastavení webového filtru u programu Kurupira.

### 6.2.5 K9 Web Protection

K9 Web Protection je program na podporu rodičovské kontroly a filtrování nevhodného obsahu na Internetu, viz Obr 10. Tento program může blokovat více jak 60 kategorií nežádoucího obsahu např. pornografie, násilí, rasismus, nenávisť, hazardní hry, ale také malware a spyware.

Funkce programu

- Program filtruje data na principu commercial-grade filtering, což je kombinace centrální databáze, dynamické kontroly stránky a také ratingové technologie.
- Možnost výběru konkrétních oblastí, které se budou filtrovat.
- Bezpečné vyhledávání ve všech prohlížečích.
- Blokování Internetu v závislosti na čase.
- Real-time prozkoumávání stránek s jejich příslušnou kategorizací.



Obr. 13 – K9 Web Protection úvodní stránka.

Výhody

- Jednoduché komplexní řešení dětské ochrany na Internetu.
- Velmi jednoduché nastavení programu. (Ihned po instalaci program 100% funguje).
- Kvalitní filtrování webů s širokou databází.
- Funguje ve webovém prohlížeči.
- Ochrana i přes spyware a malware.

### Nevýhody

- Není česká podpora.
- Složitá prvotní registrace.
- Pouze ochrana pohybu na Internetu.

### 6.2.6 HostsMan

Program HostsMan (Obr. 11) slouží na jiný typ ochrany. HostsMan je editor souboru Hosts, kde můžete zapisovat adresy blokových domén, případně záznamy o přesměrování na jiný server. Tento způsob ochrany se doporučuje zkušenějším uživatelům.



Obr. 14 – HostsMan.

Program dokáže scanovat. Prohledávat chyby v souboru, nebo odstraňuje duplikáty. Přes HostsMan můžete do souboru Hosts zapisovat i jiné příkazy.

### Výhody

- Velmi jednoduchý program pro zkušenějšího uživatele.
- Efektivní práce se souborem Hosts.

### Nevýhody

- Není česká podpora.
- Umí pouze filtrování přes IP adresy domén.
- Určen hlavně zkušenějším uživatelům.

## 6.3 Shrnutí testování doplňujících programů

Programy na filtrování nevhodného obsahu nebo na monitoring počítače jsou na Internetu velmi dostupné, avšak velké procento z nich jsou placené programy. V bakalářské práci bylo primárně zaměřeno na programy, které jsou zdarma kvůli jejich dostupnosti.

V této oblasti softwarové ochrany hodně závisí na stáří daného produktu. Z testovaných programů nemohu doporučit program Naomi. U programu Naomi, který má poslední aktualizaci z roku 2006, byly zjištěny vážné chyby ve filtrování nevhodného obsahu. Naopak program Kurupira se osvědčil jako kvalitní program na blokaci nevhodných aplikací a webových stránek. Pro pokročilejší a náročnější uživatele bych doporučoval program Norton Security, který je ale zpoplatněn.

## 6.4 Webové prohlížeče

S rodičovskou kontrolou se můžete setkat i na úrovni prohlížečů. Byly vybrány čtyři nejznámější prohlížeče, které lidé v České Republice nejvíce používají. Google Chrome, Mozilla Firefox, Opera a Internet Explorer. Bylo vycházeno z výzkumů společnosti StatCounter za období březen 2014 – březen 2015 [1]

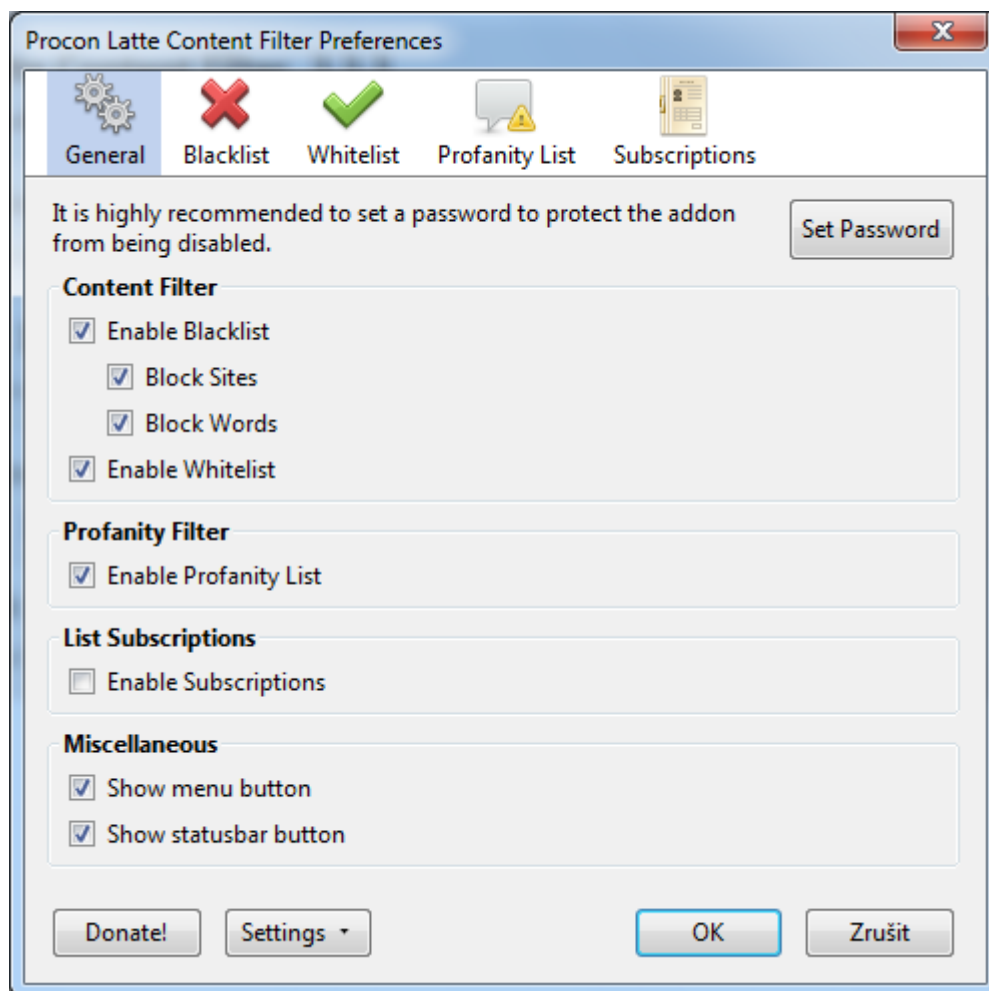
U tohoto řešení je výhodou, že nepotřebuje být doinstalován do počítače další software, ale přímo do prohlížeče se naimplementuje doplněk, který tuto ochranu řeší.

Níže budou konkrétně rozebrány webové prohlížeče a jejich možnosti ochrany, které byly zkoumány v dubnu 2015. Díky rychlému vývoji těchto doplňků, je možné najít i novější verze doplňků i samotných prohlížečů.

### 6.4.1 Mozilla Firefox 37.0.1

Prohlížeč Mozilla podporuje 17 doplňků (na jaře 2015), které se zabývají ochranou dětí na webu. Byly vybrány tři nepoužívanější doplňky podle počtu uživatelů, kteří je používají.

- BlockSite – tento doplněk automaticky blokuje nevhodné stránky dle zadaných domén. Tento doplněk blokuje i hypertextové odkazy na tyto stránky. Tento doplněk využívá k 9. 4. 2015 203 900 uživatelů.
- CensureBlock 0.45 – blokuje nevhodné weby. Byly testovány weby typu pornhub.cz, navratdoreality.cz, kaotic.com. Weby, které přímo nejsou zaměřeny na porno a násilí, ale přesto se na těchto webech mohou objevit nevhodné obrázky, filtr nezachytí. Tento problém byl zachycen u stránky amk.to. Tento doplněk využívá 87 847 uživatelů.
- Procon Latte Content Filter – program funguje na bázi filtrování dle klíčových slov (Obr. 12). Podobně jako CensureBlock, není 100% zaručena ochrana. Domény jako jsou rozzlobenimuzi.com a nebo navratdoreality.cz bez problému fungují.

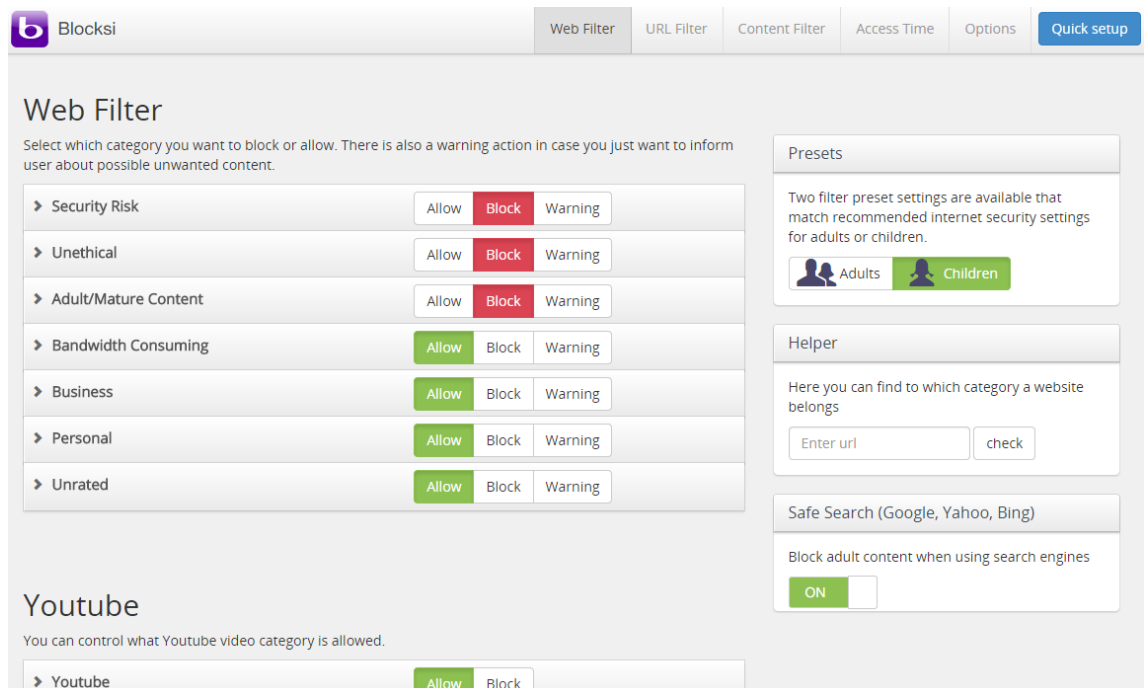


Obr. 15 – Procon Latte Content Filter.

#### 6.4.2 Opera 28.0

Prohlížeč Opera využívá jádro jako např. Chrome, proto doplňky jsou velmi podobné.

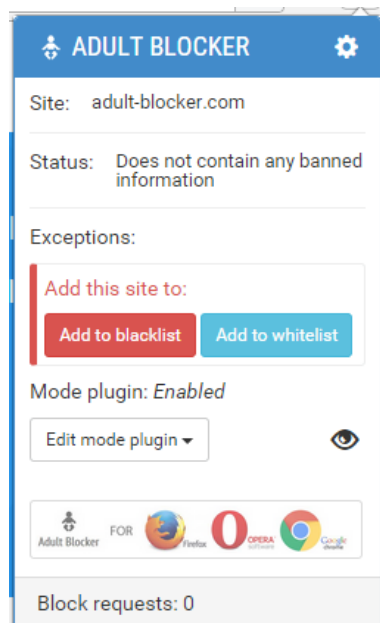
Blocksi – doplněk do Opery, který blokuje stránky s nevhodným obsahem (Obr. 13). Tento doplněk je chráněn administrátorským heslem. Poslední aktualizace proběhla 19.1.2015 pro Operu.



Obr. 16 – Doplněk Opery Blocks!

Opera, ale také i Chrome a Firefox funguje na principu jako již výše zmiňované doplňky. Poslední aktualizace proběhla 16. března 2015.

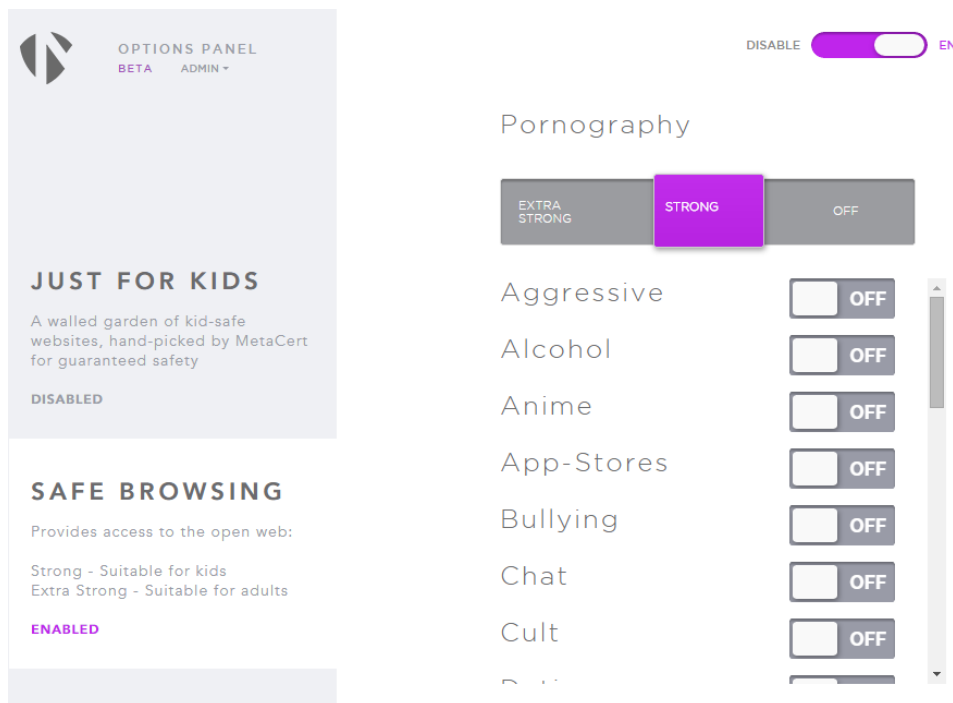
Dalším doplňkem do Opery je Adult Blocker (Obr. 14), výhodou tohoto doplňku je, že se dá použít do FireFoxu, Opery a Chromu.



Obr. 17 – Adult Blocker

### 6.4.3 Google Chrome 41.0.2272.118 m

MetaCert – doplněk do Chromu. Zde si můžeme volit i sílu ochrany, viz Obr. 15.



Obr. 18 – MetaCert.

Blocksi – tento doplněk je možné si nainstalovat v Opeře. Doplněk také filtruje výsledky vyhledávání na Googlu.

### 6.4.4 Internet Explorer 11

Pro uživatele IE11 by mohlo být pro méně zkušeného uživatele těžké, protože pro nastavení rodičovské kontroly přímo v IE11 musíme v systému povolit záložku s názvem Poradce při hodnocení obsahu. Následně můžete na jednotlivá rizika dát různou prioritu. Například násilí, aby nebylo eliminováno, jen sledováno.

### 6.4.5 AdBlock

AdBlock je jednoduchý doplněk, který také ochrání děti před nechtěnými vlivy Internetu. Tento doplněk aktivně blokuje reklamy, které mohou propagovat nevyžádaný obsah, například násilné hry, erotické doplňky nebo půjčky.

#### **6.4.6 Tablety, smartphony a aplikace v nich.**

V době smartphonů a tabletů je dobré dbát i na ochranu dětí při používání chytrých zařízení. Díky moderním technologiím můžeme používat filtrovací doplňky typu Blocksi aj. i na tabletech a chytrých telefonech.

Dalším problémem mohou být placené aplikace. Pokud si uložíte heslo do zařízení, tak dítě může nakoupit aplikace i za několik desítek tisíc korun. Pokud Vaše dítě hraje na tabletu hry, tak si dejte pozor, jestli si ve hře nekupuje doplňky, které jsou placeny z vašeho účtu.

#### **6.4.7 Shrnutí**

Doporučuji používat jeden z prohlížečů Chrome, Firefox, Opera, protože ochranu mají postavenou na velmi jednoduchém a účinném principu doplňků do prohlížeče. Tyto doplňky jsou často aktualizovány, proto riziko nefunkčnosti ochrany se snižuje. Po srovnání doplňků jsem zjistil, že všechny jsou kvalitní a v konečném důsledku vybraný doplněk nerozhoduje. Záleží čistě na uživateli, který doplněk mu nejvíce vyhovuje. Výhodou je, že některé doplňky jsou podobné jak pro Chrome, tak i pro Firefox, proto není třeba používat jiný prohlížeč jen kvůli doplňkům.

## ZÁVĚR

Po zpracování této práce jsem došel k závěru, že lidé o hrozbách na Internetu vědí, ale stále mají mezery v určitých tématech. Například co se týče sociálních sítí, nevěděli podmínky vstupu dětí na soc. sítě.

Z dotazníku také vyplývá, že lidé chtějí více preventivních opatření. Ve školách více hodin zaměřených na hrozby na Internetu a ochranu dětí, ale také i setkání nebo besedy s externími pracovníky.

V dnešní době je velký rozmach sociálních sítí, které nejen rodiče, ale také jejich děti používají ke komunikaci, ke sdílení fotografií a videí. Zdá se, že Instant Messanging je na ústupu a vše se integruje do jednoho místa.

Hodně dětí hraje hry. V tomto ohledu mohou rodičům pomoci ratingové společnosti, jako je například PEGI, které hry označují štítky. Rodiče tedy ví, pro koho je daná hra určena a s jakými hrozbami se může dítě setkat.

V praktické části bylo popsáno jak konkrétně eliminovat hrozby pomocí zabezpečení, které je přímo implementováno v operačním systému. Následně jako doplněk byly vybrány programy na ochranu dětí na Internetu. Programů, které mají chránit děti na Internetu je mnoho, avšak dost z nich je placených a některé z důvodu ukončené podpory také nefunkčních. Z této skupiny byl vybrán jeden zástupce - Norton Security. Za cenu 520 Kč (na jaře 2015) si koupíte velmi komplexní nástroj na ochranu dětí. Existují i volné verze na filtrování obsahu na Internetu nebo omezení času na počítači. Výhodou těchto programů je, že filtrují nejen činnost na Internetu, ale také můžeme omezit spuštěné programy, tak jako to umožňuje program Kurupira.

Dalším nástrojem ochrany je přidání ochranného doplňku do webového prohlížeče. Výhodou u tohoto řešení je, že jsou velmi časté aktualizace těchto doplňků. Do počítače nemusíte instalovat další software, ale blokuje a filtruje pouze činnost na Internetu.

Závěrem bych chtěl podotknout, že ať máte nejmodernější zabezpečení počítače nebo nedovolujete svým dětem používat počítač, tak nejlepší a nejúčinnější ochranou dětí je komunikace s dětmi o jejich hrozbách, což je součástí prevence.

**SEZNAM POUŽITÉ LITERATURY**

- [1] Joseph Carl Robnett Licklider. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/Joseph\\_Carl\\_Robnett\\_Licklider](http://cs.wikipedia.org/wiki/Joseph_Carl_Robnett_Licklider)
- [2] ČERNÁ, Zuzana a Michal ČERNÝ. 2012. Historie Internetu. *Historie Internetu* [online]. [cit. 2015-05-14]. Dostupné z: <http://clanky.rvp.cz/clanek/c/o/14791/HISTORIE-INTERNETU.html/>
- [3] DARPA. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: <http://cs.wikipedia.org/wiki/DARPA>
- [4] PETERKA, Jiří. 2011. Na počátku byl ARPANET .. In: *Na počátku byl ARPANET ..* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.earchiv.cz/a95/a504c502.php3>
- [5] CHLAD, Radim. Historie Internetu v České republice. *Historie Internetu v České republice* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm>
- [6] Služba World Wide Web. 2010. In: *Služba World Wide Web* [online]. [cit. 2015-05-14]. Dostupné z: [https://moodle.sspbrno.cz/pluginfile.php/2241/mod\\_resource/content/0/www.pdf](https://moodle.sspbrno.cz/pluginfile.php/2241/mod_resource/content/0/www.pdf)
- [7] World Wide Web Consortium. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/World\\_Wide\\_Web\\_Consortium](http://cs.wikipedia.org/wiki/World_Wide_Web_Consortium)
- [8] Tim Berners-Lee. 2015. *Tim Berners-Lee* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.w3.org/People/Berners-Lee/>
- [9] Web 2.0: bublina, nebo nový směr webu. 2007. In: *Web 2.0: bublina, nebo nový směr webu?* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.lupa.cz/clanky/web-2-0-bublina-nebo-novy-smer-webu/>
- [10] Web 1.0. 2015. In: *Web 1.0* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.techopedia.com/definition/27960/web-10>

- [11] SINGEL, Ryan. 2015. Are You Ready for Web 2.0? In: *Are You Ready for Web 2.0?* [online]. [cit. 2015-05-14]. Dostupné z: <http://archive.wired.com/science/discoveries/news/2005/10/69114>
- [12] Web 2.0. 2010. *Web 2.0* [online]. [cit. 2015-05-14]. Dostupné z: [http://wiki.rvp.cz/Knihovna/1.Pedagogicky\\_lexikon/W/Web\\_2.0](http://wiki.rvp.cz/Knihovna/1.Pedagogicky_lexikon/W/Web_2.0)
- [13] Web 3.0. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/Web\\_3.0](http://cs.wikipedia.org/wiki/Web_3.0)
- [14] KASÍK, Pavel. 2008. Web 3.0 vám bude rozumět, Web 4.0 se s vámi bude dohadovat. *Web 3.0 vám bude rozumět, Web 4.0 se s vámi bude dohadovat* [online]. [cit. 2015-05-14]. Dostupné z: <http://1url.cz/YXCy>
- [15] KEJDUŠ, Radek. 2012. Stručná historie emailu: už 40 let si posíláme počítačové dopisy. *Stručná historie emailu: už 40 let si posíláme počítačové dopisy* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.cnews.cz/clanky/strucna-historie-emailu-uz-40-let-si-posilame-pocitacove-dopisy>
- [16] Historie e-mailu – od kosmonautů po současnost. 2013. *Historie e-mailu – od kosmonautů po současnost* [online]. [cit. 2015-05-14]. Dostupné z: <http://computerworld.cz/Internet-a-komunikace/historie-e-mailu-od-kosmonautu-po-soucasnost-49996>
- [17] Instant messaging. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/Instant\\_messaging](http://cs.wikipedia.org/wiki/Instant_messaging)
- [18] 7 tipů pro ochranu před viry na ICQ. 2010. *7 tipů pro ochranu před viry na ICQ* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.novinky.cz/Internet-a-pc/bezpecnost/219899-7-tipu-pro-ochranu-pred-viry-na-icq.html>
- [19] Sociální sítě. 2014. *Sociální sítě* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.jaknainternat.cz/page/1751/socialni-site/>
- [20] Rizika sociálních sítí. *Rizika sociálních sítí* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.bezpecnyInternet.cz/zacatecnik/socialni-site/rizika.aspx>
- [21] Nebezpečné komunikační praktiky: Co je kyberšikana? 2009. *Nebezpečné komunikační praktiky: Co je kyberšikana?* [online]. [cit. 2015-05-14]. Dostupné z: <http://cms.e-bezpeci.cz/content/view/14/39/lang,czech/>

- [22] BYSTRONĚ, Marcel. 2009. Kyberšikana zabíjí!. *Kyberšikana zabíjí!* [online]. [cit. 2015-05-14]. Dostupné z: <http://bystron.blog.idnes.cz/c/64160/Kybersikana-zabiji.html>
- [23] KOPECKÝ, Kamil. 2010. *STALKING A KYBERSTALKING NEBEZPEČNÉ PRONÁSLEDOVÁNÍ*. Olomouc. ISBN 978-80-254-7737-3. Dostupné také z: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu>. Studie. Univerzita Palackého.
- [24] Nebezpečné komunikační praktiky: Kybergrooming. 2008. *Nebezpečné komunikační praktiky: Kybergrooming* [online]. [cit. 2015-05-14]. Dostupné z: <http://cms.e-bezpeci.cz/content/view/42/35/lang,czech/>
- [25] Co je to kybergrooming? *Co je to kybergrooming?* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybergrooming.html>
- [26] Případy kybergroomingu I. 2009. *Případy kybergroomingu I.* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.e-bezpeci.cz/index.php/temata/kybergrooming/33-112>
- [27] CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE. 2013. *Sexting: Co je sexting?* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.sexting.cz/>
- [28] BRECHLEROVÁ, Dagmar. 2007. Sociální inženýrství. *Sociální inženýrství* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.systemonline.cz/it-security/socialni-inzenyrstvi.htm>
- [29] PALATINUS, Lukáš. 2014. Počítačové útoky: Sociotechnika. *Počítačové útoky: Sociotechnika* [online]. [cit. 2015-05-14]. Dostupné z: <http://blog.banan.cz/Internet/Pocitacove-utoky-Sociotechnika>
- [30] Phishing a pharming. *Phishing a pharming* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.bezpecnyInternet.cz/pokrocily/Internetove-bankovnictvi/phishing-a-pharming.aspx>
- [31] Co je to hoax? 2015. *Co je to hoax?* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.hoax.cz/hoax/co-je-to-hoax>

- [32] Čím hoax škodí? 2015. *Čím hoax škodí?* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.hoax.cz/hoax/cim-hoax-skodi>
- [33] ŠÍBLOVÁ, Jaroslava. 2007. Paragraf 11/55. *Paragraf 11/55*: [online]. (15) [cit. 2015-05-14]. Dostupné z: <http://www.ucitelskenoviny.cz/?archiv&clanek=337&PHPSESSID=0f25f5ca140cecb2f5e2a53fa17d088d>
- [34] Historie: Historie Aliance Zákon 18. *Historie: Historie Aliance Zákon 18* [online]. [cit. 2015-05-14]. Dostupné z: <http://www.aliance18.cz/historie/>
- [35] STATCOUNTER. *StatCounter: GlobalStat* [online]. 1999-2015 © [cit. 2015-04-08]. Dostupné z: <http://gs.statcounter.com/#all-browser-CZ-monthly-201403-201503-bar>
- [36] Pan European Game Information. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/Pan\\_European\\_Game\\_Information](http://cs.wikipedia.org/wiki/Pan_European_Game_Information)
- [37] Entertainment Software Rating Board. 2015. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2015-05-14]. Dostupné z: [http://cs.wikipedia.org/wiki/Entertainment\\_Software\\_Rating\\_Board](http://cs.wikipedia.org/wiki/Entertainment_Software_Rating_Board)
- [38] Zapnutí nebo vypnutí Bezpečného vyhledávání. 2015. *Zapnutí nebo vypnutí Bezpečného vyhledávání* [online]. [cit. 2015-05-14]. Dostupné z: <https://support.google.com/websearch/answer/510?hl=cs&rd=1>

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IM	Instant Messanging
NS	Norton Security
NFS	Norton Family Security

**SEZNAM OBRÁZKŮ**

Obr. 1 – Prostředí Skype.....	17
Obr. 2 – Úvodní stránka soc. sítě Facebook .....	18
Obr. 3 – Portál superhry.cz .....	23
Obr. 4 – Vytvoření standardního uživatelského účtu. ....	47
Obr. 5 – Nastavení rodičovské kontroly. ....	48
Obr. 6 – Nastavení časového limitu.....	48
Obr. 7 – Nastavení typů her, které může dítě hrát. ....	50
Obr. 8 – Povolení používaných programů. ....	53
Obr. 9 – Úvodní nabídka NS .....	55
Obr. 10 – Rozhraní Naomi.....	56
Obr. 11 – Prostředí programu Manic Time.....	57
Obr. 12 – Nastavení webového filtru u programu Kurupira. ....	58
Obr. 13 – K9 Web Protection úvodní stránka.....	59
Obr. 14 – HostsMan.....	60
Obr. 15 – Procon Latte Content Filter. ....	62
Obr. 16 – Doplněk Operry Blocksí. ....	63
Obr. 17 – Adult Blocker .....	63
Obr. 18 – MetaCert. ....	64

**SEZNAM TABULEK**

Tab. 1 – Srovnání Web 1.0 a Web 2.0. [9] .....	13
Tab. 2 – Pohlaví respondentů. ....	25
Tab. 3 – Tabulka věku respondentů. ....	26
Tab. 4 – Nejvyšší vzdělání.....	26
Tab. 5 – Tabulka o povědomí sociálních sítí. ....	27
Tab. 6 – Tabulka kolik respondentů využívá.....	28
Tab. 7 – Přehled soc. sítí, které respondenti využívají. ....	28
Tab. 8 – Věk dětí.....	29
Tab. 9 – Dovolujete pracovat.....	30
Tab. 10 – Tabulka doplňujících odpovědí k otázce č. 9. ....	30
Tab. 11 – Tabulka počtu hodin, které dítě tráví na počítači. ....	31
Tab. 12 – Tabulka činností dětí na počítači. ....	32
Tab. 13 – Tabulka komunikace dětí na Internetu. ....	33
Tab. 14 – Tabulka profilu .....	34
Tab. 15 – Tabulka opatření, aby se děti mohly pohybovat bezpečně na Internetu.....	34
Tab. 16 – Tabulka největších hrozeb Internetu dle respondentů. ....	36
Tab. 17 – Tabulka navrhovaných řešení hrozeb na Internetu dle respondentů. ....	37
Tab. 18 – Tabulka věkové hranice pro registraci na Facebook a Twitter.....	38
Tab. 19 – Tabulka postoj k sociálním sítím.....	38
Tab. 20 – Tabulka dostačující.....	39
Tab. 21 – Tabulka návrhů od respondentů na zlepšení osvěty. ....	40
Tab. 22 – Druhy obsahu dle ESRB[37]. ....	51

**SEZNAM GRAFŮ**

Graf 1 – Pohlaví respondenta.....	25
Graf 2 – Graf věku respondenta.....	26
Graf 3 – Graf vzdělání respondentů.....	26
Graf 4 – Graf povědomí o sociálních sítích.....	27
Graf 5 – Přehled sociálních sítí, které využívají respondenti.....	28
Graf 7 – Kolik respondentů má dítě.....	29
Graf 8 – Graf počtu hodin, které tráví děti na počítači.....	31
Graf 9 – Graf činností dětí na počítači.....	32
Graf 10 – Graf komunikace dětí na Internetu.....	33
Graf 11 – Graf největších hrozeb na Internetu dle respondentů.....	35
Graf 12 – Graf navrhovaných řešení hrozeb na Internetu dle respondentů.....	37
Graf 13 – Graf postoje k sociálním sítím.....	38
Graf 14 – Graf návrhu řešení osvěty.....	40

## SEZNAM PŘÍLOH

P1 – Dotazník k bakalářské práci

## **PŘÍLOHA P I: DOTAZNÍK K BAKALÁŘSKÉ PRÁCI**

1. Vaše pohlaví?
  - a. žena
  - b. muž
  
2. Váš věk?
  - a. 15-20
  - b. 20-40
  - c. 40-60
  - d. 60 +
  
3. Nejvyšší dosažené vzdělání
  - a. střední
  - b. střední s maturitou
  - c. vysokoškolské
  
4. Máte děti
  - a. ano
  - b. ne
  
5. Co si představíte pod pojmem sociální sítě?
  - a. (kolonka pro vyplnění)
  
6. Využíváte sociální sítě?
  - a. ano
  - b. ne
  
7. Jaké?
  - a. Facebook
  - b. Twitter
  - c. LinkedIn
  - d. Badoo
  - e. YouTube

- f. Lidé
- g. jiné (jaké?)

8. Věk vašich dětí

- a. 0-6
- b. 6-10
- c. 10-15
- d. 15-18

9. Dovolujete vašemu dítěti pracovat na počítači?

- a. ano
- b. ne

10. Kolik hodin tráví vaše děti na počítači?

- a. 0-2

11. „Když ne“ -> Proč?

- a. důvod 1
- b. důvod 2

12. Co je podle Vás největší hrozba na internetu pro děti?

- a. (kolonka pro vyplnění)

13. Jak byste tuto hrozbu řešili?

- a. (kolonka pro vyplnění)

14. Co Vaše děti dělají na počítači?

- a. hrají hry (akční)
- b. hrají hry (logické nebo strategie)
- c. Vzdělávají se (věci do školy, vzdělávací programy, videa, dokumenty)
- d. brouzdají po internetu
- e. jiné

15. Víte, jak vaše dítě komunikuje na internetu?

- a. IM

- b. síť
- c. mail

16. Má Vaše dítě účet na sociální síti?

- a. ano
- b. ne

17. Od kolika let může být dítě zaregistrováno na Facebooku či Twitteru?

- a. možnosti
- b. ne

18. Jaký máte postoj k sociálním sítím?

- a. pozitivní
- b. spíše pozitivní
- c. neutrální
- d. spíše negativní
- e. negativní

19. Co děláte pro vzdělávání Vašich dětí, aby se mohli bezpečně pohybovat na internetu

- a. Mluvím s nimi o hrozbách (stalking, kyberšikana, pedofilové...)
- b. Spoléhám na to, co se dozví ve škole
- c. Nic
- d. Jiné

20. Myslíte, že osvěta v dnešní době je dostačující?

- a. ano
- b. ne

21. (Pokud ne!) Co byste udělal/a nebo zavedl/a, aby osvěta byla dostačující?

Zkuste popsat, co by podle Vás bylo dostačující, aby děti si uvědomovali hrozby internetu. Např. Více hodin ve školách zaměřených na toto téma, Semináře pro širokou veřejnost atd.

- a. (text)