Univerzita Pardubice

Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Návrh zabezpečení pro ochranu dětí před nebezpečným obsahem internetu

Hana Vrzalová

Diplomová práce
2013

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Hana Vrzalová**
Osobní číslo:	**E110154**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Název tématu:	**Návrh zabezpečení pro ochranu dětí před nebezpečným obsahem internetu**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Definice nebezpečného obsahu internetu, definice vybrané věkové skupiny.
Popis stávající situace ochrany dětí. Organizace a instituce působící v oblasti bezpečnosti dětí na internetu.
Monitoring nabízených SW produktů pro zabezpečení přístupu na nevhodné www stránky.
Testování produktů pro ochranu dětí před nebezpečným obsahem internetu.
Návrh vlastního řešení vycházejícího z testování produktů.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 55 stran**

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

Seznam odborné literatury:

KOPECKÝ, K. Kybergrooming: Nebezpečí kyberprostoru [online]. Olomouc: NET UNIVERSITY, 2010 [cit. 2012-05-05]. Kybergrooming? pozor na internetové uživatele, 16 s. Dostupný z WWW: http://www.e-nebezpeci.cz/index.php/ke-stazeni/category/4-materialy-pro-studium?download=5%3Akybergrooming-studie. ISBN 978-80-254-7573-7.

KOPECKÝ, K. Moderní trendy v e-komunikaci. Olomouc: Hanex, 2007, 98 s. ISBN 978-808-5783-780.

LIVINGSTONE, S., HADDON, L. Kids online: opportunities and risks for children. Portland, OR: Policy Press, 2009, 272 s. ISBN 978-184-7424-389.

SMITH, G., S. How to protect your children on the Internet: a roadmap for parents and teachers. Westport, Conn.: Praeger, 2007, 193 s. ISBN 02-759-9472-4.

ŠMAHEL, D. Psychologie a internet: děti dospělými, dospělí dětmi. Praha: Triton, 2003, 158 s. Psychologická setkávání, sv. 6. ISBN 80-725-4360-1.

Vedoucí diplomové práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **3. října 2012**

Termín odevzdání diplomové práce: **30. dubna 2013**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 3. října 2012

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 1. 8. 2013 Hana Vrzalová

PODĚKOVÁNÍ:

Tímto bych velice ráda poděkovala své vedoucímu práce, paní doktorce Renatě Máchové, za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování diplomové práce. Také bych chtěla poděkovat svým blízkým za trpělivost a pochopení.

ANOTACE

Tato práce pojednává o každodenních nebezpečích, která číhají v Internetu, zejména nebezpečích pro děti, jimž se stal Internet téměř každodenním společníkem. Práce může sloužit jako rady nebo doporučení rodičům, jakým způsobem mohou ochránit své děti v prostředí Internetu. Přináší přehled produktů pro filtrování webových stránek s různou možností integrace v rámci platformy PC, ale také produkty dostupné pro dnes často využívané zařízení typu smartphone. V další části se práce věnuje testování vybraných produktů a výběru vhodného produktu pro navržení zlepšení ochrany dětí na Internetu při použití vybraného produktu.

KLÍČOVÁ SLOVA

nebezpečný obsah Internetu, kyberšikana, sociální inženýrství, ochrana před nebezpečným obsahem, filtrování webových stránek, PC, smartphone, rodičovský ochrana

TITLE

Design of security to protect children from harmful content online

ANNOTATION

This work deals with the everyday dangers that lurk on the Internet, in particular dangers for children, for which became the Internet almost everyday companion. The work can serve as advice or recommendation to parents how they can protect their children on the Internet. Provides an overview of products for filtering websites with different integration options at the PC platform, but also products available today often used for a Smartphone. The next part deals with the testing of selected products and selecting the right product for designing improved child protection on the Internet using the selected product.

KEYWORDS

dangerous, harmful Internet content, cyberbullying, social engineering, protection from harmful content, web filtering, PC, smartphone, parental control

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

COOPA	Children's Online Privacy Protection Act
CSS	Cascading Style Sheets
ČSN	Česká Technická Norma
ČR	Česká republika
DNS	Domain Name System
EU	Evropská unie
GPS	Global Positioning System
HTML	HyperText Markup Language
ICQ	I Seek You
IEC	International Electrotechnical Commission
IM	Instant messaging
IP	Internet Protocol
ISO	International Organization for Standardization
MPL	Mozilla Public License
MS	Microsoft
NCBI	Národní centrum bezpečnějšího internetu
OS	Operační Systém
PC	Personal Computer
Sb.	Sbírka zákonů
SSL	Secure Sockets Layer
Wi-fi	Wireless Fidelity
WCDMA	Wideband Code Division Multiple Access

ÚVOD

Internet je v dnešní době téměř všudy přítomný. Díky různým zařízením si můžete své oblíbené webové stránky prohlédnout kdykoliv, elektronickou poštu stáhnout kdekoliv nebo chatovat s kýmkoliv. O Internetu je možné tvrdit, že je dobrý sluha, ale špatný pán. Přináší mnoho důležitých a zajímavých informací, můžeme ho vidět, jako prvek zábavy, zdroj informací nebo komunikační kanál. Zároveň ale také přináší rizika spojená s možností anonymního nebo pseudonymního vystupování na Internetu. Toto riziko se zejména týká těch, kteří jsou snadno ovlivnitelní a kteří se s takovým nebezpečím nejsou schopni vyrovnat, tedy zejména dětí

Cílem této práce je navrhnout zabezpečení pro ochranu dětí před nebezpečným obsahem Internetu. Abych dosáhla tohoto cíle, definuji ohroženou věkovou skupinu dětí a také nebezpečný obsah Internetu, který může děti ohrožovat. Zabývat se budu také současnou situací ochrany dětí a organizacemi působícími v této oblasti. Provedu monitoring dostupných produktů pro zabezpečení přístupu na nevhodné www stránky. Další část práce bude věnována testování produktů pro ochranu dětí před nebezpečným obsahem Internetu. Z testování pomocí vhodných metod vyberu produkt, pro který navrhnu zlepšení zabezpečení ochrany dětí.

Zabezpečení se bude týkat softwarových nástrojů, které mají za úkol filtrovat nebo blokovat webové stránky s nevhodným obsahem, zabezpečit komunikaci prostřednictvím Internetu nebo monitorovat činnosti dětí na Internetu.

1 VYMEZENÍ PROBLEMATIKY

Dříve než mohu přistoupit k monitoringu produktů pro ochranu dětí na Internetu a návrhu zlepšení takového produktu, musím definovat, koho a před čím bude daný produkt chránit. Definice ohrožené skupiny je důležitá zejména z toho důvodu, že s věkem zpravidla rostou znalosti a dovednosti. Pokud by ohrožená skupina nebyla stanovena, je možné, že pro ochranu bude vybrán produkt, který není vhodný pro danou skupinu, například může být méně zabezpečen a jeho prolomení pro děti nebude problém.

Další definicí v této kapitole je definice nebezpečného obsahu Internetu. Je důležité znát, před čím vlastně chceme děti chránit. Stejně tak jako v případě opomenutí definice ohrožené skupiny je možné, že pro ochranu dětí bude vybrán produkt, který nebude dostatečně nebo vůbec chránit děti v prostředí Internetu.

1.1 Definice ohrožené skupiny

Nebezpečím číhajícím v prostředí Internetu jsou ohroženi prakticky všichni jeho uživatelé. Na rozdíl od dospělých uživatelů jsou děti ohroženy zejména díky nedostatku životních zkušeností. Nebezpečí pro dětské uživatele je tedy jejich naivita a neznalost nebo neschopnost odhadu důsledků, které mohou nastat, setkají-li se s, pro ně, nevhodným obsahem.

Tato práce se zabývá návrhem ochrany dětských uživatelů, před nebezpečným obsahem Internet, které je možné rozdělit dle etapy psychického a fyzického vývoje na několik skupin: Prenatální období, novorozenecké období, kojenecké období, batolecí věk, věk hry – předškolní období, školní věk. Tato období jsou obdobími dětství.[84] Ze zde uvedených skupin je zřejmé, že v prostředí Internetu jsou nejohroženější dětští uživatelé školního věku. V této vývojové etapě totiž nejčastěji přicházejí do styku s Internetem, ať už ve škole, doma, u kamarádů nebo na veřejně přístupných Wi-fi[1] sítích.

Skupinu uživatelů školního věku je možné dále rozdělit na podskupiny, a to na: raný školní věk, střední školní věk a starší školní věk. Všechna tato období pokrývají věk dítěte od 6 až do 15 let života.[84]

Další odborná literatura uvádí rozdělení školního věku na mladší školní období a starší školní věk. Starší školní věk je také často označován jako období pubescence, zpravidla se jedná o 10-11 až 15-16 rok života.[42]

[1] Wi-fi - Wireless Fidelity, bezdrátová síť. [6]

V tomto období skupina dětí školního věku (dále jen děti) sbírá zkušenosti, poznává, učí se chodu vnějšího světa. Je tedy zřejmé, že tyto děti mají málo zkušeností, aby se dokázaly vyrovnat s číhajícím nebezpečím v prostředí internetu. Na rozdíl od uživatelů raného školního věku, případně mladšího školního období, tyto děti vědí, že Internet může skrývat určitá nebezpečí, také vědí co je dobré a co špatné, ale přesto sami často dobrovolně riskují. Proto je důležité děti proti tomuto nebezpečí chránit. Ze stejného důvodu jsem tuto skupinu vybrala jako ohroženou skupinu dětí, kterou by měl před nebezpečným obsahem chránit sofistikovaný softwarový produkt. Zda děti tato rizika budou či nebudou ignorovat je do jisté míry závislé na rodičích a výchově. Rodinné zázemí, rodinná pohoda je svým způsobem nejdůležitějším faktorem při ochraně dětí před nevhodným obsahem internetu.

1.2 Nebezpečný obsah internetu

Nebezpečí představují různé druhy ohrožení od různých druhů útočníků. Některé z těchto nebezpečí mají přímý dopad na děti, některé se také přímo dotýkají rodiny a ostatních uživatelů.

Nebezpečný obsah internetu z hlediska nebezpečí představujícího pro vybranou věkovou skupinu dětí jsou dle projektu EU Kids Online II zejména tato rizika[44]:

- zneužití informací,
- vystavení obsahu s násilím,
- setkávání se s cizími lidmi on-line a následně off-line,
- vystavení obsahu se sexuálním podtextem.

1.2.1 Zneužití informací

Zneužití informací je právě jedním z nebezpečí, které se přímo dotýká jak dětí, tak i jejich okolí. Metody, jejichž cílem je získat a po té zneužít informace se nazývají sociotechnika nebo sociální inženýrství. Podle autora tohoto termínu Kevina Mitnicka je sociotechnika definována takto [48]:

„Sociotechnika je ovlivňování a přesvědčovaní lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využit lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.“

Tuto definici je možné uplatnit na jakékoliv komunikační kanály a na jakékoliv příjemce v komunikačních kanálech. Ve vztahu k dětem se může jednat o zneužití jejich důvěry za účelem vylákání důvěrných informací o dětech, rodičích nebo o prostředí kde žijí.

Sociotechnikem v tomto pohledu může být například i zloděj nebo online-predátor, který se snaží získat důvěru dítěte a přimět jej tak, aby mu sdělilo potřebné informace pro svůj „plán“.

1.2.2 Vystavení obsahu s násilím

Vystavení dětí obsahu s násilným se může jak přímo dotýkat dítěte, tak se může jednat i o druhotné setkání, tedy v případě, kdy dítě je pouze svědkem násilí na třetí osobě nebo osobách.

Velmi častým případem, kdy je dítě vystaveno násilí, ať už z důvodu rasové nesnášenlivosti, nebo jen z rozmaru agresora v prostředí Internetu je šikana online, tedy tzv. Kyberšikana.

Kyberšikana

Kyberšikana, je termín který pochází z anglického slova *cyberbullying*. SAMEER a W. PATCHIN v článku Journal of School Violence, kyberšikanu popisují jako úmyslné, opakující se působení újmy, nebo ublížení prostřednictvím elektronického textu.[31] Dnes se takové chování nevtahuje pouze na elektronický text, ale také na další komunikační prostředky jako jsou fotografie, videa, nebo hlasový přenos, případně jiné techniky využívající informační technologie. Jiná literatura kyberšikanu popisuje jako formu emocionální šikany, jejímž cílem je způsobit pocit strachu, izolace a ponížení. Přičemž jako nástroj kyberšikany je používán Internet nebo jiné digitální zařízení. [7]

Šikana je jev, ke kterému, zejména na základní škole, dochází bohužel velice často. Kyberšikana pak může být doprovodným jevem šikany jako takové, nebo samostatnou činností. Jak jsem uvedla výše, kyberšikanu je možné provozovat prostřednictvím nejrůznějších prostředků. Z hlediska internetu se jedná zejména o tyto: email, Instant Messaging (IM)[2], chat[3], sociální sítě, obsah zveřejněný na veřejně přístupných webových stránkách, apod.

Zásadním rozdílem mezi klasickou šikanou a kyberšikanou, kromě použitého média, je i anonymita. Šikana jako taková zpravidla bývá takzvaně tváří v tvář (face to face)[76]. Agresor zná svou oběť z běžného života a oběť zpravidla zná svého agresora.

[2] Instant Messaging je aplikace využívající prostředí Internetu umožňující oboustrannou komunikaci mezi uživateli různých zařízení, zpravidla ve formě krátkých textových zpráv. [24]
[3] Chat je uměle vytvořené prostředí v Internetu, jehož prostředím může probíhat textová komunikace několika uživatelů najednou. Zpravidla probíhá v tzv. místnostech.

V prostředí Internetu toto pravidlo spíše neplatí. Internet nabízí větší anonymitu, než při klasické šikaně. Kyberšikanu pak může provádět i jedinec, který by se k takové agresi tváří v tvář neodvážil. Jak uvádí odborná literatura (Šmahel D., 2003), virtuální svět, tedy Internet, je prostředí bez zábran. Díky tomu je agresivní chování na internetu oproti realitě až čtyřikrát častější. Tento trend se projevuje spíše u agresivního chování, tzv. flamingu než u šikany jako takové.[78] Jiná odborná literatura (Willard N., 2007) definuje flaming jako součást kyberšikany, přičemž obsahuje i další aktivity [89]:

- Flaming: agresivní a neslušné jednání.
- Harašení: opakované zasílání útočných zpráv.
- Pomlouvání: šíření pomluv on-line, zveřejňování lživých informací.
- Vylákání a zneužití soukromých informací: získání a šíření intimních soukromých informací.
- Krádež identity: vydávání se za jinou osobu za účelem poškození této osoby.
- Vyloučení: záměrné vyloučení jedince z on-line komunity.
- Cyberstalking: zastrašování oběti opakovaným zasíláním útočných zpráv a využití jiných škodlivých on-line aktivit.

Další rozdíl oproti šikaně je vzdálenost. Agresor je od své oběti vzdálen, respektive jedná přes prostředníka, médium, a ne vždy si je vědom účinků svého chování. Toto je pro šikanu netypické, agresor totiž při šikaně tváří v tvář chce vidět reakci své oběti, případně reakci svědků šikany na jednání agresora. Při kyberšikaně mohou zůstat agresorovi důsledky skryté, to je ovšem vykoupeno anonymitou agresora. Další výhodou agresora v prostředí Internetu je skutečnost, že svou oběť může pronásledovat kdykoliv, kdekoliv a odkudkoliv.

1.2.3 Setkávání se s cizími lidmi online

Prostředí Internetu nám umožňuje být v kontaktu s rodinou a přáteli (nejen) na velké vzdálenosti. Zároveň nám Internet a jeho komunikační kanály (jako jsou sociální sítě, diskusní fóra, atd.) umožňují poznávat nové lidi se stejnými nebo podobnými zájmy a smýšlením.

Současná doba je někdy natolik uspěchaná, že lidé v podstatě nemají čas seznamovat se a setkávat se konvenčními cestami tváří v tvář. Pomocníkem pro řešení takových situací je právě Internet, který umožňuje tzv. setkávání online. Stejně jako při setkání tváří v tvář, tak i při setkání online tedy hrozí rizika. Specifickou vlastností online komunikace, která může

způsobit riziko, jsou menší bariéry nebo zábrany pro navázání kontaktu a interakci s cizími lidmi. Snížení zábran je dáno anonymitou prostředí Internetu.[45]

Jedním z možných rizik setkávání se s cizími lidmi online může být již výše zmíněná Kyberšikana, dalším závažným rizikem pak může být online setkání s tzv. sexuálním predátorem. Takový predátor je motivován buď již samotnou komunikací, nebo také touhou se s dítětem setkat následně osobně. Predátor se při online setkání zpravidla chová jako chápající a podporující člověk, ať už vrstevník nebo dospělý, který se tímto způsobem snaží přiblížit k dětem, které veřejně vyjadřují svoji zranitelnost. Takové informace o dětech může predátor často získat z veřejně přístupných sociálních sítí, chatu nebo blogovacích webových stránek.[45]

Výše uvedený způsob chování a ovlivňování dítěte predátorem se v odborné literatuře nazývá grooming. Tento termín obecně označuje chování, jehož prostřednictvím se útočník nebo predátor snaží v dítěti vyvolat falešnou důvěru s plánem dítě připravit na setkání tváří v tvář[36]. Odborná literatura také uvádí, že dalším aspektem online komunikace, ve větší míře s cizími lidmi, je nevyžádaná komunikace se sexuálním podtextem. V tomto případě predátoři nemusí vyžadovat osobní setkání, ale spokojí se pouze s komunikací na toto téma. [45]

Na anonymitu je možné v tomto případě pohlížet ze dvou různých pohledů. V jednom se anonymita uživatelů Internetu může jevit jako riziko, v druhém naopak jako způsob obrany. Anonymita umožňuje predátorům vydávat se za jinou osobu, ať už z hlediska identity nebo z hlediska jím vyjadřovaných vlastností a tím působit na děti, ovlivňovat je a získávat osobní informace o nich. Zároveň je také anonymita doporučována jako způsob prevence dětí, před takovými predátory.

1.2.4 Vystavení obsahu se sexuálním podtextem

Jedním z obávaných a kontroverzních rizik číhající na děti v prostředí Internetu je jejich vystavení obsahu internetu se sexuálním nebo pornografickým tématem. V tomto případě je možné na danou problematiku nazírat dvěma možnými způsoby. Z jednoho úhlu pohledu se může jednat o ohrožení vývoje a vnímání dítěte v oblasti sexuálního vývoje, na druhou stranu, chybí-li dítěti vzor, který by jej poučil o sexuální výchově, může se jednat o způsob samovzdělávání se. Ovšem i tento způsob samovýchovy má své hranice, jejichž překročením se dítě může dostat do bezprostředního ohrožení.[83]

Touha dětí poznávat sebe sama a svou sexualitu pramení z normální dětské zvídavosti. Lze tedy předpokládat, že dítě se bude chtít obsahu se sexuálním podtextem vystavit samo a dobrovolně. Je důležité brát v úvahu, že webové stránky se sexuální tematikou, stejně jako jiné pornografické materiály, nemohou nahradit sexuální výchovu jako takovou. V případě, že se taková výchova zanedbá, vystavení dítěte obsahu se sexuální tematikou může vést ke zkresleným představám dítěte a ohrozit jeho budoucí sexuální vývoj.[83]

Z uvedeného je zřejmé, že při výchově a ochraně dítěte je důležité vytvořit kompromis mezi ochranou a přísunem informací o této tematice.

2 SOUČASNÁ SITUACE OCHRANY DĚTÍ NA INTERNETU

Do roku 2012, v evropských státech a Evropské unii, vzniklo několik zákonů, nařízení a pokynů, které mají za účel chránit děti před nebezpečným obsahem internetu. Tato ochrana je jak legislativního charakteru, tak i formou doporučení a postupů pro zajištění ochrany dětí v prostředí Internetu. Blíže k samotné ochraně a prevenci mají organizace a sdružení, která poskytují informace o možných nebezpečí číhající na uživatele Internetu. Zároveň také poskytují rady a návody, tak se těchto nebezpečí vyvarovat a případně se před nimi chránit.

2.1 Organizace působící v oblasti bezpečnosti na Internetu

V oblasti ochrany dětí na Internetu dnes přímo v rámci Internetu působí několik neziskových organizací, projektů v rámci univerzit poskytující informace i vzdělávání v této oblasti.

Národní centrum bezpečnějšího internetu (NCBI)

NCBI je nevládní, neziskové sdružení, které působí na poli ochrany uživatelů Internetu. Sdružení je členem celoevropské sítě národních osvětových center bezpečnějšího Internetu INSAFE a sítě horkých linek INHOPE, která nabízí široké společnosti zapojit se do boje proti nástrahám v Internetu, možností anonymně nahlásit podezřelý obsah.[55][23]

NCBI realizuje v současné době několik projektů na podporu informovanosti a prevence proti nebezpečím Internetu. Jedním z těchto projektů je portál Saferinternet.cz, jehož prostřednictvím se sdružení snaží vnést do povědomí široké veřejnosti možná rizika číhající na uživatele Internetu.[53] Dalším projektem sdružení, je portál Bezpecne-online.cz, jehož prostřednictvím poskytuje rady rodičům i pedagogům v oblasti prevence rizik Internetu a výukové materiály pojednávající o rizicích.[51] V neposlední řadě, důležitým projektem toto sdružení je projekt Horka-linka.cz. Jedná se o projekt zaměřený na spolupráci s uživateli Internetu, jehož prostřednictvím mají uživatelé možnost nahlásit nevhodné či nebezpečné webové stránky. V rámci projektu NCBI spolupracuje se sociální sítí Facebook, a to zejména v oblasti kyberšikany. Prostřednictvím tohoto projektu je možné předat stížnost o takovém chování přímo zástupcům sociální sítě Facebook.[52]

Google Inc.

Aktivitami v oblasti ochrany a prevence bezpečnosti na Internetu, se také zabývají komerční organizace působící v oblasti Internetu. V celosvětovém měřítku se zejména jedná o společnost Google. Společnost Google ve svém prohlášení uvádí[1], že se aktivně zapojuje

v oblasti zajišťování všeobecné bezpečnosti poskytováním jak odborných znalostí v oblasti šifrování SSL[4], tak i poskytováním nástrojů pro vývojáře webových stránek, umožňující analyzování bezpečnostních rizik jejich webových stránek a návrh řešení jejich zabezpečení. Dále si společnost Google zakládá na komunikaci s uživateli i vlastníky webových stránek a jejich podnětech o podezřelých webových stránkách, nebo o možnosti zlepšení bezpečnosti. Svou politiku bezpečnosti pak uplatňuje jak v rámci poskytovaných služeb (např. Youtube.com, vyhledávač Google, Google Play) i prostřednictvím svého prohlížeče Chrome.[1]

Seznam.cz, a.s.

V České republice se k ochraně dětí na Internetu připojila i společnost Seznam a.s.. Společnost zaštiťuje projekt Seznam se bezpečně, jehož cílem je upozornit na rizika spojená se zneužíváním identit v Internetu. Projekt společnost Seznam pojala formou filmu určeného jak pro širokou veřejnost, tak pro vzdělávací zařízení. Součástí projektu je také metodická příručka pojednávající o nástrahách Internetu, včetně konkrétních případů rizik.[77]

EU Kids Online

EU Kids Online je mezinárodní síť odborníků, která pod záštitou The London School of Economics and Political Science, spolupracuje v oblasti ochrany dětí na Internetu, zabývá se jejich aktivitami, riziky a bezpečností. Ačkoliv se jedná o mezinárodní síť, největší zastoupení má v zemích EU, včetně České republiky. Tato síť je jakýmsi pomyslným mostem mezi uživateli Internetu, především z řad dětí a jejich rodičů a evropskými politickými subjekty. Činností EU Kids Online jsou různé průzkumy napříč zeměmi, které se zabývají jak riziky, tak i informovaností široké veřejnosti o rizicích, která Internet přináší. Výsledky sítě mimo jiné tvoří i publikace zaměřené na toto téma.[13]

Centrum prevence rizikové virtuální komunikace

Jedná se o centrum pod záštitou Pedagogické fakulty Univerzity Palackého. Centrum se zabývá prevencí zaměřenou na děti v oblasti používání informačních a komunikačních technologií. Zejména pak na rizika jako jsou kyberšikana, grooming, cyberstalking, metody sociotechniky, sdílení osobních informací prostřednictvím sociálních sítí a jiných komunikačních kanálů. Centrum provádí výzkum těchto rizik, na jehož základě vytváří metodické příručky pro rodiče a pedagogy.[2]

[4] Secure Sockets Layer - protokol, který zajišťuje šifrování přenášených dat a autentizaci serveru pomocí digitálních certifikátů.[32]

Projektem centra je portál E-bezpečí.cz, jehož prostřednictvím poskytují výsledky výzkumů a také přináší ucelený přehled možných rizik a jejich prevence ve srozumitelné formě pro širokou veřejnost. Projekt je podporován Ministerstvem vnitra, Ministerstvem školství a dalšími veřejnými i soukromými organizacemi. Portál také nabízí obětem, které se dostali do rizikových situací, pomoc prostřednictvím specializované poradny.[3]

2.2 Legislativa

Zákony jsou důležitým aspektem při boji proti nebezpečím v Internetu, jelikož tato nebezpečí jsou často postavena mimo zákon. V České republice, je díky Zákonu č. 40/2009 Sb.,[10] trestního zákoníku, postižena většina činností úzce souvisejících s nebezpečnými projevy agresorů v Internetu. Zákon obsahuje značné množství definic různých trestných činů, které souvisí s tematikou této práce. Uvedu zde však jen ty, dle mého názoru, nejdůležitější.

Přesto, že se jedná o zákon, který má primárně chránit děti, může být použit i proti nim, pokud se dopustí některého z těchto trestních činů. Je důležité si uvědomit, že děti za tyto činy nejsou téměř postižitelné, jelikož do věku 15 let jsou za ně odpovědní rodiče. Přesto však tato věková hranice není, pro trestní postih vždy podmínkou.

Kyberšikana přímo v zákoně jako trestný čin definována není, ale postižitelné jsou její projevy. Součástí kyberšikany je vydírání, to je v uvedeném Zákoně č. 40/2009 Sb., trestního zákoníku v § 175, odstavci (1) definováno následovně[10]:

Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.

Přičemž zákon neopomíjí ani možnost, že by postižená osoba mohla v důsledku takového jednání zemřít. Zákon také postihuje samotnou přípravu vydírání. S kyberšikanou také mimo vydírání úzce souvisí vyhrožování, jemuž je věnován § 353 Nebezpečné vyhrožování, odstavec (1)[10]:

Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

Jak jsem uvedla v kapitole 1.2.2, součástí kyberšikany je cyberstalking, který je zákonem postižitelný dle § 354 Nebezpečné pronásledování, odstavec (1)[10]:

Kdo jiného dlouhodobě pronásleduje tím, že

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,
b) vyhledává jeho osobní blízkost nebo jej sleduje,
c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,
d) omezuje jej v jeho obvyklém způsobu života, nebo
e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,
a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

Vystavení obsahu se sexuálním podtextem, které jsem v kapitole 1.2.4 uvedla jako jednu z oblastí nebezpečného obsahu, je možné postihnout jako šíření pornografie. Definicí a postihy za šíření pornografie se ve výše uvedeném zákoně zabývá § 191. Ve vztahu k dětem je důležitý odstavec (2)[10]:

Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo

a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo
b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Přesto, že se v této práci nezabývám konkrétně tématem dětské pornografie, soudím, že je v tomto kontextu také důležité uvést § 192 Výroba a jiné nakládání s dětskou pornografií, odstavec (1) a (2), který je možné také zahrnout do oblasti obsahu se sexuálním podtextem[10]:

Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, bude potrestán odnětím svobody až na dva roky.

Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Obdobně i v případě § 193 Zneužití dítěte k výrobě pornografie, odstavec (1)[10]:

Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.

Důležitou součástí legislativní ochrany dětí před sexuálními predátory v prostředí Internetu je § 202 Svádění k pohlavnímu styku, který v odstavci (1) definuje trestně právní odpovědnost za následující činnosti[10]:

Kdo nabídne, slíbí nebo poskytne dítěti nebo jinému za pohlavní styk s dítětem, pohlavní sebeukájení dítěte, jeho obnažování nebo jiné srovnatelné chování za účelem pohlavního uspokojení úplatu, výhodu nebo prospěch, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem.

Oblastí ochrany osobních informací v prostředí Internetu se zabývá zákon č. 101/2000 Sb., o ochraně osobních údajů, který určuje, jak smí být nakládáno s osobními informacemi získanými státními orgány, orgány územní samosprávy, jinými orgány veřejné moci, fyzickými i právnickými osobami.[8]

Dalším zákonem vztahující se k ochraně informací v Internetu je zákon 480/2004 Sb., o některých službách informační společnosti. Tento zákon se věnuje zejména oblasti poskytování služeb v rámci Internetu a uchovávání informací potřebných pro přenos. Ukládá, například na jak dlouhou dobu mohou být tyto informace uchovávány a také ustavuje odpovědnost při nakládání s těmito informacemi. Zásadním bodem tohoto zákona je § 7 věnovaný šíření obchodních sdělení. Zde je jasně definováno, co je obchodním sdělením a co jím není [9]:

Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle.

3 MONITORING PRODUKTŮ PRO PC

Monitoring produktů pro PC, provedený v této kapitole se týká pouze produktů pro filtrování nevhodného obsahu webových stránek, respektive filtrování celých stránek, na kterých se takový nevhodný obsah nachází. Na trhu s produkty určených pro PC, sloužících pro zabezpečení přístupu dětí na nevhodné www stránky, je veliké množství produktů, které se liší svými funkcemi a stupni integrace.

Dostupné nástroje člením dle úrovně integrace, v operačním systému počítače, v internetovém prohlížeči, jako samostatný softwarový produkt nebo na úrovni DNS[5]. Uvedené členění jsem zvolila, abych nastínila, jaké produkty jsou vhodné pro různé situace v domácnostech, kde může být jedno, nebo více zařízení připojených na Internet, nebo více uživatelů jednoho počítače, přičemž omezení zavedená pro ochranu dětí se nemusí týkat všech uživatelů.

3.1 Produkty integrované na úrovni operačního systému

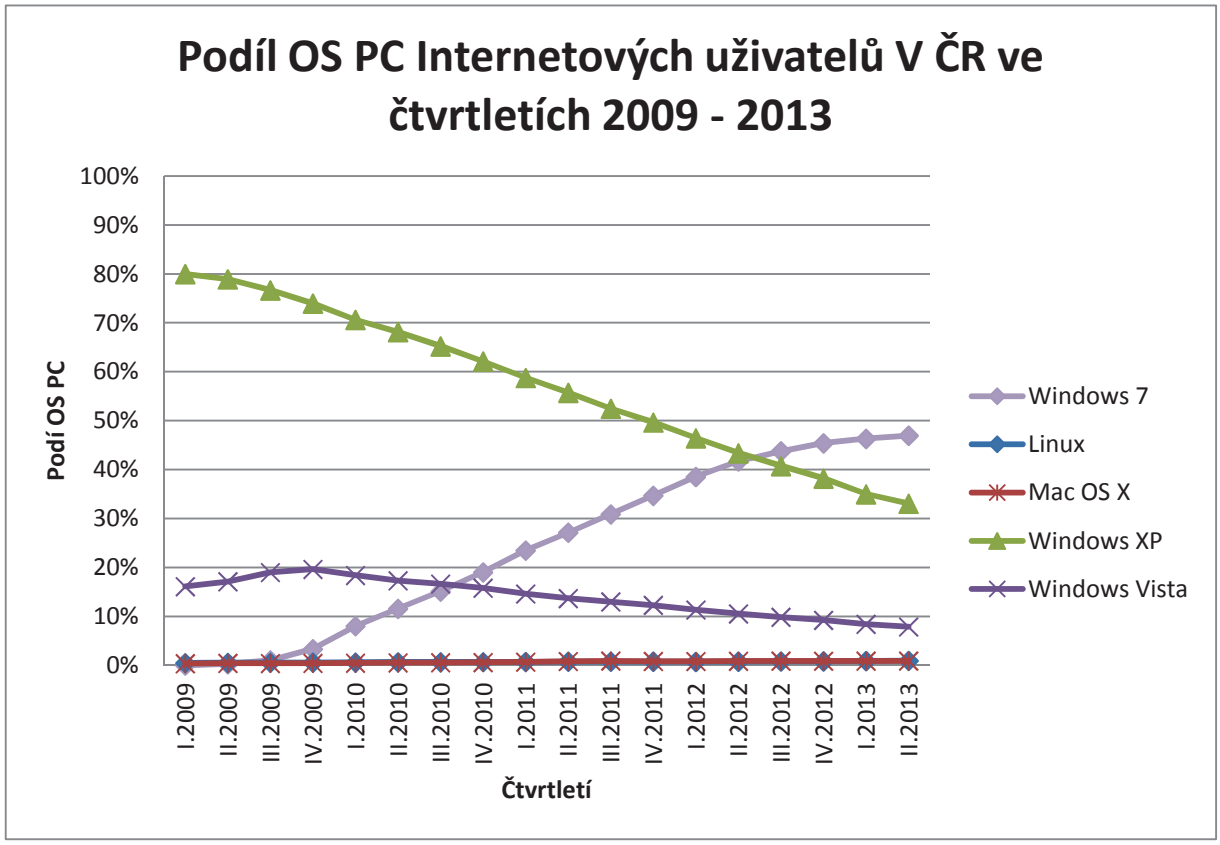
Tvůrci operačních systémů si plně uvědomují, jak důležitá je ochrana dětí na Internetu. Své operační systémy vylepšují v mnoha směrech. Jedním z těchto směrů je zlepšení správy systémů, jednotlivých uživatelských účtů a možnost nastavení tzv. rodičovské ochrany v rámci těchto systémů.

Při výběru, nástrojů na úrovni operačního systému, jsem vycházela jak z informací o dostupných nástrojích na trhu, tak z databáze výše zmíněného výzkumu SIP-BenchmarkII. Tento výzkum nabízí možnost vyhledání software pro 3 platformy operačních systémů, a to: Windows, Mac OS a Linux. V rámci prvních dvou platforem jsou dostupné nástroje rodičovské kontroly a možnosti pokročilejší správy uživatelských účtů (v závislosti na verzi OS[6]). V případě operačních systému rodiny Linux je možné si pro některé distribuce (např. Ubuntu) volně stáhnout z tzv. respozitářů[7] softwarové balíčky s podobnými funkcemi platforem Windows a Mac OS.

Pro další zpracování ovšem platformy Linux a Mac OS vynechám. Důvodem je fakt, že se jedná o minoritní skupiny. Toto tvrzení podporuje i veřejný výzkum společnosti Gemius.[58] Dle výzkumu této společnosti jsou Linux a Mac OS významně nejméně používané platformy operačních systémů v České republice. Podíl počtu internetových uživatelů s operačním

[5] DNS – Domain Name Server – Server sloužící pro překlad doménových jmen na IP adresy[4]
[6] OS – Operační Systém
[7] Respozitář – veřejně dostupné úložiště softwarových balíčků pro platformu Linux[85]

systémem typu Linux zobrazuje Obrázek 1. Na zobrazeném grafu je možné vidět, že podíl internetových uživatelů této platformy za období od roku 2007 až do dubna 2012 nepřekročil 5%. V případě Mac OS je využití této platformy obdobné. Naopak je jasně znázorněn pád dosluhujícího operačního systému Windows XP a vzestup operačního systému Windows 7. Tento trend je možné označit za celoevropský. Mimo Evropu je možné pozorovat větší vzestup operačních systémů platforem Mac OS.



Obrázek 1 - Podíl operačních systémů PC Internetových uživatelů v ČR ve čtvrtletích 2009 – 2013

Zdroj:upraveno dle [58]

Windows Live zabezpečení rodiny

Produkt, Windows Live Zabezpečení rodiny, je doplňkem integrovaného nástroje Rodičovská kontrola v rámci OS Windows. Oba produkty jsou součástí balíčku Windows Live Essentials. Prostřednictvím tohoto produktu je možné v rámci OS nastavit, jaké aktivity mohou děti provozovat při práci s počítačem. Jedná se v podstatě o komplexní produkt, který nabízí nejen možnost filtrování webových stránek, ale také správu povolených či zakázaných aplikací, her nebo nastavení času, po který mohou děti počítač užívat[20].

Předpokladem tohoto produktu je skutečnost, že každý uživatel počítače má svůj vlastní účet v rámci OS Windows. Pokud ne, nastavené změny jsou platné pro všechny uživatele v rámci jednoho účtu. Zároveň se předpokládá používání programů a nástrojů již integrovaných v OS Windows a využívání služeb poskytnutých společností Microsoft[20]. Je ovšem nutné zmínit fakt, že IM klient známý jako Windows Live Messenger byl nahrazen službou Skype, kterou společnost Microsoft koupila v roce 2011.[46]

Podmínkou pro spuštění produktu Windows Live Zabezpečení rodiny je registrace do služby Windows Live Essentials. Prostřednictvím zřízeného účtu a jeho přirazení k příslušnému účtu rodiče v počítači, je možné spravovat účty v rámci Windows Live Zabezpečení rodiny.[54]

Funkce produktu

Funkce produktu jsou rozšířeny o funkce rodičovské kontroly, jehož je Windows Live Zabezpečení rodiny nadstavbou. Proto jsou zde uvedeny i funkce, které umožňuje rodičovská kontrola ve Windows. Jejich vzájemným propojením je možné dosáhnout lepšího zabezpečení a monitoringu činností dětí nejen v prostředí Internetu, ale zároveň také v rámci celého operačního systému.

Hlavními funkcemi produktu je filtrování webových stránek a sledování aktivit uživatele na Internetu. Filtrování je zajištěno pomocí kategorizace webových stránek do kategorií: Vhodné pro děti, Sociální sítě a Obsah pro dospělé[30]. Filtrování obsahu webových stránek platí i pro jiné webové prohlížeče než je MS Internet Explorer, běžně integrovaný v systému Windows.

Další funkcí produktu je filtrování obsahu webových stránek s možností vlastního nastavení blokovaných nebo povolených webových stránek. Součástí této funkce je také možnost povolení nebo zamítnutí webové stránky rodičem v okamžiku, kdy se dítě dožaduje přístupu na blokovanou webovou stránku. V případě, že se dítě v rámci účtu, který má nastavenou službu Windows Live Essentials s Windows Live Zabezpečení rodiny dostane na webovou stránku, která je blokovaná může požádat o její zpřístupnění emailem nebo osobně. Rodič, který službu zřídil, má možnost žádost povolit nebo zamítnout pro daný účet dítěte, nebo pro všechny účty na daném počítači.[54]

Důležitou součástí je také monitorování aktivit dětí na Internetu. Jedná se v podstatě o sledování všech webových stránek, které dítě navštěvuje a také kolikrát dané webové stránky navštívilo.[54]

Produkt je dostupný pouze pro některé verze operačního systému Windows. V případě, že rodič chce využít tohoto produktu, musí mít jeden z následujících operačních systémů[64]:

- Windows 7 (32 or 64 bit edice).
- Windows Vista Service Pack 2.
- Windows Server 2008 R2.
- Windows Server 2008 Service Pack 2.

V rámci produktu Windows Live Zabezpečení rodiny je možné ve webových prohlížečích nastavit jako domovskou stránku tzv. Dětské weby služby Zabezpečení rodiny. Jedná se o seznam webových stránek, které jsou dle společnosti Microsoft zařazené jako webové stránky vhodné pro děti. Tato služba ovšem není dostupná v českém jazyce ani zde neexistuje seznam českých webových stránek vhodných pro děti.

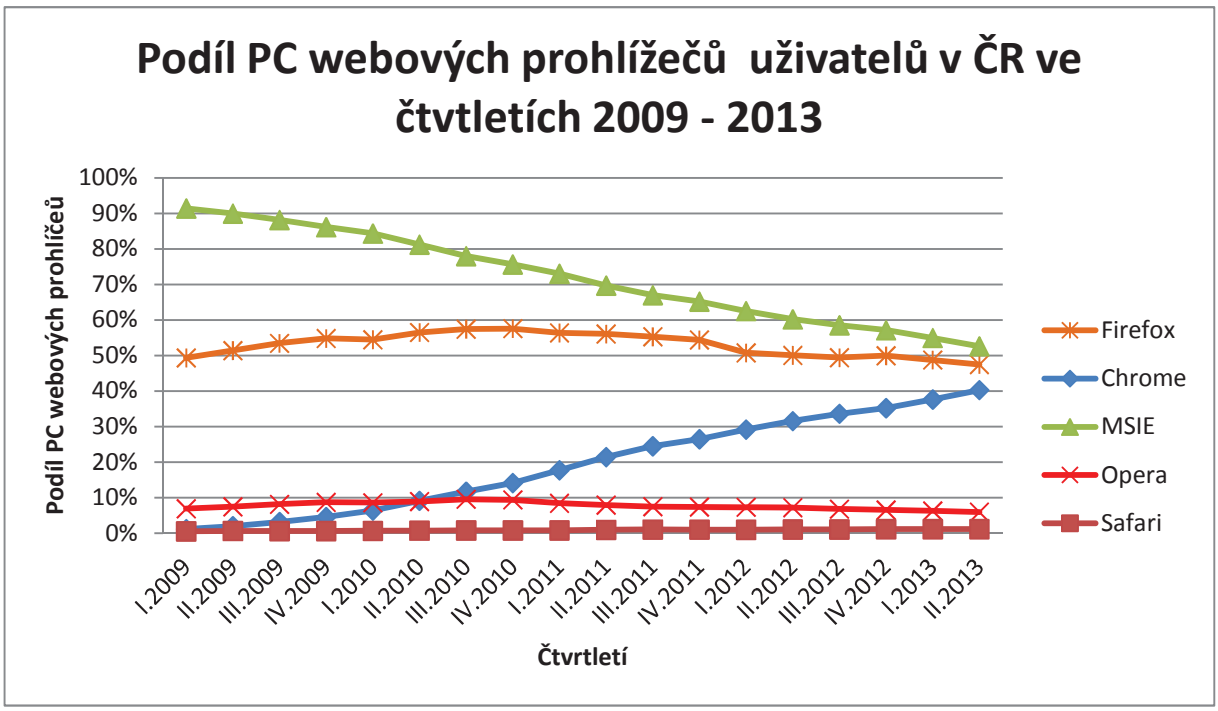
3.2 Produkty integrované na úrovni webového prohlížeče

Webový prohlížeč je ve své podstatě program, který slouží k prohlížení www stránek, tedy World Wide Webu. Program interpretuje, respektive překládá webové stránky vytvořené pomocí značkovacího jazyku HTML[8] a jeho modifikací. Důvodem, proč neexistuje jeden univerzální webový prohlížeč je vývoj Internetu a snaha vývojářů webových prohlížečů vylepšit nebo rozšířit HTML kód o nestandardní funkce za účelem implementace nových prvků.[75]

V současné době, verze HTML5 obsahuje některé, dříve nestandardní, prvky. Webové prohlížeče se příliš neliší v interpretaci HTML kódu a kaskádových stylů (CSS) platných v této verzi.

Dle výzkumu společnosti Gemius[88], nejpoužívanějšími webovými prohlížeči za poslední tři roky, jsou prohlížeče skupin MS Internet Explorer, Mozilla Firefox a Google Chrome. Jejich podíl zobrazuje Obrázek 2. Jako skupiny je označuji z toho důvodu, že paralelně mohou uživatelé používat různé verze těchto prohlížečů. Nadále se budu věnovat pouze třem výše zmíněným skupinám prohlížečů, jelikož skupiny prohlížečů Opera a Safari jsou mezi těmito skupinami minoritní.

[8] HyperText Markup Language – značkovací jazyk pro tvorbu webových stránek[75]



Obrázek 2 - Podíl webových prohlížečů PC Internetových uživatelů v ČR ve čtvrtletích 2009 – 2013

Zdroj: upraveno dle[88]

3.2.1 MS Internet Explorer

Webový prohlížeč Internet Explorer společnosti Microsoft je unikátní zejména v tom smyslu, že byl integrován téměř ve všech verzích operačního systému Windows. Díky tomu, že je operační systém Windows hojně využíván, prvenství webového prohlížeče Internet Explorer není překvapivé. V minulosti byla tato skutečnost předmětem antimonopolního řízení[86].

V tomto prohlížeči ve své podstatě neexistuje sofistikovanější způsob ochrany, než nastavení úrovně zabezpečení v prostředí Internetu a intranetu a nastavení důvěryhodných, případně nedůvěryhodných webových stránek, případně celých webových sídel. Poskytuje ovšem ochranu před phisingem[9] a malware[10] prostřednictvím filtru SmartScreen, který je dostupný od verze Internet Explorer 9[15]. Součástí této základní ochrany je také možnost nastavení poskytování osobních údajů, která může zablokovat ukládání souborů cookies[11] nebo zablokovat poskytování údajů o poloze. Toto nastavení není ovšem nijak chráněno a je možné jej snadno změnit.

[9] Phising – druh Internetového podvodu, jehož účelem je vylákat přístupové informace uživatelů k účtu.[61]
[10] Malware – software, jehož účelem je poškození počítače a odcizení citlivých údajů.[29]
[11] Cookies – soubory cookies jsou malé soubory ukládané navštíveným serverem do počítače uživatele prostřednictvím webového prohlížeče.[79]

Přesto však tento prohlížeč není zcela bezbranný při ochraně dětí v prostředí Internetu. Jak jsem již uvedla výše v kapitole 3.1, Internet Explorer může pomoci k ochraně dětí jako součást produktu Windows Live zabezpečení rodiny. Předpokladem je ovšem použití minimálně verze OS Windows Vista nebo Windows server 2008.

3.2.2 Firefox

Firefox je open source webový prohlížeč společnosti Mozilla Corporation, jejímž zakladatelem je nezisková organizace Mozilla Foundation. Prohlížeč Firefox je freeware, který je volně šiřitelný pod licencí MPL (Mozilla Public License)[75].

Firefox, na rozdíl od prohlížeče Internet Explorer neumožňuje vlastní nastavení blokace nevhodných webových stránek. Tato funkce je nahrazena pouze blokací nahlášených útočných stránek, nebo blokací nahlášených podvodných stránek. Ukládání souborů cookies je možné v prohlížeči vypnout a použít režim tzv. anonymního prohlížení. Ovšem stejně jako u předchozího prohlížeče, i tato opatření je možné jednoduše změnit.

V rámci tohoto prohlížeče je však možné přidat prvky pro filtrování, nebo blokaci webových stránek prostřednictvím doplňků, addonů. Díky tomu, že Firefox je open source software, doplňky vytváří sami uživatelé tohoto prohlížeče. V oblasti ochrany dětí v prostředí Internetu je doplňků pro Firefox velmi málo a některé podle hodnocení ostatních uživatelů vzbuzují dojem nepříliš dobře vytvořeného doplňku. V této části jsem vybrala doplňky, které slouží k filtrování a blokování obsahu webových stránek právě s ohledem na hodnocení uživatelů, tedy nejvíce kladně hodnocené v dané kategorii doplňků.

Doplněk Blocksi - Web filtering and parental control

Účelem doplňku Blocksi je ochrana uživatelů webového prohlížeče před nevhodným obsahem webových stránek. Kromě obsahu webových stránek blokuje i celé URL adresy. Nabízí možnost vytvořit si vlastní white a black list, což jsou seznamy povolených a blokovaných webových stránek. Filtrování webových stránek a jejich obsahu je postaveno na kategorizaci, hodnocení webových stránek a na blokování konkrétních slov a frází. Doplněk také poskytuje možnost správy času, tedy doby, kdy je možné prohlížeč používat. Zároveň je možné všechny tyto funkce ovládat prostřednictvím vzdálené správy, která umožňuje nastavení aplikovat a synchronizovat, v případě využití na několika počítačích, zároveň. Pomocí doplňku je také možné blokovat videa umístěná na populárním serveru Youtube.com podle kategorií, do kterých videa tematicky spadají. [26]

Pro některé uživatele může být nevýhodou rozhraní lokalizované pouze v angličtině. Naopak výhodou doplňku je možnost jeho instalace jak do prohlížeče Firefox, tak i Google Chrome.

Nastavení doplňku je chráněno heslem, ale možnost ochrany deaktivace doplňku v nastavení prohlížeče chybí. Doplněk je tedy možné kdykoliv v prohlížeči vypnout a vyřadit tak veškerá omezení, která tento doplněk přináší. Tímto omezením je doplněk vhodný spíše pro děti nižšího věku, které ještě neumí s nastavením prohlížeče manipulovat.

3.2.3 Google Chrome

Google Chrome (dále jen Chrome) je webovým prohlížečem společnosti Google, která jej představila v druhé polovině roku 2008. Jedná se o prohlížeč založený na jádru WebKit, které je součástí operačních systémů a má na starosti interpretaci HTML a JavaScriptu.[19]

Chrome je postaven na projektu s otevřeným zdrojovým kódem Chromium. Chronium je dle vývojářů Google projekt, který se snaží dosáhnout vytvoření bezpečnějšího, rychlejšího a stabilního způsobu využívání Internetu.[22]

Z grafu, který zobrazuje Obrázek 2 na straně 26 je možné odhadnout stoupavý trend v počtu použití Chrome pro přístup na webové stránky. Stává se tak silnou konkurencí pro vedoucí webové prohlížeče, jako jsou MS Internet Explorer a Firefox.

Chrome nabízí možnost nastavení ochrany soukromí ve smyslu uchovávání souborů cookies v prohlížeči, odesílání informací o fyzické poloze uživatele, použití multimediálních zařízení, jako je webkamera, nebo mikrofon. Chrome poskytuje také ochranu proti škodlivému obsahu internetu jako je malware a phishing. Možnost blokování webových stránek v základním nastavení prohlížeče Chrome, chybí.

V rámci webového prohlížeče Chrome, je možné instalovat doplňky, tedy rozšířit stávající verzi prohlížeče o doplňující software. Na rozdíl od přecházejících webových prohlížečů, je pro prohlížeč Chrome dostupných několik doplňků pro ochranu před nebezpečným obsahem Internetu a filtrování webových stránek s nevhodným obsahem. Vybrala jsem pouze zlomek těchto doplňků, které od uživatelů dostali nejvyšší hodnocení v oblasti filtrování a ochrany.

Doplněk avast! Online Security

Stejně jako u prohlížeče Firefox je možné i do Chrome dodat prostřednictvím doplňků aplikace, které slouží k ochraně uživatelů a počítače před nebezpečným obsahem Internetu. V této oblasti je nejlépe hodnoceným a zdarma dostupným doplňkem (ze strany uživatelů)

avast! Online Security. Jedná se o doplněk vytvořený společností AVAST Software a.s.. Tento doplněk je dostupný zdarma pro uživatele Chrome. Výhodou tohoto doplňku je české rozhraní. Účelem doplňku je varovat uživatele před phishingovými a infikovanými webovými stránkami, varovat uživatele při návštěvě s nevhodným obsahem (webové stránky s pornografickým obsahem, stránky obsahující násilí, apod.).[25] Varování před webovými stránkami s nevhodným obsahem je založeno na hodnocení webových stránek samotnými uživateli, čímž je hodnocení zavádějící a nemusí poskytovat správné informace. Doplněk je v prohlížeči Chrome dostupný všem uživatelům a tudíž má každý možnost jej vypnout.

Doplněk FoxFilter – The content filter!

Doplněk FoxFilter, který je možné instalovat do prohlížeče Firefox je určený zejména pro filtrování webových stránek s pornografickou tématikou. Zároveň tento doplněk také umožňuje filtrování dalšího obsahu, které si nastaví sám uživatel. Stejně jako předchozí doplněk, i FoxFilter je možné získat zdarma. Ovšem pro získání některých dalších bezpečnostních funkcí je nutné zaplatit roční poplatek dle zvoleného počtu počítačů a úrovně zabezpečení. Rozšířené funkce zabezpečení spočívají v zpřístupnění možnosti ochrany odebrání nebo deaktivace doplňku heslem, nebo ochraně před pokusem obejít doplněk. Tato funkce je dostupná za € 9,00 ročně.

Ve verzi dostupné zdarma je možné nastavit úrovně blokování webových stránek, od úrovně blokování definovaných blokovaných webových stránek, definovaných klíčových slov až po úroveň povolení vybraných webových stránek. Zároveň je možné v nastavení blokovaných webových stránek a klíčových slov definovat klíčová slova, která mají být filtrem ignorována. Doplněk umožňuje také tzv. citlivostní filtrování, které umožňuje filtrování pouze určitého obsahu webové stránky. Tato nastavení nejsou ve verzi dostupné zdarma chráněna heslem.

Tento doplněk jsem vybrala jako uživatelsky nejlépe hodnocený doplněk z nabízených v oblasti filtrování obsahu webových stránek a také z důvodu, že nabízí možnost ochrany deaktivace doplňku, ač je přístupná až po zaplacení roční licence, která u ostatních doplňků chybí.

V případě, že se uživatel pokusí navštívit webovou stránku, která je obsažena v seznamu blokovaných, nebo naopak není obsažena v seznamu povolených webových stránek, je doplňkem přesměrován na stránku s dialogem, kde po zadání přístupového hesla může vstoupit na blokovanou webovou stránku. Toto upozornění, jakož i celý doplněk je

v angličtině. Přes tuto minimální překážku, je možné volně pokračovat na požadovanou webovou stránku.

3.3 Samostatné softwarové produkty

Samostatné softwarové produkty jsou další možností jak omezit dětem přístup na nevhodné webové stránky s nebezpečným obsahem. Na trhu je mnoho samostatných produktů, které umožňují filtrovat nevhodné webové stránky podle jejich obsahu a zároveň také nabízí další funkce, které slouží pro ochranu dětí v Internetu. Všeobecně se takové produkty dají označit jako tzv. Rodičovská ochrana (volně přeloženo z Parental Control). Užší výběr těchto produktů jsem provedla na základě výzkumu SIP-Benchmark II, který zajišťuje Evropská komise v rámci programu Safer Internet. Tento výzkum každoročně monitoruje software, který má sloužit k ochraně dětí na Internetu.[14]

3.3.1 Profil Parental Filter 2

Produkt Profil Parental Filter 2 je software, který pochází z laboratoře společnosti Profil Technology. Produkt zabezpečuje ochranu před přístupem na nevhodné webové stránky podle kategorií, do kterých dané webové stránky spadají, nebo umožňuje vytvoření vlastního seznamu vyloučených, či povolených webových stránek. Mimo tyto funkce produkt také nabízí filtrování emailů, ochranu osobních a systémových složek v počítači, blokování streamovaných[12] videí (např. Youtube.com), blokování stahování souborů do počítače nebo omezení času pro přístup k Internetu nebo k vybraným programům instalovaných na počítači. Produkt také umožňuje vytvořit profily s různým nastavením omezení a filtrování, přičemž vytvořený profil lze přiřadit jednomu uživateli počítače. V oblasti zabezpečení produktu a jeho funkcí nabízí produkt jak ochranu složky, ve které je produkt nainstalován, tak ochranu heslem proti pokusům o jeho odebrání. Produkt je dostupný v několika jazykových mutacích mimo češtiny. [67]

Technická specifikace[67]:

- Operační systém: Windows® XP, Vista nebo 7.
- Procesor: 500 MHz nebo vyšší.
- Minimální volné místo na pevném disku: 200 MB.
- Minimální paměť RAM: 512 MB.
- CD-ROM nebo DVD mechanika.
- Připojení k Internetu.

[12] Streamované video – video uložené na serveru, přehrávané v reálném čase.[59]

Produkt je možné si vyzkoušet díky 30-ti denní verzi zdarma, která obsahuje všechny dostupné funkce jako placená verze produktu. Produkt není možné zakoupit jednorázově, lze jej pořídit formou roční licence. Cena roční licence produktu je 39,99 €.[67]

3.3.2 PureSight Owl

Produkt PureSight Owl, společnosti PureSight Technologies Ltd., je samostatný produkt, který stejně jako Profil Parental Filter 2 umožňuje nejen filtrování nevhodných webových stránek, ale také poskytuje další funkce, které napomáhají k ochraně dětí v prostředí Internetu.[74]

Produkt umožňuje vzdálené monitorování činností dětí v Internetu, prakticky odkudkoliv, kde je možné se připojit k Internetu. Nabízí také možnost ochrany nejen na počítači, ale také i na dalších zařízeních, která se mohou k Internetu připojit (např. smartphone[13]). Součástí produktu je také možnost nastavení času, po který má dítě umožněn přístup k Internetu. Mimo blokování a filtrování nebezpečného obsahu, produkt ještě nabízí monitorování činností dětí v sociální síti Facebook. Poskytuje informace o veškerých informacích související s profilem dítěte na této sociální síti, od seznamu přátel až po zveřejněné fotografie, videa nebo textové příspěvky na profilu. Produkt, dle uvedených informací, poskytuje možnost filtrování obsahu a blokování kontaktů v komunikaci prostřednictvím IM. Mimo monitoring a restrikce produkt umožňuje zasílání výstražných zpráv, o pokusech porušení restrikcí, prostřednictvím emailu. Ovšem všechny tyto informace, stejně jako produkt samotný jsou lokalizovány pouze v anglickém jazyce.[74]

Technická specifikace[72]:

- Operační systém: Windows XP Home/Professional, Vista, 7.
- PC s procesorem Pentium 300 MHz.
- 128 MB RAM nebo vyšší.
- 50MB volného prostoru na HDD
- Grafické rozlišení 1024 x 768 nebo vyšší.
- Připojení k Internetu.

Produkt je možné si před zakoupením vyzkoušet, nabízí 30-ti denní bezplatnou verzi. Tato verze ovšem neobsahuje všechny funkce dostupné v placené verzi. Alternativou může být zakoupení měsíční licence za 5,99 $. Cena roční licence produktu je 59,90 $.

[13] Smartphone – mobilní telefon s pokročilými funkcemi.[40]

3.3.3 Kaspersky Pure

Produkt Kaspersky Pure je, na rozdíl od předchozích produktů, určen pro ochranu počítače jako takového. Jedná se o kombinaci antivirové ochrany a rodičovské ochrany. Možnosti ochrany dětí v Internetu, které produkt poskytuje, jsou obdobné jako u předchozích produktů. Součástí ochrany je blokování webových stránek dle kategorií nebezpečného obsahu, nebo nastavení vlastního seznamu vyloučených či povolených webových stránek.[35]

Zároveň produkt umožňuje filtrování a blokování komunikace prostřednictvím IM, nabízí možnost nastavení časového plánu pro přístup k Internetu, a také k programům v počítači. Poskytuje možnost blokování stahování souborů, blokování odesílání osobních informací jako jsou například telefonní čísla, nebo čísla platebních karet. Další z funkcí produktu je monitoring činností jak v prostředí Internetu, včetně komunikace prostřednictvím IM, tak i monitoring spuštěných programů v rámci počítače.[35]

Technická specifikace[34]:

- Operační systém: Microsoft Windows XP, Vista, 7.
- 600 MB dostupného volného místa na HDD.
- CD/DVD-ROM .
- Internetové připojení.
- Počítačová myš.
- Internet Explorer 6.0 a vyšší.
- Windows Installer 2.0 a vyšší.

Trialová, 30 denní, plně funkční verze, produktu je dostupná na webových stránkách tvůrce produktu, společnosti Kaspersky Lab[35] Produkt je v angličtině, případně v jiné jazykové mutaci mimo češtiny. Cena roční licence produktu je 75,95 $.

3.4 Produkty integrované na úrovni DNS

DNS, neboli domain name server je server umístěný v síti Internetu, který pomáhá při získávání webových stránek požadovaných uživatelem. Jeho účelem je překlad snadněji zapamatovatelných doménových jmen na těžko zapamatovatelné IP[14] adresy serverů s webovými stránkami a naopak.[4]

Při domácím využití Internetu se běžně používají DNS servery Internetového poskytovatele. V případě produktů integrovaných na úrovni DNS jsou dotazy na webové stránky směřovány přes DNS třetí strany. Uživatel, který chce takového DNS využít má

[14] IP – Internet Protocol – numericky vyjádřená adresa počítače v počítačové síti.

možnost nastavit si vlastní filtrování webových stránek nebo využít přednastavené bezpečnostní politiky.

Produkty na úrovni DNS jsou ve své podstatě služby, které jsou poskytovány prostřednictvím serverů poskytovatele, specializovaného na filtrování DNS, umístěných v Internetu. Integrace takové služby pak spočívá v přesměrování domácího routeru[15] nebo příslušného počítače na IP adresu s filtrovaným DNS.

Jedním ze zástupců těchto produktů je OpenDNS společnosti OpenDNS, Inc [57]. Pro domácí využití společnost OpenDNS nabízí produkt Parental Controls v různých verzích. V nabídce jsou tedy jak free verze DNS s přednastaveným filtrováním a blokováním nevhodného obsahu Internetu pro děti, free verze s možností vlastního nastavení filtrování a blokování webových stránek, tak i prémiová placená verze umožňující tvorbu statistik navštěvovaných stránek v Internetu. Samozřejmostí u placené verze je zákaznická podpora.

Jak jsem zmínila výše, IP adresu serveru s DNS je možné nastavit jak na samotném počítači, tak i v rámci domácí sítě na příslušném routeru. V druhém případě je zajištěno filtrování obsahu pro všechna možná zařízení, která se v domácnosti prostřednictvím domácí sítě připojují k Internetu, tedy notebooky, tablety, smartphony i herní konzole.

Filtrované DNS servery jsou jako služby také součástí antivirových programů, které umožňují zajištění bezpečného filtrování webových stránek v Internetu.

[15] Router – aktivní síťový prvek sloužící pro přenos dat mezi propojenými sítěmi.

4 MONITORING SW PRODUKTŮ PRO SMARTPHONE

V dnešní době mají děti přístup k Internetu nejen prostřednictvím PC, ale také prostřednictvím tzv. smartphone. V doslovném překladu se jedná o chytrý mobilní telefon. Od běžného mobilního telefonu se liší zejména přítomností operačního systému připomínající operační systém platformy PC. Dalším zásadním rozdílem je možnost rozšíření OS smartphone o další aplikace. Tato možnost u starších mobilních telefonů je také, ale ve velmi omezené míře, většinou se jedná o herní aplikace. Smartphone se také vyznačuje dotykovým displejem s hardwarovou qwerty klávesnicí, nebo její softwarovou obdobou. Posledním z nejdůležitějších znaků smartphone je možnost připojení k Internetu a použití plnohodnotného Internetového prohlížeče. U starších mobilních telefonů je také možné připojit se na Internet, ale dostupné jsou pouze webové stránky ve verzi pro mobilní telefony. V případě starších mobilních telefonů surfování na Internetu zdaleka nenabízí takové možnosti, jaké jsou dostupné při používání smartphone.[40]

Běžnou součástí dnešních smartphone je přítomnost Wi-fi adaptéru. Vlastník smartphone se tedy může kdykoliv připojit na veřejnou nezabezpečenou síť bez nutnosti znát heslo, nebo na jakoukoliv Wi-Fi síť, ke které zná přístupové údaje. Stejně jako běžné mobilní telefony, tak i smartphone nabízí připojení k Internetu prostřednictvím mobilní sítě GSM[16] nebo pokročilejší WCDMA[17] .

Smartphone jsou pro dnešní děti i mládež nedělitelnou součástí jejich komunikace, a proto je nutné věnovat pozornost i těmto zařízením a zejména tomu, jak jsou tato zařízení účinná při ochraně dětí před nebezpečími, která jim jejich používáním mohou hrozit.

Hranice mezi smartphone a tabletem je velmi úzká, v některých případech téměř neexistuje. Jediným dělícím prvkem je v podstatě název, které danému zařízení dávají sami výrobci. Proto softwarové prostředky, které zde uvádím, je často možné použít jak ve smartphonech, tak i v tabletech.

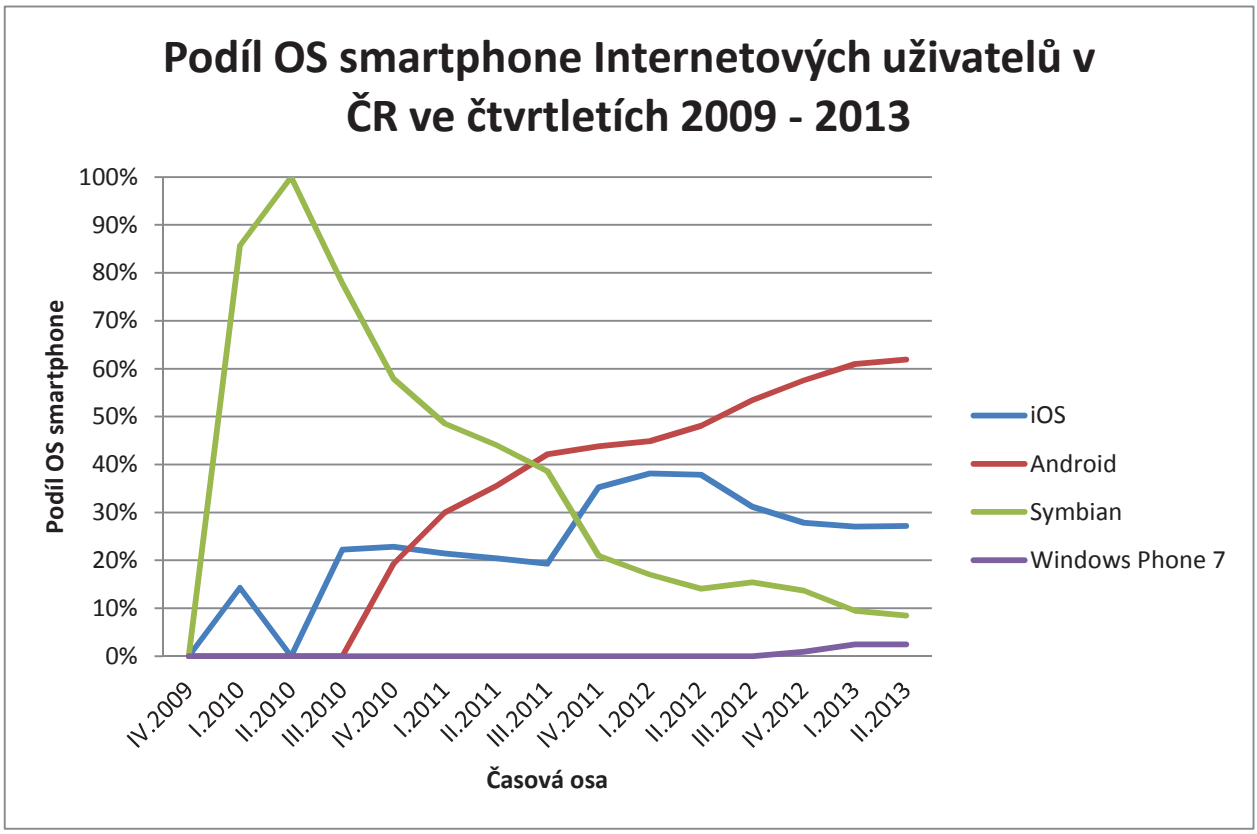
Rozdělení produktů do kategorií dle stupně integrace, jak jsem produkty rozdělila v případě produktů pro platformu PC, není pro platformu smartphone vhodné. Produkty na úrovni DNS jsou stejné jak pro platformu PC, tak pro platformu smartphone. Tyto produkty jsou totiž nezávislé na aplikované platformě, jelikož filtrování nevhodných webových stránek může probíhat již na úrovni aktivního síťového prvku, jako je například domácí router.

[16] GSM - Global System for Mobile Communication – standart pro bezdrátovou mobilní komunikaci.[5]
[17] WCDMA - Wideband Code Division Multiple Access – technologie přenosu dat.[87]

Operační systém smartphone

Trh se smartphone se rozděluje nejen podle jednotlivých výrobců zařízení, ale také podle OS. Stejně jako u PC je u některých smartphone možné zvolit si vlastní OS nebo si zvolit model smartphone s přednastaveným OS.

Smartphone se v České republice ve větší míře začaly rozšiřovat začátkem roku 2010. Mezi největší zástupce OS pro smartphone patří Android společnosti Google, iOS společnosti Apple, Symbian společnosti Nokia a Windows mobile (phone) společnosti Microsoft. Jak zobrazuje Obrázek 3, v současné době na trhu dominuje OS Android. V příloze A je uveden graf podílu OS PC a smartphone Internetových uživatelů V ČR ve čtvrtletích 2009 – 2013, který zobrazuje celkový přehled podílu OS pro platformy PC a smartphone.



Obrázek 3 - Podíl OS smartphone internetových uživatelů v ČR ve čtvrtletích 2009 – 2013

Zdroj: upraveno dle[58]

Produkty vhodné pro operační systém Android jsem vybrala na základě výzkumu SIP-Benchmark II [14] a také dle oblíbenosti uživatelů mobilních aplikací pro ochranu dětí v Internetu. Produkty jsou dostupné prostřednictvím služby Google Play, která slouží pro poskytování digitálního obsahu od hudby, přes filmy, knihy až po hry nebo aplikace.[56]

F-Secure Mobile Security

F-Secure Mobile Security je učený pro ochranu dětí v Internetu při použití smartphone, či jiného zařízení s operačním systémem Android. Jedná se o produkt, který v sobě kombinuje Anti-Virus, technologii Anti-Theft, která slouží jako ochrana proti krádeži, zabezpečený webový prohlížeč, funkce rodičovské ochrany a funkce zabezpečení kontaktů smartphone.[17]

Funkce rodičovské kontroly zajišťuje filtrování webových stránek dle obsahu a také dle zvoleného profilu věku uživatele. Zároveň také produkt umožňuje nastavení povolených, v zařízení nainstalovaných, aplikací. Veškerá tato nastavení, včetně možnosti odebrání produktu jsou chráněna heslem.[17] V případě použití technologie Anti-Theft a GPS modulu, který je dnes součástí téměř všech mobilních zařízení tohoto typu, je možné sledovat pohyb dítěte.

Produkt je plně lokalizován do českého jazyka a v rámci služby Google Play je dostupná 30-ti denní, plně funkční, zkušební verze a také plná verze s roční licencí za € 14,95.[49]

Funamo Parental Control

Produkt Funamo Parental Control v sobě zahrnuje hned několik funkcí spadající do oblasti rodičovské ochrany. Nabízí filtrování webových stránek při použití zabezpečeného prohlížeče produktu a možnost sestavení seznamu vyloučených nebo povolených webových stránek. Nabízí také možnost sestavení seznamu klíčových slov, při jejichž výskytu produkt zablokuje přístup na danou webovou stránku. Produkt umožňuje blokování sociálních sítí, jako jsou například Facebook, Myspace nebo Twitter. Poskytuje funkci bezpečného vyhledávání webových stránek prostřednictvím vyhledávačů Google, Bing nebo Yahoo. Nastavení produktu mohou být provedena přímo v zařízení, ve kterém je produkt nainstalován, i prostřednictvím vzdáleného přístupu přes webový prohlížeč.[18]

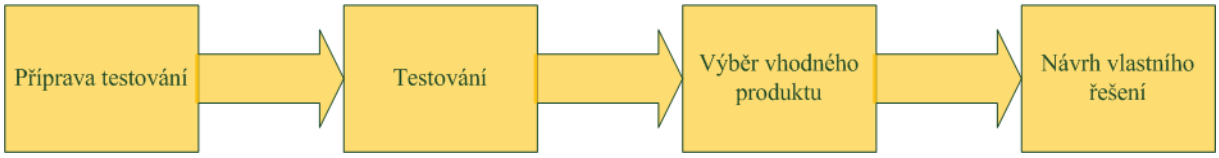
Mimo filtrování webových stránek produkt také nabízí sledování aktivit prováděných na zařízení. Rodiče tak mohou mít přístup k historii volání, SMS[18] zpráv, spuštěných aplikací nebo navštívených webových stránek. [18]

Oproti předchozímu produktu, Funamo Parental Control nabízí i možnost správy času, po který dítě může používat nainstalované mobilní aplikace, jako jsou například hry, kanály pro sledování videí, apod. Produkt je dostupný v anglickém jazyce.[18]

[18] SMS – Short Message Service, krátká textová zpráva sloužící pro komunikaci prostřednictvím mobilní sítě.

5 PŘÍPRAVA TESTOVÁNÍ PRODUKTŮ

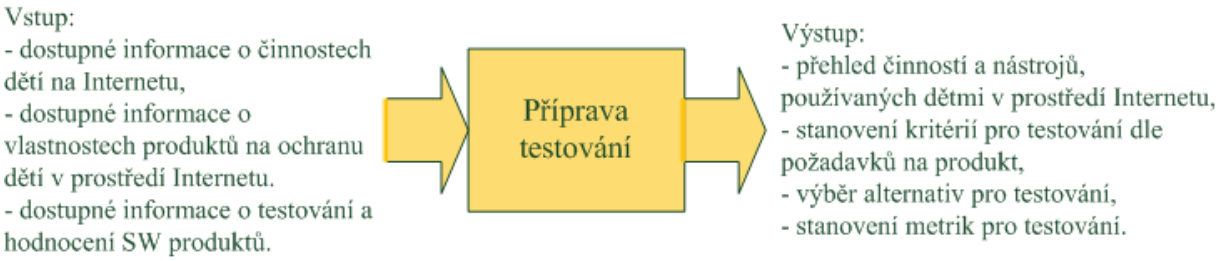
Příprava testování produktů je prvním krokem ze série postupů, které vedou k cíli této práce a tím je navržení vlastního řešení zlepšení ochrany dětí v prostředí Internetu. Jednotlivé kroky na sebe úzce navazují a výstupy jedné kapitoly jsou vstupy další kapitoly. Takový proces je možné vyjádřit jako schéma, jak jej zobrazuje Obrázek 4.



Obrázek 4 - Schéma postupu relizace vlastního návrhu řešení

Zdroj: vlastní

Samotnému testování předchází příprava testování produktů pro ochranu dětí před nebezpečným obsahem Internetu. V tomto případě je nutné zjistit, jaké činnosti děti v prostředí Internetu provádí. Z těchto informací je pak možné odvodit požadavky na produkty, tedy na funkce, které mají za úkol chránit děti v prostředí Internetu. Tyto činnosti a vlastnosti slouží jako vstupy pro přípravu testování. Transformaci vstupů na výstupy této části zobrazuje Obrázek 5.



Obrázek 5 - Schéma vstupů a výstupů pro přípravu testování produktů

Zdroj: vlastní

Výstupem této části je stanovení kritérií pro testování produktů a výběr vhodných alternativ k testování. Jelikož v další části této práce hodnotím tyto alternativy a vybírám z nich optimální alternativu dle stanovených kritérií, musí se jednat o srovnatelné alternativy. Součástí přípravy testování je také výběr prostředí, ve kterém budou prováděny testy.

5.1 Činnosti dětí na internetu

Před výběrem software k testování je nutné znát, chování dětí v prostředí Internetu, tedy jaké činnosti nejčastěji provádějí. Dle studie, Risks and safety on the internet, provedenou napříč 25 státy Evropské unie, děti ve věku 9 - 16 nejčastěji provádí tyto činnosti [80]:

- Využití Internetu pro školní účely (85%).
- Hraní her (83%).
- Prohlížení obsahu produkovaného jinými uživateli (např. sledování videí, 76%).
- Komunikace (zejména v rámci sociálních sítí a IM, 62%).
- Zveřejňování a sdílení obrázků, fotografií (39%).
- Zveřejňování a sdílení zpráv (31%)
- Používání webkamery (31%)
- Návštěva stránek s datovými úložišti (18%)
- Trávení času ve virtuálním světě (16%)
- Psaní blogu (11%)

Jak je vidět z uvedeného přehledu, převládá využití Internetu pro studijní účely, díky čemuž Internet hraje významnou roli při vzdělávání. Ovšem v případě prohlížení obsahu produkovaného jinými uživateli, jakož i komunikace a následně i sdílení obrázků a zpráv, se jedná o rizikové činnosti. Rizikové zejména z toho důvodu, že jsou mezi dětmi hojně rozšířené a mohou být snadno zneužitelné.

Z uvedených informací je tedy možné odvodit, jaké předpoklady by produkt poskytující ochranu dětí na Internetu měl mít, tedy jaké by měly být jeho hlavní funkce:

- filtrování přístupu na webové stránky,
- filtrování obsahu komunikace,
- sdílení a poskytování osobních dat.

5.2 Stanovení kritérií a alternativ pro testování

Před testováním je nutné si stanovit kritéria, podle kterých budou produkty testovány a která budou sloužit k hodnocení vybraných alternativ.

5.2.1 Skupiny kritérií

Produkty pro zabezpečení ochrany dětí před nebezpečným obsahem Internetu, které splňují výše uvedené předpoklady, budu testovat podle následujících skupin kritérií. Některá kritéria je možné tematicky shrnout do jedné oblasti, ovšem každé kritérium působí na celkový výběr vlastní váhou.

Hlavní funkce produktu

V rámci této oblasti jsou testovány následující kritéria (funkčnosti produktu):

- filtrování, omezení přístupu na nevhodné stránky (K1),
- zabezpečení emailové komunikace (K2),
- zabezpečení komunikace prostřednictvím IM (K3),

- zabezpečení komunikace prostřednictvím sociální sítě (K4).

Součástí všech těchto kritérií bude také testování sdílení a poskytování osobních informací.

Vedlejší funkce produktu

Za vedlejší funkce považuji funkce, které nepřímo zajišťují ochranu, ale přesto jsou důležitou součástí takového produktu, zejména pro rodiče, kteří chtějí porozumět aktivitám svých dětí v prostředí Internetu a při práci s počítačem obecně. Za takové funkce je možné považovat následující:

- monitoring a reporting činností a času stráveného na Internetu (K5),
- řízení času stráveného na Internetu (K6).

Zabezpečení produktu

Oblastí zabezpečení je myšleno zabezpečení proti vnějšímu zásahu do produktu. Tedy pokusům funkce produktu obejít, nebo dokonce prolomit. V této oblasti budu testovat kritérium zabezpečení produktu (K7).

Cena produktu

Dalším kritériem důležitým pro následné rozhodování je cena produktu. Ačkoliv se může zdát, že cena v případě ochrany dětí je naprosto bezvýznamná, jelikož pro ochranu dětí jsou rodiče schopni obětovat nemalé prostředky, nelze vliv ceny produktu zcela eliminovat. Zjišťované ceny jsou uvedeny za roční licence (K8). Ceny produktů jsou zveřejněné jak v jednotkách měny Evropské měnové unie, EUR €, tak i v Amerických dolarech, USD $. Primárně budu používat měnu Evropské měnové unie, přičemž přepočet do této měny provedu prostřednictvím kurzů platných ke dni 26. 6. 2013[41].

5.2.2 Alternativy

Předpoklady uvedené v podkapitole 5.1 a dle výzkumu SIP-Benchmark II splňují 3 softwarové produkty, které jsem krátce představila již v kapitole 3.3:

- PureSight Owl (A1), společnosti PureSight Technologies Ltd.
- Kaspersky Pure (A2), společnosti Kaspersky Lab.
- Profil Parental Filter 2 (A3), společnosti Profil Technology.

5.3 Metriky pro testování

Testování produktů, tedy software, je vhodné provést podle odpovídajících norem. V současné době existuje Norma ISO/IEC 29119, která se zabývá přímo testováním software, ovšem tato norma je ještě ve fázi ověřování a schvalování odborníky[28]. Mimo této normy

jsou k dispozici již schválené normy ISO, které jsou zavedené i v rámci České soustavy norem (ČSN). Vývojem a kvalitou software se zabývají normy z řady ČSN ISO 9000. [60]

Hodnocení softwarových produktů se také přímo zabývá norma ČSN ISO/EIC 14598[11] Informační technologie – Hodnocení softwarového produktu, část 1 - 6. Tato norma pouze stanovuje postupy a metody hodnocení softwarového produktu. Zároveň se tato norma odkazuje na normu ČSN ISO/IEC 9126 Hodnocení softwarového produktu – Charakteristiky jakosti a návod pro jejich používání. V rámci této normy byl stanoven tzv. model jakosti, podle kterého je možné softwarové produkty hodnotit. V současné době norma ČSN ISO/IEC 9126 již není platná v rámci ČR a částečně ji nahrazuje norma ČSN ISO/IEC 9126-1 Jakost produktu. V této normě jsou definovány charakteristiky kvalitního software a také metriky pro určení jejich dosažení.

Další části normy, ISO/IEC 9126-2, ISO/IEC 9126-3 a ISO/IEC 9126-4, které nejsou v současné době vydané pod hlavičkou Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví, ale jsou mezinárodně uznávané, definují metriky, jejichž prostřednictvím je možné dané oblasti jakosti produktu hodnotit. Jedná se o tzv. interní, externí metriky a metriky jakosti v užití. Pro účel této práce využiji metriky obsažené v normě ISO/IEC 9126 - 4[27], Software engineering -- Product quality -- Part 4: Quality in use metrics (Metriky jakosti v užití). Tato norma jako cílovou skupinu uživatelů naměřených výsledků definuje zejména koncové uživatele, v druhé řadě tvůrce uživatelského rozhraní.

Jakost v užití měří jakost produktu, které dosahuje při použití různými druhy uživatelů pro různé scénáře práce. Z tohoto způsobu měření vyplývá, že hodnocení daného produktu se může lišit z hlediska různých koncových uživatelů. Zároveň je možné metriky této normy použít i pro měření jakosti produktu jako celku.[82]

V rámci metrik normy ISO/IEC 9126-4 provedu testování a měření z hlediska rodiče jako koncového uživatele. Budu tedy k hodnocení přistupovat jako rodič, který od daného produktu očekává splnění všech deklarovaných funkcí produktu v produktové dokumentaci nebo uživatelském manuálu.

Pro hodnocení jednotlivých kritérií produktu využiji charakteristiky uvedené v normě ISO/IEC 9126-4 (dále jen Norma)[27]:

- účinnost (effectiveness),
- výkonnost (productivity),
- bezpečnost (safety),
- spokojenost (satisfaction).

Každé z výše uvedených kritérií, v podkapitole 5.2.1 na straně 38, budu testovat podle těchto charakteristik. Hodnocení každého kritéria, mimo ceny, se tedy bude skládat z dalších částí, dle vybraných metrik. Měření provedená u jednotlivých metrik budou prováděna pouze jedním člověkem, je tedy možné, že pro některé metriky nebude dosaženo vypovídajících hodnot. Ovšem právě z důvodu, že měření provede jeden člověk, budou výsledky těchto měření vzájemně porovnatelné.

Metrika pro hodnocení účinnosti

Hodnocení účinnosti je metrika, která odpovídá na otázku „Jakého podílu z cílů úkolu je dosaženo správně“. Metrika se počítá dle následujícího vzorce:

$$M_1 = |1 - \sum_{i=1}^{n} A_i|, \qquad (1)$$

kde A_i váha nesprávně nebo neúplně vykonaného úkolu vzhledem k celkovému cíli. Například váha chybného filtrování obsahu webových stránek v prohlížeči Firefox vzhledem k celkovému cíli filtrování nebezpečného obsahu webových stránek. Norma udává rozsah této metriky $0<M_1<1$ přičemž hodnoty blížící se k 1 jsou dobrým výsledkem hodnocení. V případě, že suma vah překročí hodnotu 1, je hodnota M_1 rovna 0.[27]

Stanovení váhy je subjektivní a její určení závisí na dokumentaci, či manuálu pro daný produkt. V rámci této metriky tedy budu hodnotit, v jaké míře je schopný splnit deklarované funkce dle stanovených kritérií.

Metrika pro hodnocení výkonnosti

Výkonnost je možné hodnotit prostřednictvím několika metrik. Pro účel této práce použiji hodnocení času. Tato metrika odpovídá na otázku „Jak dlouho trvá dokončit úkol?“. Metrika je určena měřením času, který zabere daný úkol. Metriku je možné také vyjádřit vzorcem[27]:

$$X = T_a, \qquad (2)$$

kde T_a je čas potřebný pro vykonání úkolu. Jednotky času jsou sekundách. Pro tuto metriku se uvádí, že dobrým výsledkem je, pokud je naměřená hodnota T_a „malá“ (v tomto případě v řádech desítek sekund).[27] V rámci této metriky budu například zjišťovat nastavení produktu pro požadovaný typ filtrování, nebo blokování. Jelikož produkt testuje pouze jeden člověk, největší vypovídající hodnotu bude mít první měření. Další měření budou provedena s odstupem času pro zajištění nejmenšího možného rozptylu hodnot. Přestože tato metrika z předpokladu celého testování nemůže dosáhnout dostatečně vypovídající hodnoty, budou ze stejného předpokladu výsledky vzájemně porovnatelné.

Metrika pro hodnocení bezpečnosti

Bezpečností je v Normě myšlena bezpečnost lidí postižených používáním systému. Metrika stanovuje míru bezpečnosti systému, v tomto případě produktu, a vychází z počtu lidí, kteří používají software a z počtu lidí, kteří byli ohroženi nějakým nebezpečím při používání systému.

Z důvodu nesplnění podmínek pro testování kritéria bezpečnosti v této normě musím od testování tohoto kritéria upustit. Předpokladem kritéria je dostatečný počet jedinců, kteří by software testovali.

Metrika pro hodnocení spokojenosti

Metrika spokojenosti vyjadřuje postoj uživatele k používání produktu v daném kontextu použití. Metrika tedy hodnotí celkovou spokojenost uživatelů s produktem. Zjišťování spokojenosti uživatelů se provádí prostřednictvím vhodně sestavených dotazníků.[27]

Metriku a hodnocení spokojenosti z tohoto testování a hodnocení jsem nucena vynechat z důvodu nedostatku uživatelů, kteří by hodnotili vybrané produkty.

5.4 Příprava prostředí testování

Pro testování použiji virtualizační nástroj VMware 8.0., v rámci kterého instaluji operační zvolený operační systém. Tento nástroj umožňuje využívat více operačních systémů na jednom počítači, přičemž systémy instalované v rámci tohoto nástroje jsou pouze ve virtuálním prostředí. Tento nástroj jsem zvolila kvůli předchozí zkušenosti s ním.

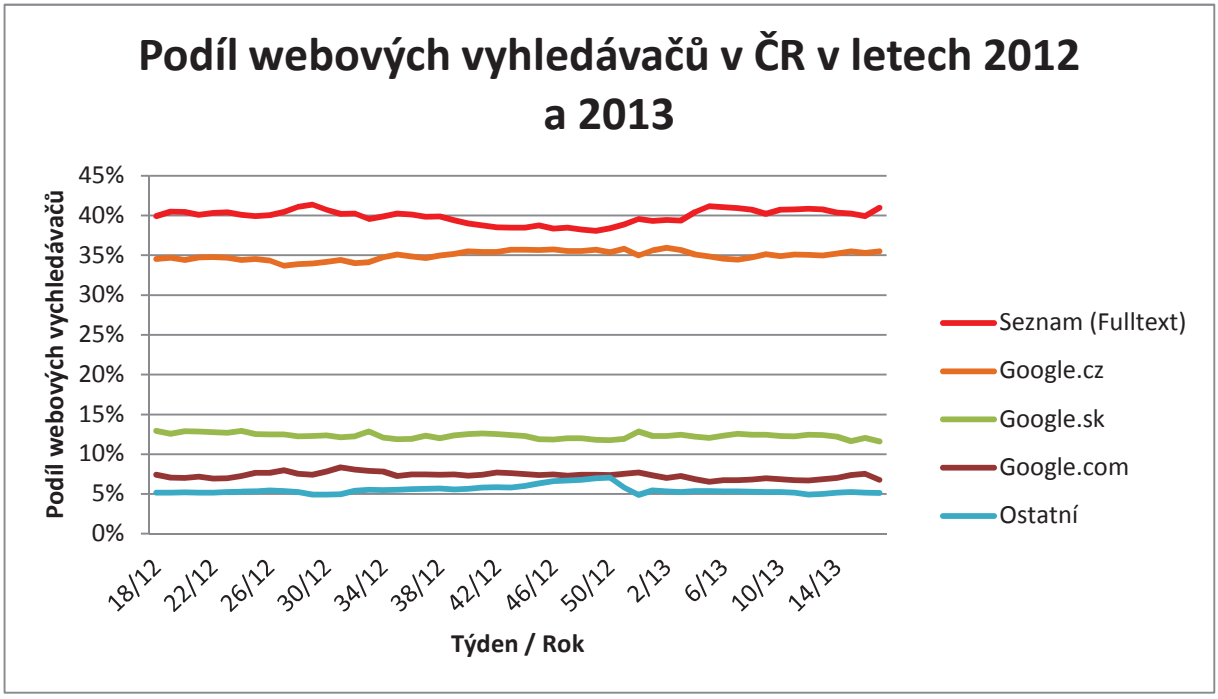
5.4.1 Operační systém

Jako operační systém pro testování jsem zvolila operační systém Windows 7 v české lokalizaci. Důvody pro zvolení tohoto systému vyplývají ze statistik společnosti Gemius [58], které zobrazuje Obrázek 1 na straně 23.

5.4.2 Emailový klient (schránka), webmail

Při výběru emailových klientů vycházím z nejpoužívanějších vyhledávačů v České republice, a které zároveň nabízí možnost zřízení webmailu. Prvním z těchto vyhledávačů je Seznam.cz, nabízející webmail na subdoménách seznam.cz, email.cz, post.cz, spoluzaci.cz, stream.cz a firmy.cz. Druhým vyhledávačem je Google.cz, který nabízí webmail na subdoméně gmail.com.

Tvrzení, že Seznam.cz a Google.cz jsou nejpoužívanějšími vyhledávači v České republice, vychází jak z výsledků výzkumů společností na českém trhu, které se zabývají SEO[70], tak i z mé dlouholeté pracovní zkušenosti. Například společnost Ataxo, která se zabývá nejen optimalizací pro vyhledávače a má více než desetiletou zkušenost v oboru, uvádí odhad podílu na vyhledávání v případě Seznam.cz 57%. V případě Google.cz je podíl 42%. Mimo vlastních zkušeností, společnost Ataxo vychází také ze statistik monitorovacího portálu Toplist.cz[70]. Obrázek 6 zobrazuje graf podílu vyhledávačů v ČR v týdnech v letech 2012 a 2013, tedy za dobu uplynulého roku. Celkem je dle serveru Toplist.cz[81] využíváno v České republice 19 webových vyhledávačů, přičemž v grafu jsou samostatně zastoupeny pouze vyhledávače s významným podílem. Další vyhledávače, jako jsou Bing.com, Centrum.cz nebo Atlas.cz jsou zahrnuty v součtu pod označením Ostatní. Z tohoto grafu jasně vyplývá, že Sezam.cz a Google.cz mají převahu nad ostatními vyhledávači.



Obrázek 6 - Podíl webových vyhledávačů v ČR v letech 2012 a 2013

Zdroj: vlastní dle[81]

V této podkapitole zanedbám využití emailových klientů typu MS Outlook nebo Thunderbird. Nepředpokládám totiž, že děti by využívaly těchto klientů, případně se dle mého názoru bude jednat o velmi malé procento dětí, kterým jej zřídili rodiče. Zanedbáním emailových klientů tuto skupinu nijak nevyřazuji. Filtrování obsahu emailu by na úrovni webmailu i emalového klienta mělo probíhat obdobně.

5.4.3 IM klient (služba)

IM (Instant Messaging) klient, je častým způsobem komunikace prostřednictvím Internetu. K tomuto způsobu online komunikace je nejprve nutné si založit účet u odpovídající služby. Často využívanými službami, které zároveň nabízí i vlastní IM klienty jsou ICQ, Windows live messenger nebo Skype. Tyto služby i klienti, mimo textové formy komunikace, nabízí také hlasovou komunikaci nebo komunikaci prostřednictvím online video přenosu.

Jelikož provozovatelé těchto komunikačních služeb neposkytují údaje o svých uživatelích, není možné přesně určit, která z těchto služeb je nejpoužívanější. Služba ICQ je přesto označována jako nerozšířenější služba pro synchronní komunikaci. Velkou konkurencí této službě jsou v současnosti sociální sítě, díky nimž počet uživatelů služeb ICQ a podobných, roste nižším tempem.[63] Pro provoz služby ICQ je možné používat různé klienty, než základní ICQ klient, jako jsou například Trillian, Miranda, Jaber, qip. Pro účely této práce budu ovšem uvažovat pouze základního klienta pro tuto službu, tedy klienta ICQ.

Služba Windows live messenger se v dubnu roku 2013 stala součástí služby Skype. Uživatelé, kteří dříve využívali služby Windows live messenger byli převedeni společností Microsoft na službu Skype.[47] Z tohoto důvodu pro testování zvolím pouze službu a klienta Skype.

5.4.4 Webový prohlížeč

Již z monitoringu prohlížečů v kapitole 3.2 vyplývá, že převahu na poli webových prohlížečů mají prohlížeče Firefox, MS Internet Explorer a v poslední době také Chrome. Při testování produktů tedy vycházím z těchto údajů a používám všechny tři zmíněné prohlížeče. Zejména pak z důvodu, že na jednom počítači je možné instalovat více těchto prohlížečů, které nemusí společně sdílet bezpečnostní politiku. Je tedy možné, že dítě se může pokusit obejít bezpečnostní funkce produktu tím, že spustí jiný prohlížeč.

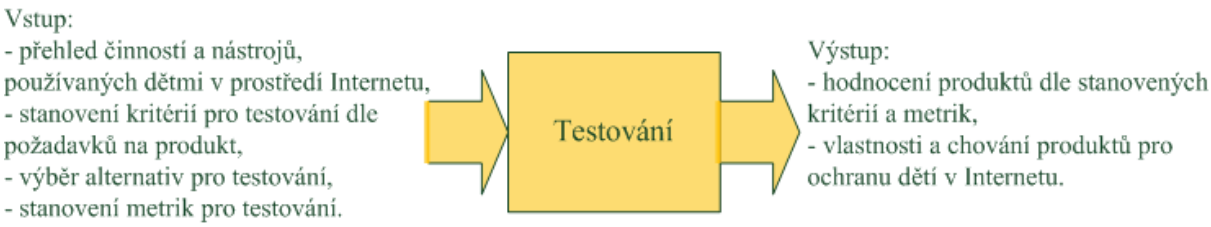
5.4.5 Sociální síť

Sociální síť je v dnešní době často využívaným zdrojem informací, nejen o lidech, které známe, ale také o různých událostech, apod. Zároveň se sociální sítě také staly novým komunikačním kanálem. Ačkoliv je registrace a užívání sociálních sítí zpravidla podmíněna minimálním věkem uživatelů, například v případě sociální sítě Facebook je minimální povolený věk uživatele 13 let[68], je toto pravidlo dětmi a jejich rodiči často porušováno.

Získat data o přesných počtech uživatelů vztažené k různým sociálním sítím je nemožné, jelikož provozovatelé těchto sítí informace o počtu svých uživatelů nezveřejňují. Pro účely této práce jsem vybrala pouze jednu sociální síť a to Facebook. Tuto sociální síť jsem vybrala na základě názoru odborníků v oblasti Internetu, že se jedná o jednu z nejčastěji používaných sociálních sítí v ČR[12].

6 TESTOVÁNÍ

V této části provedu testování vybraných produktů podle předem stanovených kritérií a za stanovených podmínek. Vstupem této části jsou výstupy vytvořené v předchozí části, tedy přehled činností a nástrojů, které děti používají v prostředí Internetu, kritéria dle kterých budu kritéria testovat a metriky, podle nichž budu daná kritéria hodnotit. Výstupem této části je hodnocení produktů dle jednotlivých kritérií, i záznam vlastností a chování produktů při testování. Přehled vstupů a výstupů jsem vyjádřila jako schéma, které zobrazuje Obrázek 7.



Obrázek 7 - Schéma vstupů a výstupů pro testování produktů

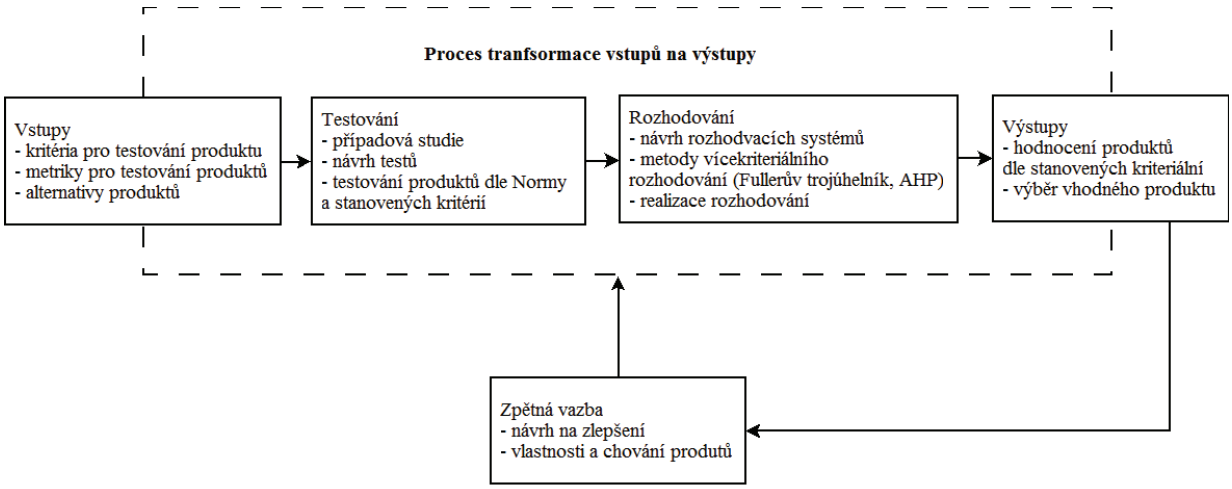
Zdroj: vlastní

Při testování budu využívat dokumentaci produktů, ve formě uživatelských manuálů. Důležitým aspektem této části je osoba, která testování provádí. Ačkoliv se jedná o produkty, které by měly chránit děti, z morálních důvodů je z této části vynechám. Předpokladem této práce je totiž fakt, že stávající produkty dostupné na trhu nejsou dokonalé a tudíž by i tato fáze testování mohla zavést děti tam, kde by mohlo vzniknout riziko jejich ohrožení. S ohledem na schopnosti a inteligenci dnešních dětí, jejich důvtip a vynalézavost je možné testování produktů provést i z pohledu dospělého člověka.

Cílem testování je zjistit chování produktů, jejich reakce, zda se chovají tak, jak udává jejich dokumentace a sestavení hodnocení produktů pro jednotlivá kritéria.

V rámci této kapitoly také uvedu významné aspekty chování všech produktů. Ačkoliv se svými vlastnostmi produkty příliš neliší, jejich chování na obdobné situace může být rozdílné.

Testování produktů a následný výběr vhodného produktu spolu úzce souvisí. Tento vztah lze vyjádřit prostřednictvím vhodně zvoleného schéma, které zobrazuje systém transformace vstupů na výstupy (Obrázek 8). Blok testování v sobě zahrnuje všechny činnosti nutné pro provedení testování, od vytvoření případové studie, přes návrh testů, až po samotné testování. Zpětná vazba systému v sobě zahrnuje návrh na zlepšení, který vychází, jak z výběru vhodné alternativy, tak z monitorování chování produktů.



Obrázek 8 - Schéma testování produktů a rozhodování o optimální alternativě

Zdroj: vlastní

6.1 Případová studie

Pro lepší demonstraci testování jednotlivých produktů jsem zvolila formu případové studie. V rámci této případové studie se pokusím napodobit činnosti chování dítěte v prostředí Internetu. Zvolila jsem fiktivní identitu žákyně 6té třídy, ve věku 12 let. Fiktivní žákyně se jmenuje Lenka Nováková. Dále budu označovat fiktivní žákyni pouze křestním jménem Lenka. Otcem Lenky je Pavel Novák, který bude používat produkty jako rodič, který chce tímto ochránit své dítě

V předchozí kapitole 5 jsem definovala programy a nástroje, které jakékoliv dítě může při práci s Internetem využívat. Některé nástroje je nutné registrovat, například emaily nebo účty komunikačních služeb IM. K tomu jsem využila právě výše zmíněnou fiktivní identitu. Při registraci některých služeb je nutné zadat věk uživatele. V některých případech, jako jsou například sociální sítě (konkrétně Facebook) je podmínkou užívání věk nejméně 13 let[69]. Tuto podmínku však lze snadno obejít a zadat nepravdivý rok narození, který podmínku splňuje.

Pro testování emailové komunikace jsem vytvořila fiktivní emailové účty u poskytovatelů Seznam.cz a Google.cz, jejichž výběr jsem zdůvodnila v kapitole 5.4.2 na straně 42. Pro založení nové emailové adresy Gmail na portálu Google.cz je nutné, mimo jiné, souhlasit se smluvními podmínkami společnosti Google. Tyto podmínky nijak neomezují minimální věk uživatele, pouze upozorňují, že se tato podmínka může vyskytnout u dalších služeb nabízených v rámci účtu Google. Přesto, při zadání věku Lenky, tedy 12 let, není možné účet Google vytvořit. Pro zdůvodnění zamítnutí registrace se společnost Google odkazuje na

pravidla COPPA[19][21]. Pro registraci účtu je nutné uvést věk nejméně 13 let, což je nejnižší možná hranice pro schválení účtu Google. Pro dokončení registrace účtu je nutné ověření prostřednictvím SMS, či hlasového volání. Po ověření je možné se přihlásit do služby Gmail.

V případě založení nové emailové adresy na Seznam.cz je postup obdobný. Zde je možné se prostřednictvím emailu přihlásit do různých služeb poskytovaných společností Seznam. Ve smluvním ujednání, jehož souhlas je součástí registrace emailu, není uvedeno věkové omezení. Při registraci je ovšem nutné vyplnit rok narození uživatele. Při zadání roku narození Lenky, tedy 2001, se nevyskytl žádný problém a účet byl schválen.

Pro testování komunikace prostřednictvím ICQ, jsem vytvořila nový účet v rámci této služby. Opět jsem při registraci použila smyšlené údaje o Lence. Registrací služby jsem mimo jiné souhlasila se Smlouvou koncového uživatele, ve které je uvedena klauzule o používání služby dětmi. Zaujala mne natolik, že zde uvedu její plné znění (s upravenou diakritikou)[43]:

Rodiče a zákonní zástupci, kteří chtějí svým dětem dovolit používat služby ICQ, by jim měli pomoci vytvořit si svůj vlastní účet ICQ a dohlížet na to, jak služby ICQ používají. Služby ICQ mohou zahrnovat obsah a funkce nevhodné pro děti. Je odpovědností rodičů a zákonných zástupců, aby dohlédli na způsob, jakým jejich děti využívají služby ICQ, a případně omezili používání služeb ICQ, které nejsou pro jejich dítě vhodné.

Jako poslední v řadě jsem registrovala účet, pro Lenku, ve službě Skype. Podmínky této služby jsou přísnější než podmínky služby ICQ. Obsahují klauzuli, která mimo jiné uvádí, že podmínky použití není oprávněna přijmout osoba, která nenabyla zákonného věku pro uzavření dohody se společností Skype[62]. Přesto jsem však Lence, v rámci této služby vytvořila účet.

6.2 Testování černé skříňky

Způsob testování, kterým budu ověřovat funkce jednotlivých produktů dle stanových kritérií, se nazývá dynamické testování černé skříňky. Tento způsob testování jsem zvolila zejména z důvodu, že pro testované produkty nejsou dostupné zdrojové kódy, tudíž nemohu testovat vnitřní procesy produktů. Dalším důvodem, proč je vhodné testovat produkty tímto způsobem je skutečnost, že touto cestou lze produkty testovat takovým způsobem, jak je mohou používat koncoví uživatelé.

K efektivnímu testování je potřeba mít k dispozici specifikaci produktů, tedy popis činností, které produkt má vykonávat. Testy, které lze provádět s ohledem na specifikaci

[19] Children's Online Privacy Protection Act[21]

produktu jsou tzv. funkční testy, které je možné rozdělit na testy splněním a testy selháním. Účelem testů splněním je zjistit, zda produkt poskytuje funkce dle specifikace a zda tyto funkce vykonávají deklarované činnosti. Naopak testy selháním slouží pro odhalení nefunkčních prvků produktu, nebo chyb, kterých se produkt dopouští provádění stanovených činností.[60]

6.3 Návrh testů

Pro všechny produkty je nutné navrhnout testy, které odpovídají reálným situacím při používání software. Jednotlivé testové situace jsou vždy shrnuty do jedné tematické oblasti dle stanovených kritérií testování navržených v kapitole 5.2.1. Testové situace, jejich obsah, vychází také z monitoringu produktů provedeného v kapitole 3.

6.3.1 Přístup na nevhodné webové stránky

Testování budu provádět prostřednictvím webových prohlížečů definovaných v kapitole 5.4.4. Pro testování přístupu na nevhodné webové stránky, tedy filtrování webových stránek budu volit různé kombinace možností nastavení, od přísného filtrování, při kterém má Lenka přístup pouze na povolené webové stránky až po různé kombinace mírného filtrování, při kterém jsou zakázány určité webové stránky přímo, nebo dle kategorie do které spadají.

Filtrování webových stránek mimo povolené

Tento způsob nastavení přístupu na webové stránky, tedy blokace všech stránek mimo seznam uživatelem vyplněných webových stránek, je nejpřísnějším režimem filtrování webových stránek. Pro účely tohoto testování zvolím pro Lenku jako přístupné následující webové stránky včetně jejich podstránek: Facebook.com, Google.cz. a Seznam.cz Tyto webové stránky jsem zvolila z toho důvodu, že chci Lence umožnit komunikaci se svými přáteli a také ji chci umožnit vyhledávat informace. Zároveň tím umožním kontrolu, nad informacemi, které chci Lence zpřístupnit. Blokování Lence sice umožní vyhledávat informace, ovšem o přístup na určité webové stránky, které jsou výsledkem vyhledávání, musí požádat rodiče.

Výsledkem požadované funkce produktů je blokování všech webových stránek mimo seznam povolených.

Filtrování webových stránek dle kategorií obsahu

U všech produktů budu testovat filtrování webových stránek dle kategorií obsahu. Jedná se o tzv. režim mírného filtrování, kdy jsou mezi blokované webové stránky zahrnuty všechny

běžné, riziko obsahující kategorie webových stránek, jako jsou například webové stránky s násilnou, gamblerskou či sexuální tematikou. Ostatní webové stránky, které nespadají do těchto kategorií, budou pro Lenku běžně přístupné.

Očekávaným výsledkem funkce produktů je blokování webových stránek spadajících svým obsahem do nastavených kategorií filtrování webových stránek.

Filtrování vybraných webových stránek

Dalším nastavením je režim, při kterém se využívá kombinace blokování kategorií webových stránek a seznamu povolených či vyloučených webových stránek definovaných rodičem. V tomto případě budu včetně kategorií uvedených v předchozí části blokovat i sociální sítě. Přesto však vytvořím výjimku pro Facebook, jelikož Lenka tuto síť používá pro komunikaci s kamarády. Tímto nastavením zamezím, aby si vytvářela profil, nebo přistupovala na jiné sociální sítě. Dále pro rodiče není žádoucí, aby si Lenka do počítače stahovala nebo vyhledávala obsah, který byl nelegálně umístěn na tzv. veřejná úložiště, kterými jsou například portály Ulozto.cz, Rapidshare.com, a fóra, která zveřejňují odkazy pro stažení tohoto obsahu, jakými jsou například Warcenter.cz a Warforum.cz. Zahrnu je tedy do seznamu vyloučených webových stránek. Ačkoliv by bylo možné zakázat veškerá fóra a stahování veškerého obsahu, neučiním tak, jelikož by toto nastavení mohlo postihnout veškerá fóra a stahování veškerého obsahu.

Výsledkem úspěšného filtrování by mělo být umožnění přístupu Lenky pouze na sociální síť Facebook a zamezení přístupu na jiné sociální sítě, dále zamezení přístupu na vyloučené webové stránky a webové stránky zahrnuté do blokovaných kategorií.

6.3.2 Emailová komunikace

V rámci testování emailové komunikace budu testovat možné situace, které mohou nastat při využívání emailu Lenkou. Jak jsem již uvedla v kapitole 5.4.2, pro testování využiji pouze webmail, tedy přístup k emailové schránce prostřednictvím webových stránek.

O možnosti filtrování obsahu emailu jsem v uživatelském manuálu všech testovaných produktů objevila minimum informací, nebo žádné, které by udávaly, zda je možné blokování obsahu emailu, nebo zda je možné filtrovat, nebo blokovat konkrétní emaily na základě jejich obsahu a na základě odesílatele, respektive jeho umístění v adresáři webmailu. V uživatelském manuálu u dvou ze tří produktů je pouze zmínka o tom, že je možné blokovat přístup na webmail jako takový. Ve své podstatě takové blokování může být řešením ochrany emailové komunikace, jelikož v případě zavedení omezení na jeden konkrétní účet, si Lenka

bez vědomí rodičů může založit jinou webmailovou schránku, kterou již rodiče nemusí mít pod dohledem.

Přesto však zahrnu filtrování obsahu a blokování emailové komunikace do návrhu testů. Toto filtrování může být zahrnuto v definici blokovaných slov, definovaných v rámci produktů s účinností na webové stránky. Veškeré testování budu provádět prostřednictvím prohlížečů zvolených v kapitole 5.4.4. a webmailů v kapitole 5.4.2.

Blokování emailů dle obsahu

V rámci testování emailů dle obsahu budu odesílat na emailové adresy Lenky (lenka.novakova01@email.cz a lenka.novakova01@gmail.com) emaily obsahující nevhodný obsah, jako jsou například emaily obsahující vulgární výrazy, výrazy odkazující se na násilí, obsah s explicitními výrazy v oblasti sexuální tematiky, ale také emaily s přílohami, včetně instalovatelných souborů s příponou *. exe, atd. Obdobně budu testovat blokování odeslání takových emailu z emailových adres Lenky.

Výsledkem správného fungování produktu by mělo být blokování otevření emailu, případně zablokování webové stránky s otevřenou emailovou zprávou a blokování stažení přílohy.

Blokování přístupu na webmail

V rámci testování přístupu na webmail budu testovat, zda je možné se přihlásit do emailové schránky prostřednictvím webového prohlížeče. Testování budu provádět pomocí zvolených poskytovatelů webmailu, které Lenka používá, a také prostřednictvím zvolených prohlížečů.

Výsledkem správné funkce produktů by mělo být zablokování webové stránky s emailovou schránkou, tedy stránkou, která se objeví po přihlášení do webmailu.

6.3.3 Komunikace prostřednictvím IM

Při testování komunikace prostřednictvím IM, využiji služby a jejich výchozí klienty uvedené v kapitole 5.4.3, tedy službu a klienta ICQ a službu a klienta Skype.

Přidání nového kontaktu

V rámci obou zvolených služeb a klientů je možné nastavit omezení přijímání zpráv, video či audio hovorů od kontaktů, které nejsou v adresáři daného účtu služby. Taková komunikace je zpravidla možná v případě, že je kontakt uveden v adresáři. Z tohoto důvodu budu tedy testovat blokování přidání nového kontaktu do adresáře v obou zvolených klientech.

Správným výsledkem funkce produktů by měla být blokace akce přidání kontaktu do adresáře klienta.

Blokování vybraných slov

Při používání komunikace prostřednictvím IM je důležité filtrování určitý výrazů, které nejsou vhodné pro komunikaci Lenky. Ať již v případě, že tyto výrazy do komunikace vnáší sama Lenka, či jsou Lence posílány druhou osobou. Tyto výrazy jsou buď již předem definované, nebo je rodič stanoví sám.

Produkty by v tomto případě blokovaná slova měly nahradit zástupnými znaky nemající žádný význam v komunikaci prostřednictvím IM, nebo daná slova skrýt, či zamezit jejich odeslání.

6.3.4 Komunikace prostřednictvím sociální sítě

Komunikace prostřednictvím sociálních dalším z komunikačních kanálů, jejichž filtrování a blokaci budu testovat. Pro testování jsem v kapitole 5.4.5 zvolila sociální síť Facebook. Testování provedu prostřednictvím Lenčina profilu v síti Facebook, pod jménem Lenka Nováková.

Blokování vybraných slov

Pro testování blokování vybraných slov předpokládám přítomnost nastavení blokovaných slov používaných jak v synchronní, tak asynchronní komunikaci. Testování provedu při komunikaci s přáteli, kteří mohou komunikovat prostřednictvím chatu, a při komunikaci s cizími lidmi, kteří Lence mohou posílat zprávy, aniž by byli jejími přáteli. V obsahu komunikace použiji slova, která jsem označila jako blokovaná.

Blokování zpráv od uživatelů

Další možností ochrany komunikace v prostředí sociální sítě je blokování komunikace směřované k/od určitých uživatelů. Při testování budu simulovat jak komunikaci s přáteli Lenky, tak komunikaci mimo seznam jejích přátel.

6.3.5 Monitoring a reporting činností a času stráveného na Internetu

Možnost kontroly činností Lenky v prostředí Internetu je důležitou součástí produktu pro další nastavení produktů. Monitoring a reporting poskytují informace o tom, jaké webové stránky Lenka navštěvuje a kolik času tráví v prostředí Internetu. Z těchto informací je možné

dále vyvodit, jaké webové stránky je nutné dále zakázat, nebo naopak povolit, a jak je vhodné upravit omezení času po který má Lenka povoleno přistupovat na Internet.

Monitoring a reporting přístupu na nevhodné stránky

Testování monitoringu a reportingu přístupu na nevhodné stránky zahrnuje přehled webových stránek, které Lenka navštívila, nebo se pokusila navštívit, přičemž jí byl přístup produktem povolen nebo zamítnut.

Úspěšným výsledkem testování by měl být podrobný přehled o navštěvovaných webových stránkách, pravidelný reporting o navštívených webových stránkách a reporting o pokusech navštívit zakázané nevhodné stránky.

Monitoring a reporting o komunikaci prostřednictvím emailu

Při testování monitoringu a reportingu komunikace prostřednictvím emailu budu testovat zaznamenávání pokusů Lenky přihlásit se do emailové schránky, je-li tento způsob komunikace zakázán. V případě, že má Lenka povoleno přihlásit se do své emailové schránky prostřednictvím webmailu, budu testovat zaznamenávání a reportování pokusů Lenky o otevírání, čí posílání emailů s nevhodným obsahem, ať již ve formě textu, nebo ve formě příloh.

Očekávaným výsledkem testování je zaznamenávání a reportování všech pokusů o přístup do blokovaného webmailu. V případě, že není blokace zavedena, monitorování a reportování o emailech s nevhodným obsahem.

Monitoring a reporting o komunikaci prostřednictvím IM

V rámci monitoringu a reportingu o komunikaci prostřednictvím IM budu testovat možnost sledování a reportování pokusů o použití služeb IM, které byly zakázány. Součástí testování je také sledování a reportování používání, případně pokusů o použití vyloučených slov pro IM komunikaci.

Výsledkem testování by mělo být zaznamenávání a reportování všech pokusů o spuštění zakázaných IM klientů (služeb) a použití, případně pokusy o použití vyloučených slov.

Monitoring a reporting o komunikaci prostřednictvím sociálních sítí

Monitoring a reporting týkající se komunikace prostřednictvím sociálních sítí otestuji posíláním zpráv obsahující blokovaná slova, na profil Lenky a naopak z profilu Lenky. Zároveň budu testovat možnost sledování aktivit, které Lenka na sociální síti provádí.

Očekávaným výsledkem testování je získání informací a upozornění o užití blokovaných slov a také výpis aktivit, které Lenka na sociální síti provádí.

Monitoring a reporting času stráveného v prostředí Internetu

Jednotlivé produkty budu testovat v oblasti monitoringu a reportingu času stráveného v prostředí Internetu takovým způsobem, že budu simulovat situaci, kdy se Lenka pokouší přistupovat do sítě Internetu i přes zavedené časové omezení. Dále budu testovat, zda součástí monitoringu a reportingu je i záznam času, který Lenka trávila v prostředí Internetu bez ohledu na jeho omezení.

Výsledkem úspěšného testování je přehled informací o čase, který Lenka strávila v síti Internetu.

6.3.6 Řízení času stráveného na Internetu

Nastavení času, po který může Lenka přistupovat k Internetu je vhodné zejména, pokud rodič nemůže Lenku neustále kontrolovat. Testovat budu přístup k Internetu prostřednictvím webových prohlížečů zvolených v kapitole 5.4.4 a také komunikaci prostřednictvím služeb IM zvolených v kapitole 5.4.3, které po posílání zpráv využívají sítě Internet.

Přístup na webové stránky

Při testování časového omezení přístupu na webové stránky nastavím pro každý den časové rozmezí, během kterého si Lenka může prohlížet webové stránky. Ve všední dny od 16:00 do 20:00 a o víkendu od 14:00 do 21:00.

Výsledkem úspěšného testování by měla být situace, kdy má Lenka v určených hodinách povolený přístup na webové stránky a v okamžiku uplynutí nastaveného času bude Lence přístup zakázán.

Komunikace prostřednictvím IM

Nastavení časového omezení pro komunikaci prostřednictvím služeb IM bude obdobné jako v předchozím případě, budu tedy testovat nastavení omezení komunikace ve všední dny na dobu od 16:00 do 20:00 a o víkendu na 14:00 a 21:00.

Přípustným výsledkem testování je omezení povolené komunikace na stanovený čas a zamezení použití služeb v okamžiku uplynutí povoleného času.

6.3.7 Zabezpečení produktu

Součástí produktů na ochranu dětí v prostředí Internetu by měla být i funkce, která chrání produkt samotný před možností deaktivace či odebrání produktu z operačního systému.

Ochrana nastavení produktu

V oblasti ochrany nastavení produktu budu testovat možnost nastavení hesla a dalšího zabezpečení pro zvolené filtrování a omezení. A zároveň budu simulovat pokusy Lenky o změnu tohoto nastavení.

Požadovaným výsledkem této funkce je ochrana nastavení heslem, případně jiným zabezpečeným způsobem a ochrana proti pokusům změnit nastavení produktu bez řádné autorizace.

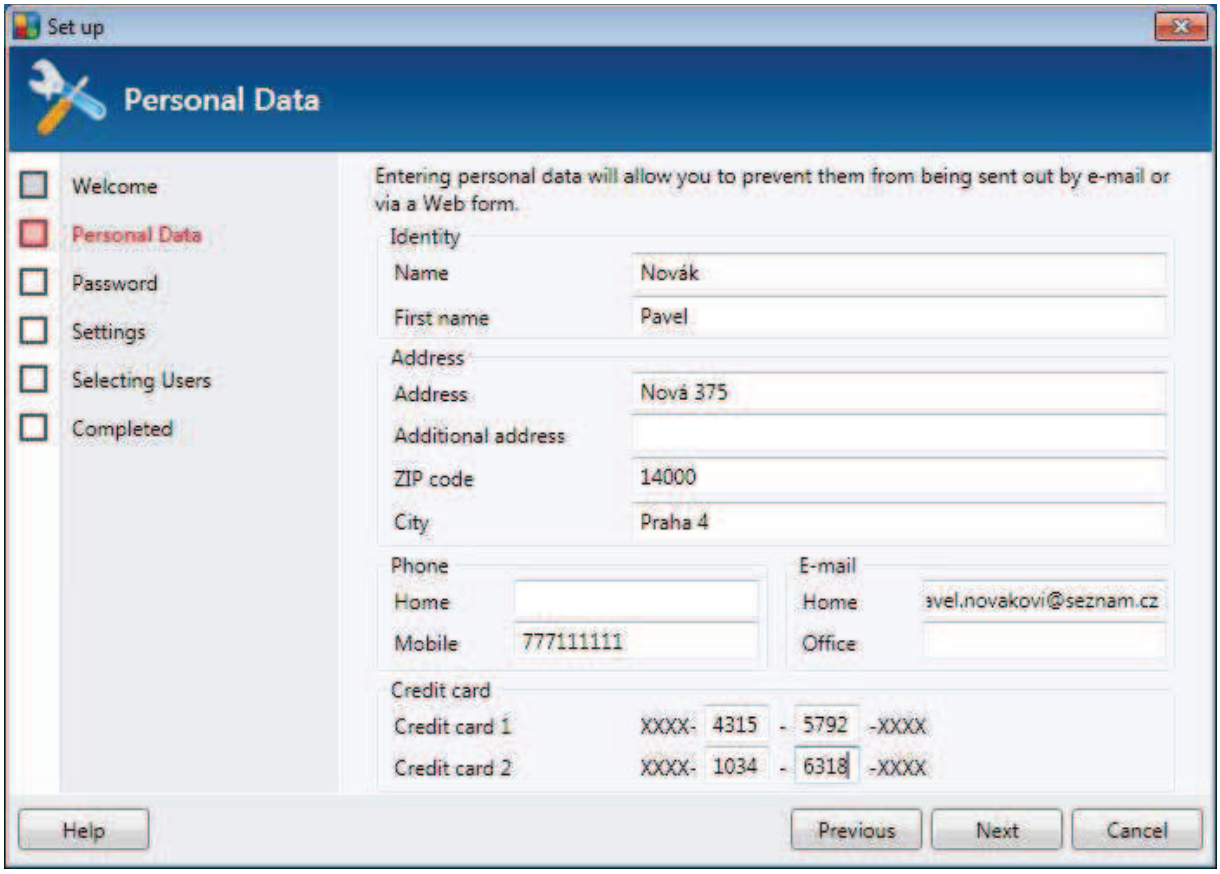
Ochrana odebrání produktu

V případě ochrany odebrání produktu budu testovat možnosti nastavení ochrany odebrání produktu a zároveň simulovat situaci, při které se Lenka snaží produkt odebrat z operačního systému.

Výsledkem testování by mělo být nastavení ochrany produktu proti jeho odebrání z operačního systému a účinná ochrana před pokusem o odebrání.

6.4 Testování produktu Profil Parental Filter 2

Při instalaci produktu je uživatel požádán o sdělení osobních informací, jako jsou jméno, adresa, telefonní číslo, email, ale také čísla platebních karet. V úvodu tohoto dialogu je uvedeno, že vyplněním těchto informací se uživatel chrání před možností jejich zveřejnění, jak zobrazuje Obrázek 9.



Obrázek 9 - Formulář pro zadání osobních údajů - Profil Panretal Filter 2

Zdroj:[66]

Pro vyplnění tohoto formuláře jsem použila smyšlená data o Pavlu Novákovi. V dalším kroku produkt žádá zvolení hesla k ochraně produktu. Zároveň také nabízí možnost nastavení jeho spuštění automaticky při startu operačního systému, nebo na vyžádání. Z těchto možností jsem zvolila spuštění automaticky při startu operačního systému. V následujícím kroku produkt vyžaduje informaci o počtu dětí a příslušné věkové skupiny, které mají přístup k Internetu. V rámci tohoto nastavení jsem vytvořila profil Lenky a zároveň jsem jejímu profilu přiřadila i heslo.

6.4.1 Přístup na nevhodné webové stránky

Produkt umožňuje podrobnější filtrování dle kategorií obsahu. Pro zvolenou kategorii je možné zvolit úroveň filtrování, která je vyjádřena škálou věku dítěte. Tedy například v případě stánek spadajících do kategorie násilí je možné zvolit úroveň filtrování pro děti do 12 let, od 12 do 15 let, atd. Dokumentace produktu však přesně neuvádí, v čem spočívá rozdíl mezi těmito úrovněmi. Domnívám se, že produkt rozlišuje frekvenci slov na webové stránce spadající do této kategorie. V kapitole 6.4.3 podrobněji uvádím filtrování dle seznamu

blokovaných slov, který je platný jak pro komunikaci prostřednictvím IM, tak i pro filtrování webových stránek.

Pro úspěšné filtrování webových stránek mimo povolené by bylo nutné do seznamu povolených webových stránek ještě zahrnout výjimku pro login.szn.cz, kde se nachází emailová schránka poskytovatele Seznam.cz a výjimku pro Google.com, kde se nachází emailová schránka Google Gmail. Produkt nesprávně filtroval podstránky těchto poskytovatelů.

Při testování blokování sociálních sítí a nastavení výjimky pro Facebook.com produkt Lence umožnil přístup na tuto sociální síť, zakázal přístup na zahraniční sociální sítě, jako jsou Linkedin.com či Twitter.com, ovšem dovolil Lence přístup na české sociální sítě, jako jsou například Lide.cz nebo Libimseti.cz.

Při testování jsem byla nucena vynechat testování prostřednictvím prohlížeče Chrome. V kompatibilitě produktu jsem našla informaci, o kompatibilních prohlížečích, přičemž mezi podporovanými prohlížeči jsou Internet Explorer, Mozilla a Opera[66]. Prohlížeč Chrome není tedy podporován, což se při testování projevilo tím, že vždy ohlásil pád a vyžadoval restart prohlížeče, který ovšem problém nevyřešil.

6.4.2 Emailová komunikace

Při testování blokování na webmail produkt dovolil Lence přistoupit k oběma webmailovým schránkám, na Seznam.cz a Google.cz. Produkt nabízí možnost blokování obsahu přílohy emailu, jehož nastavení je sdílené i pro webové stránky a stahování souborů. Přesto však neobstál při blokování emailů podle obsahu a dovolil Lence odeslat a přijmout prostřednictvím webmailu email, který obsahoval různé typy příloh, které byly označeny jako vyloučené. Ze specifikace není jasné, zda toto nastavení je funkční jak pro webmail, tak i pro emailového klienta.

6.4.3 Komunikace prostřednictvím IM

Produkt nabízí možnost, při zadávání blokovaných slov, jejich seskupení dle tématu a také podrobnější nastavení filtrovaní slov s ohledem na frekvenci jejich výskytu. Nastavení blokovaných slov je platné jak pro komunikaci prostřednictvím IM, tak pro filtrování webových stránek. Toto nastavení může být výhodné zejména, pokud některé webové stránky, jsou podle názoru rodiče bezpečné, ale přesto vyloučené slovo obsahují pouze v několika málo výskytech. Při zadávání vyloučených slov jsem ovšem zjistila, že produkt není schopný pracovat korektně s češtinou, respektive se znaky s diakritikou. Při pokusu

o zadání slov s diakritikou, administrace produktu tzv. „spadne“ a není možné v zadávání pokračovat bez restartování počítače. Z tohoto důvodu jsem zadala slova bez diakritiky, ovšem produkt při blokaci těchto slov selhal, i když se vyskytovala ve stejném tvaru, ve kterém jsem je do seznamu vyloučených slov zapsala.

Produkt umožňuje nastavení blokovaných kontaktů ve službě MSN, což je služba Windows Live messenger, která byla nahrazena službou Skype. Toto nastavení by tedy mělo být platné i pro službu Skype. V průběhu testování se však ukázalo, že tomu tak není a produkt umožnil Lence přidat kontakt, který byl uveden ve vyloučeném seznamu a to jak v případě ICQ, tak i Skype. Vyloučená slova pro komunikaci produkt ignoroval úplně.

6.4.4 Komunikace prostřednictvím sociální sítě

Produkt neumožňuje podrobnější filtrování komunikace prostřednictvím sociálních sítí, než pouhé jejich zakázání. Komunikaci prostřednictvím sítě tedy nijak neblokoval, ačkoliv by se měl řídit seznamem blokovaných slov stanovených pro filtrování webových stránek nebo pro komunikaci prostřednictvím IM.

6.4.5 Monitoring a reporting činností a času stráveného na Internetu

Produkt neumožňuje nastavení monitoringu a reportingu komunikace prostřednictvím emailu, zaměřuje se pouze na všeobecné nastavení monitoringu a reportingu. Monitoring času stráveného na Internetu je již automaticky nastavený a zapnutý při spuštění produktu. Produkt umožňuje monitorování přístupu na nevhodné stránky a poskytuje podrobné reporty o navštívených stránkách včetně informace, zda se jednalo o blokovanou stránku. Dále poskytuje informace o době strávené na webové stránce.

Přestože produkt zaznamenává navštívené webové stránky, nijak nerozlišuje, zda šlo o webovou stránku s webmailem. Nijak tedy nemonitoruje komunikaci prostřednictvím emailu, nenabízí tedy reporty o tomto způsobu komunikace, stejně tak jako v případě komunikace prostřednictvím sociální sítě. Naopak produkt poskytuje informace o spuštěných programech, tedy včetně klientů ICQ a Skype. Nemonitoruje však komunikaci jako takovou, pouze zda a jak dlouho byl program používán.

Monitoring a reporting času stráveného v prostředí Internetu je součástí monitoringů a reportů o webových stránkách a použitých službách. Přehled o čase produkt zobrazuje formou koláčového grafu, přičemž každý segment je přidělen webovým stránkám seskupených dle subdomény. Zobrazuje však celkový čas, podrobnější přehled neumožňuje.

Souhrnný report o navštívených webových stránkách a o času stráveném prohlížením webových stránek zobrazuje Obrázek 10.

Obrázek 10 - Přehled navštívených webových stránek - Profil Parental Filter 2

Zdroj:[66]

6.4.6 Řízení času stráveného na Internetu

V případě nastavení časového omezení, produkt po uplynutí stanoveného času zablokoval připojení k Internetu. Neumožnil tedy Lence jak přístup na webové stránky, tak i komunikaci prostřednictvím IM klientů. Zároveň také Lenku upozornil, že uplynul čas, po který měla povoleno přistupovat k Internetu.

6.4.7 Zabezpečení produktu

Veškerá nastavení produktu jsou chráněna heslem. Zároveň produkt umožňuje blokování přístupu do systémových funkcí. Lenka tedy omezen přístup do systémových služeb, jako je například nastavení času nebo do ovládacích panelů, jejichž prostřednictvím je možné ze systému Windows produkt odebrat. Odebrání produktu je možné ještě prostřednictvím odkazu

umístěným v nabídce Start ve složce produktu. Při pokusu o odebrání produktu tímto způsobem si produkt vyžádal heslo rodiče. Jelikož Lenka nezadala správné heslo, produkt jí odebrání neumožnil. Stejně tak se pokoušela o jeho ukončení prostřednictvím Správce úloh přístupném po stisknutí kombinace kláves CTRL +ALT + DEL. Tento pokus Lenky také nebyl úspěšný, produkt zablokoval přístup do Správce úloh.

6.5 Testování produktu PureSight Owl

PureSight Owl je produkt společnosti PureSight Technologies Ltd. Produkt je lokalizován do anglického jazyka. Na webových stránkách je možné získat dokumentaci produktu ve formě uživatelského manuálu (http://onlinechild.puresight.com/onlinehelp/1/en/index.html). Tento manuál, stejně jako produkt je v anglickém jazyce a popisuje, jaké funkce produkt poskytuje a také jak dané funkce ovládat. Z této specifikace dále vycházím při testování, kdy ověřuji, zda deklarované funkce poskytují ochranu dětem před nebezpečným obsahem Internetu, respektive do jaké míry je produkt dokáže ochránit.

Při instalaci je nutné zároveň vytvořit uživatelský účet. Instalace probíhá ve čtyřech krocích. V prvním kroku zadá uživatel svůj email, v druhém nastaví heslo pro správu produktu a kontrolní otázky pro obnovu ztraceného hesla. Zároveň má uživatel možnost změnit umístění instalovaného produktu. V dalším kroku produkt nabízí nastavení PureSearch jako výchozího poskytovatele vyhledávání a zároveň také nastavení PureSearch jako domovské stránky webových prohlížečů.[71]

6.5.1 Přístup na nevhodné webové stránky

Produkt umožňuje filtrování dle kategorií obsahu, a to webové stránky spadající do těchto kategorií[71]:

- s pornografickou tematikou, včetně webových stránek, které se zabývají seznamování za účelem budování romantických vztahů (tzv. online seznamky),
- s tematikou zabývající se závislostí,
- sociální sítě,
- fóra a chaty,
- obsahující násilí,
- se sportovní a herní tematikou,
- s tematikou zabývající se nakupováním.

Při testování přístupu na nevhodné webové stránky provedl správně filtrování českých webových stránek v případě filtrování dle zvolené kategorie. V jednom případě (http://www.rozzlobenimuzi.com) ovšem povolil Lence vstoupit na webovou stránku, která

svým obsahem spadá hned do několika kategorií filtru. Přesto však v okamžiku, kdy by Lenka chtěla zobrazit konkrétní obsah (video, článek, fotografii), produkt tuto webovou stránku zablokoval. Při testování omezení přístupu pouze na konkrétní webové stránky, tedy filtrování webových stránek mimo povolené, produkt dovolil Lence navštívit z webové stránky Seznam.cz, webové stránky Novinky.cz. Zde však Lence nedovolil přejít na konkrétní obsah (článek, fotografie, video).

V případě testování filtrování vybraných webových stránek, produkt Lence zamezil, přihlášení k sociální síti Lide.cz a zablokoval také přístup k další české síti Libimseti.cz. Blokování dalších sociálních sítí jako Google+, Linkedln.com a Twitter.com proběhlo bez problémů. Blokování přístupu k vyloučeným webovým stránkám proběhlo bezchybně.

6.5.2 Emailová komunikace

V testování blokování přístupu na webmail produkt neobstál. Přesto, že jsem kategorii webmail zahrnula do vyloučených kategorií webových stránek, produkt Lence umožnil přihlásit se ke svému účtu jak poskytovatele Seznam.cz, tak Google. com.

6.5.3 Komunikace prostřednictvím IM

Pro nastavení blokování nového kontaktu je nutné, přidat stávající kontakty, jejich ID do seznamu povolených kontaktů. Následně je možné tento seznam uzamknout a zamezit tak přidávání nových kontaktů do seznamu v rámci klienta ICQ. Ačkoliv uživatelský manuál produktu deklaruje filtrování komunikace prostřednictvím IM, v případě klienta Skype umožňuje pouze blokování tohoto klienta[72]. Zároveň také tento manuál deklaruje funkce filtrování komunikace a blokování kontaktů, které jsou v seznamu vyloučených kontaktů, pro klienta ICQ. Pro testování této funkce jsem použila verzi klienta 7.0, která je v seznamu kompatibility uvedený jako podporovaná[73]. Přesto však při zapnuté funkci filtrování IM, nebylo vůbec možné službu ICQ spustit. ICQ klienta bylo možné spustit, ale služba byla offline. Díky tomuto zjištění nebylo možné testovat blokování vybraných slov a produkt v tomto testu neobstál.

6.5.4 Komunikace prostřednictvím sociálním sítě

V rámci sociálních sítí nabízí produkt pouze monitoring, není tedy možné blokovat zprávy od určitých uživatelů. V uživatelském manuálu tvůrci produktu uvádějí možnost nastavení monitorování činností v sociální síti Facebook.[72] Propojení produktu a Lenčina profilu ovšem nebylo funkční.

6.5.5 Monitoring a reporting činností a času stráveného na Internetu

Produkt umožňuje monitorování navštívených webových stránek a jejich přehled zobrazuje v podrobném reportu. Součástí reportů je možnost filtrování historie procházení webových stránek podle povolených či zamítnutých. Dále reporty zobrazují, kolikrát byla daná webová stránka Lenkou navštívena a kolik z těchto přístupů bylo blokováno. Report neumožňuje zobrazení času, který Lenka na dané webové stránce strávila. Produkt nemonitoruje komunikaci prostřednictvím emailu, neposkytuje tak reporty o této činnosti.

Přestože filtrování komunikace prostřednictvím klienta ICQ nefunguje korektně, produkt monitoruje komunikaci prostřednictvím klienta. Reporty nabízejí informace o času stráveném komunikací prostřednictvím ICQ, rodičům také umožňuje nahlédnout do textu komunikace s konkrétním kontaktem. Zobrazuje také výstrahy ke slovům uvedených v seznamu vyloučených slov.

Produkt monitoruje čas strávený v prostředí Internetu, umožňuje jej v reportu rozdělit na čas strávený prohlížením webových stránek, čas strávený komunikací prostřednictvím IM a čas strávený stahováním dat do počítače. Nezobrazuje čas od-do, ale využití tzv. denní kvóty, tedy kolik času z daného dne Lenka strávila v prostředí Internetu.

6.5.6 Řízení času stráveného na Internetu

Řízení času, po který má Lenka povolen přístup na webové stránky, a času po který má povolenou komunikaci prostřednictvím IM, fungoval bez problémů. V okamžiku uplynutí stanoveného času, produkt zamezil Lence prohlížení webových stránek a veškerou komunikaci prostřednictvím IM.

6.5.7 Zabezpečení produktu

V oblasti ochrany nastavení produktu je možné zvolit různá hesla pro rodiče a pro dočasné povolení přístupu na webové stránky. Pokud Lenka bude znát heslo, které jí umožní dočasné zpřístupnění webové stránky, nebude moci prostřednictvím tohoto hesla změnit jiná nastavení produktu.

Produkt je chráněn proti odebrání z operačního systému heslem rodiče a to při všech možných pokusech o jeho odebrání. Zároveň také umožňuje nastavení zasílání zpráv o manipulaci se soubory produktu. Samozřejmostí je také možnost změny tohoto hesla, ovšem po přihlášení do administrace produktu. Nastavení produktu probíhá prostřednictvím webového rozhraní, které je chráněno heslem uživatele.

Jelikož je produkt ve zkušební 30-ti denní verzi pro testování nepoužitelný, zakoupila jsem si měsíční licenci tohoto produktu.

Cenu roční licence produktu jsem uvedla již kapitole 3.3.2, tedy 59,90 $. Abych mohla cenu produktu porovnat s ostatními produkty, je nutné ji vyjádřit ve stejné měně. Přepočet, podle kurzu ČNB ze dne 26.6.2013[41], je 46,06 €.

6.6 Testování produktu Kaspersky Pure

V rámci instalace produktu nebylo vyžadováno žádné nastavení, které by se týkalo vytváření profilu uživatele, nebo vytváření uživatelského účtu. Při instalaci produkt informoval uživatele o možnosti využití Kaspersky Security Network (v překladu Bezpečnostní síť Kaspersky), která pomáhá zlepšit úroveň ochrany před malware.[33]

6.6.1 Přístup na nevhodné webové stránky

Produkt neumožňuje nastavení kombinace filtrování webových stránek v režimu filtrování podle kritérií a zároveň filtrování webových stránek uvedených v seznamu povolených/blokovaných webových stránek.

Při testování filtrování webových stránek mimo povolené byl produkt příliš striktní, zejména při vyhledávání webových stránek prostřednictvím vyhledávače Seznam.cz. Produkt neumožnil zahrnout podstránku, na které se nacházejí výsledky vyhledávání, mezi povolené webové stránky. Naopak při vyhledávání pomocí vyhledávače Google.cz pracoval produkt správně a zobrazil stránku s výsledky vyhledávání.

Při testování filtrování webových stránek dle kategorií obsahu produkt nedokázal správně filtrovat české webové stránky. Umožnil Lence například navštívit webové stránky rozzlobenimuzi.com, které obsahují explicitní obsah, který spadá hned do několika blokovaných kategorií. Také Lence umožnil prohlížet si nevhodné obrázky, videa a články umístěné na těchto webových stránkách. Naopak v případě zahraničních webových stránek provedl produkt filtrování správně.

V případě nastavení filtrování webových stránek dle kategorií není možné zároveň nastavit i dodatečné filtrování dle seznamu vyloučených blokovaných stránek. Přesto však při filtrování sociálních sítí byl produkt schopen rozpoznat české sociální sítě a Lence tak odepřel přístup například na Libimseti.cz či Lide.cz.

6.6.2 Emailová komunikace

Při testování blokování webmailu produkt selhal. Umožnil Lence se přihlásit do obou webmailů, tedy jak ke schránce na Seznam.cz, tak ke schránce na Google.cz. Stejně tak neobstál při blokování emailu dle obsahu.

6.6.3 Komunikace prostřednictvím IM

Produkt umožňuje sestavení seznamu blokovaných slov, která dle rodiče nejsou vhodná pro komunikaci Lenky. V případě blokování vyloučených kontaktů IM produkt povolil odeslání i příjem zprávy k/od blokovaného kontaktu, v obou případech ovšem byla vždy doručena prázdná zpráva.

6.6.4 Komunikace prostřednictvím sociální sítě

Přestože produkt deklaruje v uživatelském manuálu možnost nastavení blokování zpráv od určitých uživatelů, při opakovaném testování se mi nepodařilo tuto funkci nastavit. Produkt nedetekoval žádný z kontaktů sociální sítě Facebook a tudíž nenabídl možnost blokovat konkrétní kontakty, či komunikaci jejich komunikaci.

6.6.5 Monitoring a reporting činností a času stráveného na Internetu

Produkt umožňuje monitoring přístupu na nevhodné webové stránky, formou reportů poskytuje kompletní přehled a zobrazuje také počet pokusů o přístup na blokované webové stránky. Neumožňuje však monitoring a reporting o komunikaci prostřednictvím emailu. Veškerá příchozí a odchozí pošta prostřednictvím webmailu tedy není monitorována.

Produkt monitoruje komunikaci prostřednictvím IM služeb a poskytuje reporty o komunikaci s konkrétními kontakty. Zároveň také umožňuje nahlédnout do obsahu komunikace. V případě zadání blokovaných slov, produkt zaznamená použití tohoto slova a jeho výskyt i frekvenci výskytu zobrazí v přehledu.

Monitorování času využití Internetu se automaticky provádí spuštěním produktu. Přehled o činnostech je rozdělen na úseky povoleného a zamítnutého přístupu z hlediska času. Zobrazuje počet a také délku trvání jednotlivých připojení k Internetu.

6.6.6 Řízení času stráveného na Internetu

Produkt neumožňuje omezení času pro komunikaci prostřednictvím IM, ovšem umožňuje nastavení času, po který je možné používat počítač. Blokování přístupu na webové stránky produkt provedl bezchybně. Jakmile uplynul stanovený čas, pro který Lenka měla povolený

přístup k Internetu, produkt okamžitě přístup zablokoval, respektive zablokoval webovou stránku, na kterou se Lenka, po uplynutí stanoveného času, pokoušela vstoupit. Zároveň tím také zablokoval veškeré připojení k Internetu, tedy i prostřednictvím služeb IM. Produkt obstál i při pokusu obejít toto omezení. Lenka změnila systémový čas na čas, který se pohybuje v povoleném pásmu, přesto však jí přístup k Internetu povolen nebyl.

6.6.7 Zabezpečení produktu

Nastavení filtrování a blokování je chráněno heslem, které je možné změnit, ovšem po zadání původního hesla. Produkt neumožňuje nastavení hesla pro dočasný přístup na blokované webové stránky. Stejně je chráněno i odebrání produktu z operačního systému.

Při pokusu Lenky změnit nastavení produktu a při pokusu odebrání produktu, Kaspersky Pure obstál. Vždy vyžadoval heslo a bez jeho zadání neumožnil žádné úpravy, ani odebrání produktu.

Cenu roční licence produktu jsem uvedla již kapitole 3.3.3 tedy 75,95 $. Abych mohla cenu produktu porovnat s ostatními produkty, je nutné ji vyjádřit ve stejné měně. Přepočet, podle kurzu ČNB ze dne 26.6.2013[41], je 61,38 €.

6.7 Shrnutí testování

Testování produktů dle stanovených kritérií probíhalo 2 měsíce. Při testování produktů dle kritéria Normy výkonnost jsem jednotlivé testy prováděla vždy s časovým odstupem pro zajištění relevantnosti výsledků. Testování jsem ukončila po desátém testování každého produktu. Pro ověření, zda je vhodné ukončit testování výkonnosti produktů jsem si z naměřených hodnot každého testovacího případu, každého kritéria, spočítala směrodatnou odchylku. Ve všech případech byla hodnota směrodatné odchylky nižší, než hodnota 0,05, kterou jsem si stanovila jako maximální přípustnou hodnotu směrodatné odchylky.

Při testování jsem zjistila několik odchylek produktů od jejich uživatelských manuálů. V několika případech v manuálu byla uvedena a popsána funkce, která při testování nefungovala dle popisu, tedy chybně i z hlediska bezpečnosti dětí, nebo nepracovala vůbec.

Produkt Profil Parental Filter 2 neuspěl při testování situace přidání nového kontaktu v testu kritéria filtrování komunikace prostřednictvím IM. Dále produkt neuspěl při testování komunikace prostřednictvím sociální sítě a při monitorování komunikace prostřednictvím emailu a sociálních sítí.

Stejně jako produkt Profil Parental Filter 2, ani PureSight Owl neuspěl při testování filtrování komunikace prostřednictvím sociální sítě. Tvůrci produktu v uživatelském manuálu uvádí jako novinku produktu možnost monitorování činností na sociální síti Facebook[71]. I přes několik pokusů, zahrnující reinstalaci produktu, úpravu Facebookového profilu a komunikaci s podporou produktu se mi nepodařilo tuto funkci spustit. Produkt tak při testování monitoringu komunikace prostřednictvím sociální sítě nesuněl.

Produkt Kaspersky Pure při testování také vykázal některé nedostatky v souladu s uživatelským manuálem. Zejména pak v případě testování komunikace prostřednictvím sociální sítě. V uživatelském manuálu tvůrci deklarují možnost monitorování komunikace prostřednictvím sociálních sítí i možnost blokace konkrétních kontaktů[33]. Ovšem tuto funkci se mi nepodařilo spustit. Konzultovala jsem tento problém s podporou produktu, nebyli ovšem schopni mi s řešením problému pomoci.

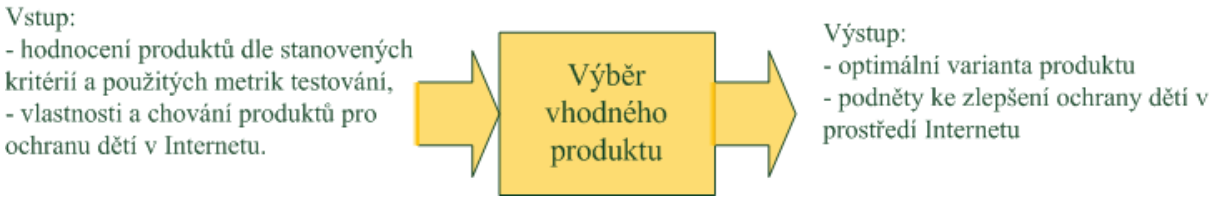
Z hodnot naměřených při testování produktů dle kritéria výkonnost jsem musela určit souhrnnou hodnotu T_a, pro jednotlivá kritéria. Její hodnotu jsem získala použitím váženého průměru, přičemž první měření mělo nevyšší váhu a poslední nejnižší.

Při testování produktů dle kritéria Normy účinnost, produkty vždy nedosáhly stejných hodnot. Provedla jsem stejný počet pokusů, jako v případě testování produktů dle kritéria Normy výkonnost. Výsledky se v několika případech lišily, ačkoliv produkty prováděli testované funkce vždy se stejným výsledkem. Cílem testování produktů dle kritéria účinnost bylo stanovit váhu nesprávně nebo neúplně vykonaného úkolu vzhledem k celkovému cíli. Stanovení vah A_i je založeno na subjektivním hodnocení splnění, či nesplnění cílů z pohledu testera. Z tohoto důvodu se mohou výsledky tohoto testování lišit. Pro zajištění vypovídající hodnoty výsledků dle kritéria účinnost jsem zaznamenala všechny určené váhy z každého testování. Dle doporučení Normy, jsem ke stanovení výsledné hodnoty váhy, použila median. Výsledným hodnocením produktů dle kritéria účinnost je hodnota M_I, která se vypočítá dle vzorce (1).

7 VÝBĚR VHODNÉHO PRODUKTU

Z nasbíraných dat testování produktů, jejichž přehled je uveden v příloze B a v příloze C, vyberu vhodnými metodami optimální variantu produktu pro zabezpečení přístupu dětí k nevhodnému obsahu Internetu, pro kterou navrhnu zlepšení. Výběr optimální alternativy provedu na základě kritérií, uvedených v kapitole 5.2.1 na straně 38, z variant, které jsem stanovila v bodě 5.2.2 na straně 39. Pro samotný výběr použiji tzv. vícekriteriální rozhodování.

Vstupem do procesu rozhodování jsou výsledky získané z testování v předchozí kapitole. Schéma jejich transformace na výstupy zobrazuje Obrázek 11.



Obrázek 11 - Schéma vstupů a výstupů pro výběr vhodného produktu

Zdroj: vlastní

V kapitole 5.2.1 definovala 8 kritérií a z dostupných alternativ vybrala 3 vhodné produkty. Pro rozhodování je možné použít ovšem pouze 7 kritérií. Při testování žádný z produktů neuspěl v testování zabezpečení komunikace prostřednictvím sociální sítě (K4) dle kritéria Normy výkonnost. Pro rozhodování jsem nucena toto kritérium vynechat, jelikož z testování nejsou dostupné relevantní hodnoty.

Pro řešení rozhodovacího problému využiji dvě metody rozhodování pro porovnání výsledků těchto metod. Na základě výběru vhodného produktu navrhnu zlepšení, formou modelu, při použití tohoto produktu.

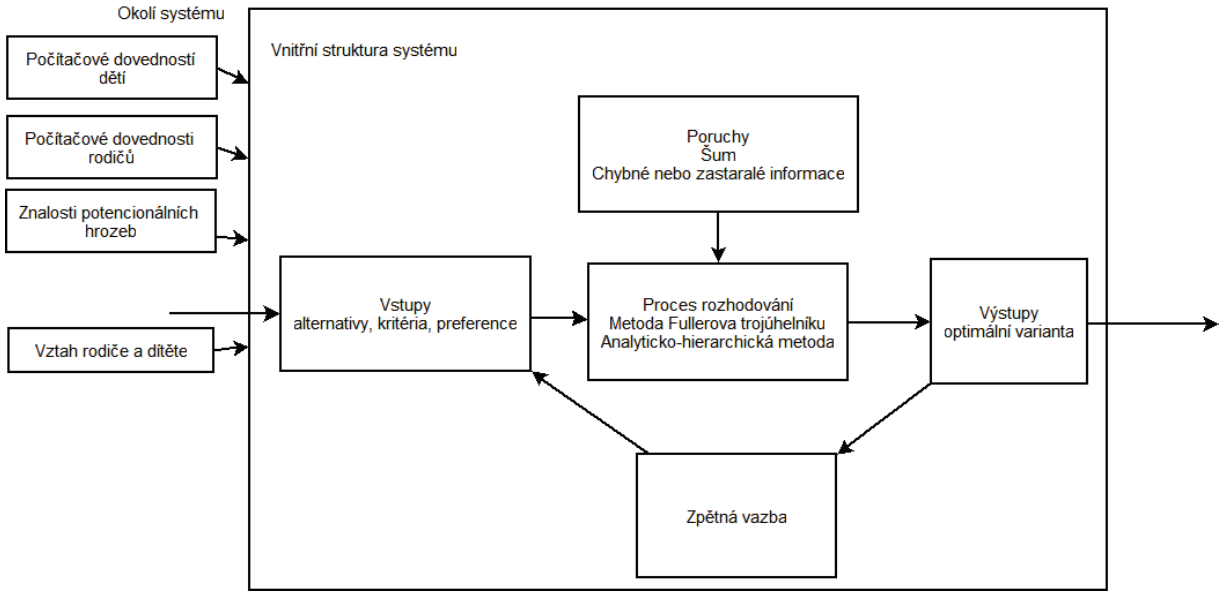
7.1 Rozhodovací systém

Rozhodovací problém, pro výběr vhodného produktu pro ochranu dětí v prostředí Internetu, je možné definovat jako rozhodovací systém nebo rozhodovací proces. Systém obecně se sestává z prvků systému, vazeb, okolí, struktury a chování[39]. Rozhodovací systém je pak modifikací obecného systému a je vyjádřen následujícím vztahem[38]:

$$RS = \{A_n, K_m, R(n*m), v_m\}, \qquad (4)$$

kde: *An* jsou alternativy, *Km* jsou kriteria, **R** (n×m) je matice reálných hodnot *RS* s prvky {*r*11, *r*12, …, *r*1*m*; *r*21, *r*22, …, *r*2*m*; …; *rn*1, *rn*2 , …*rnm*} a *vm* jsou váhy jednotlivých kriterií.

Rozhodovací systém je možné vyjádřit graficky. Obrázek 12 zobrazuje strukturu rozhodovacího systému, vztahy mezi prvky a okolí systému. Uvedený obrázek je platný pro oba rozhodovací systémy rozdělené dle kritérií Normy.



Obrázek 12 - Rozhodovací systém

Zdroj: vlastní

Okolí systému tvoří znalosti a schopnosti dětí a rodičů, které není možné přímo ovlivnit, přesto však také mohou nepřímo ovlivňovat rozhodovací systém. Důležitou součástí okolí rozhodovacího systému je také vztah rodiče a dítěte. Důležitý je zejména z toho důvodu, že pokud mají rodiče a děti dobrý vztah a zároveň děti chápou obavy rodičů z rizik v prostředí Internetu, mohou se chovat v tomto prostředí takovým způsobem, že existující riziko mohou zmírnit, ne-li téměř eliminovat.

7.2 Řešení rozhodovacího problému

Metody, které v této práci použiji pro řešení rozhodovacího problému výběru vhodného produktu, pro ochranu dětí před nevhodným obsahem Internetu, vyžadují stanovení vah kritérií. Tyto váhy jsou někdy také označovány jako koeficienty významnosti. Z tohoto označení plyne, že v rámci použitých metod budou kritériím hodnocení přiřazena významnost, jinak také důležitost. S významem kritéria roste také jeho váha a naopak, v případě méně významného kritéria je jeho váha nižší.[16] Pro řešení rozhodovacího

problému použiji 2 metody, v rámci kterých stanovím váhy pro jednotlivá kritéria a ohodnocení pro zvažované alternativy.

Z hlediska nesourodosti porovnávaných hodnot, které jsou výsledkem testování dle Normy, uvedené v kapitole 5.3, rozdělím rozhodovací problém do dvou rozhodovacích systémů. První systém bude zaměřen na rozhodování podle kritéria účinnost, druhý systém bude zaměřen na rozhodování dle kritéria výkonnost.

7.2.1 Metoda Fullerova trojúhelníku

Metoda Fullerova trojúhelníku pro stanoví vah kritérií, je metodou tzv. párového srovnávání. Účelem této metody je zjištění preferenčních vztahů dvojic kritérií. Preferenční vztahy jsou určeny počtem preferencí vzhledem ke všem ostatním kritériím obsaženým v rozhodovacím problému. Rozhodovatel, tedy ten, který řeší rozhodovací problém, ke každému kritériu přiřadí preferenci, v závislosti k jinému kritériu. Stanoví tak tedy, jestli je dané kritérium významnější než druhé, a to tím způsobem, že významnějšímu kritériu přiřadí hodnotu 1, méně významnému pak hodnotu 0.

Údaje o preferencích, tedy 0 a 1 se zapíší do čtvercové matice *n* x *n*, kde *n* je počet kritérií rozhodovacího problému. Součet preferencí každého kritéria je označen f_i. Ze získaného počtu určíme normované váhy kritéria v_i podle vztahu[16]:

$$v_i = \frac{f_i}{\sum_{i=1}^{n} f_i}. \tag{5}$$

V případě, že počet preferencí určitého kritéria je nulový, čímž bude nulová i jeho váha, je nutné normované váhy vypočítat podle následujícího vztahu[16]:

$$v_i = \frac{f_i+1}{n+\sum_{i=1}^{n} f_i}. \tag{6}$$

Počet preferencí, uvedený ve jmenovateli ve vztahu (6), se určí podle následujícího vztahu[16]:

$$\sum_{i=1}^{n} f_i = \frac{n*(n-1)}{2}. \tag{7}$$

Ohodnocení kritérií

Ohodnocení kritérií, tedy stanovení jejich vah, jsem provedla na základě vzájemného porovnání párů kritérií a posouzení jejich důležitosti. Jak jsem uvedla v úvodu této kapitoly, pro rozhodování lze použít pouze 7 kritérií. Tabulka 1 zobrazuje seznam kritérií, která budou vstupovat do metody Fullerova trojúhelníku.

Tabulka 1 - Kritéria rozhodovacího problému

Označení	Kritérium
K1	Filtrování, omezení přístupu na nevhodné stránky
K2	Zabezpečení emailové komunikace
K3	Zabezpečení komunikace prostřednictvím IM
K5	Monitoring a reporting činností a času stráveného na Internetu
K6	Řízení času stráveného na Internetu
K7	Zabezpečení produktu
K8	Cena produktu

Zdroj: vlastní

Výše uvedená kritéria mohou být jak výnosového, tak nákladového typu. V případě kritéria Normy účinnost jsou kritéria K1 – K7 výnosového typu, žádoucí jsou hodnoty blížící se k 1. Naopak dle kritéria Normy výkonnost, jsou kritéria K1 – K7 nákladového typu a žádoucí jsou v tomto případě hodnoty blížící se k nule. Výjimkou je kritérium K8 - cena, které je za všech okolností nákladového typu.

Váhy výše uvedených kritérií jsem vypočítala dle vzorců (6) a (7) na základě sestaveného párového porovnání kritérií, které zobrazuje Tabulka 2. Z uvedeného je patrné, že největší váhu má kritérium K7. Rozložení vah jsem pro lepší transparentnost zobrazila graficky, které zobrazuje Příloha D.

Tabulka 2 - Výsledek párového porovnávání kritérií

	K1	K2	K3	K5	K6	K7	K8	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
K1		1	1	1	1	0	1	5	0,2381	0,2143
K2	0		0	0	0	0	1	1	0,0476	0,0714
K3	0	1		0	1	0	1	3	0,1429	0,1429
K5	0	1	1		1	0	1	4	0,1905	0,1786
K6	0	1	0	0		0	1	2	0,0952	0,1071
K7	1	1	1	1	1		1	6	0,2857	0,2500
K8	0	0	0	0	0	0		0	0,0000	0,0357

Zdroj: vlastní

Ohodnocení alternativ

Při hodnocení alternativ vycházím z hodnot získaných testováním produktů. Zároveň alternativy porovnávám v páru a alternativa, která vzhledem k danému kritériu, oproti druhé alternativě, dosahuje lepších hodnot, udělím bod 1, alternativě s horší hodnotou udělím hodnocení 0. Alternativy vždy proti sobě porovnávám v rámci jednoho kritéria. Výsledkem

ohodnocení alternativ je tedy čtrnáct tabulek s ohodnocením alternativ dle příslušných kritérií, které jsou uvedeny v příloze E a v příloze F.

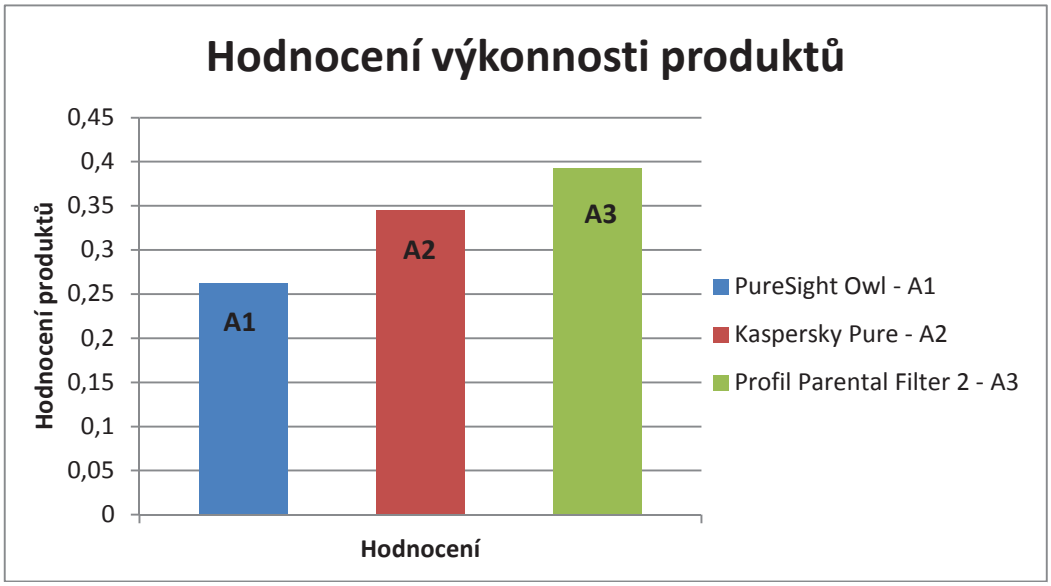
Hodnocení výkonnosti

Ze získaných hodnot párového porovnávání kritérií a alternativ získáme optimální variantu. Optimální alternativa, je taková alternativa, jejíž celkové skóre v tomto rozhodovacím procesu, nejvyšší. Skóre lze vypočíst jako násobek váhy kritérií a násobek vah jednotlivých alternativ pro daná kritéria dle vzorce (8):

$$H^j = \sum_{i=1}^{m} (v_i * h_i^j), \qquad (8)$$

hledám tedy alternativu s $(H^j)_{max}$. [38]

Výsledné dosažené skóre kritéria výkonnost zobrazuje Obrázek 13. Jako nelépe hodnocená alternativa se jeví produkt Profil Parental Filter 2.

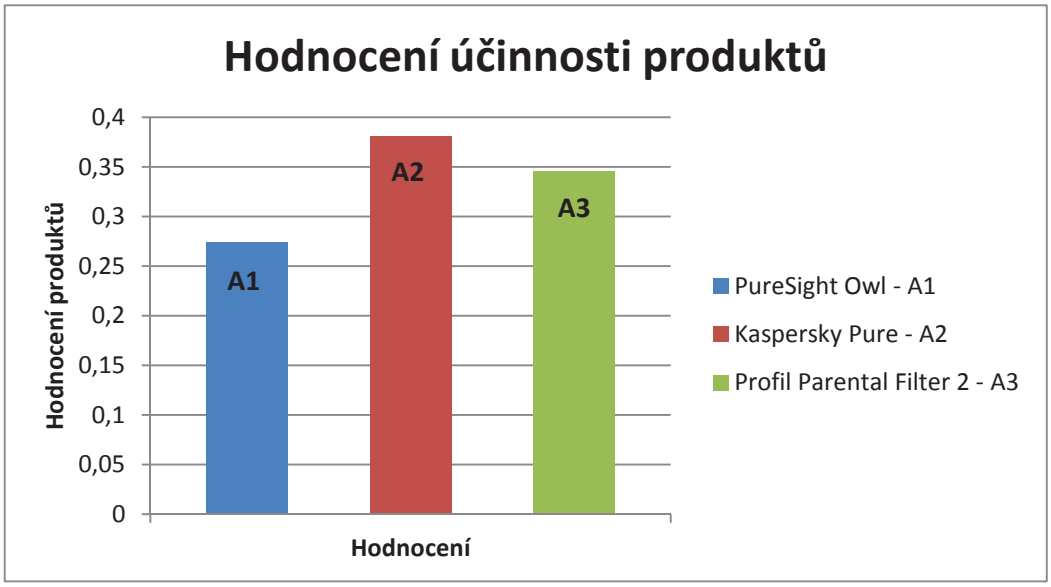


Obrázek 13 - Dosažné skóre produktů metodou Fullerova trojúhelníku - výkonnost

Zdroj: vlastní

Hodnocení účinnosti

Druhým rozhodovací systém jsem zaměřila na výběr optimální varianty podle kritéria účinnosti. Optimální variantu jsem určila obdobně jako v předchozím případě pomocí výpočtu výsledného skóre hodnocení produktů dle vzorce (8). Výsledný přehled skóre zobrazuje Obrázek 14. V tomto případě dosáhl lepšího skóre produkt Kaspersky Pure.



Obrázek 14 - Dosažné skóre produktů metodou Fullerova trojúhelníku - účinnost

Zdroj: vlastní

7.2.2 Analyticko-hierarchická metoda

Analyticko-hierarchická metoda, označována zkratkou AHP, je založena na Saatyho metodě párového srovnávání kritérií. Pro sestavení hierarchie rozhodovacího problému a výpočet hodnocení produktů jsem využila software Criterium Decision Plus (CDP). Tento software jsem vybrala na základě předchozí zkušenosti.

Hierarchie rozhodovacího problému

Pro řešení rozhodovacího problému metodou AHP jsem si sestavila hierarchickou strukturu H, která uvedena v příloze G. Struktura H se skládá ze tří úrovní, první je cíl rozhodování, druhou jsou kritéria rozhodování a poslední úrovní jsou alternativy.

Ohodnocení kritérií

Pro ohodnocení kritérií jsem použila tzv. Saatyho stupnice relativních důležitostí. Škálu a význam jednotlivých lingvistických hodnot zobrazuje Tabulka 3.

Tabulka 3 - Škála relativních důležitostí

Intenzita relativních důležitostí	Definice důležitostí
1	stejná
3	slabá
5	silná
7	prvotřídní
9	absolutní
2, 4, 6, 8	mezihodnoty

Zdroj: [37]

Saatyho matice kritérií

Z výše uvedené tabulky hodnocení jednotlivých kritérií jsem vytvořila Saatyho matici, prostřednictvím které jsou vzájemně porovnávány páry kritérií, které uvádí Tabulka 1. Jednotlivé prvky matice jsou vypočítány jako přibližné podíly jednotlivých preferenčních hodnocení, jak znázorňuje rovnice (9)[37].

$$s_{ij} \approx \frac{vi}{vj}, \text{ pro i, j = 1, 2, ..., m.} \quad (9)$$

Ohodnocení důležitosti kritérií jsem vytvořila na základě vlastního uvážení důležitosti požadavků na optimální produkt v oblasti ochrany dětí na internetu, s přihlédnutím na věk dítěte. Následně jsem vypočítala relativní váhy kritérií a normované váhy kritérií. Hodnoty S_i, R_i a v_i byly vypočteny podle vzorců (10), (11) a (12)[37].

$$S_i = \prod_{j=1}^{m} Sij \, . \quad (10)$$

$$R_j = (S_i)^{1/m} \, . \quad (11)$$

$$v_i = \frac{R_j}{\sum_{i=1}^{m} R_j} \, . \quad (12)$$

Výsledky párového porovnávání a jednotlivé váhy kritérií zobrazuje Tabulka 4.

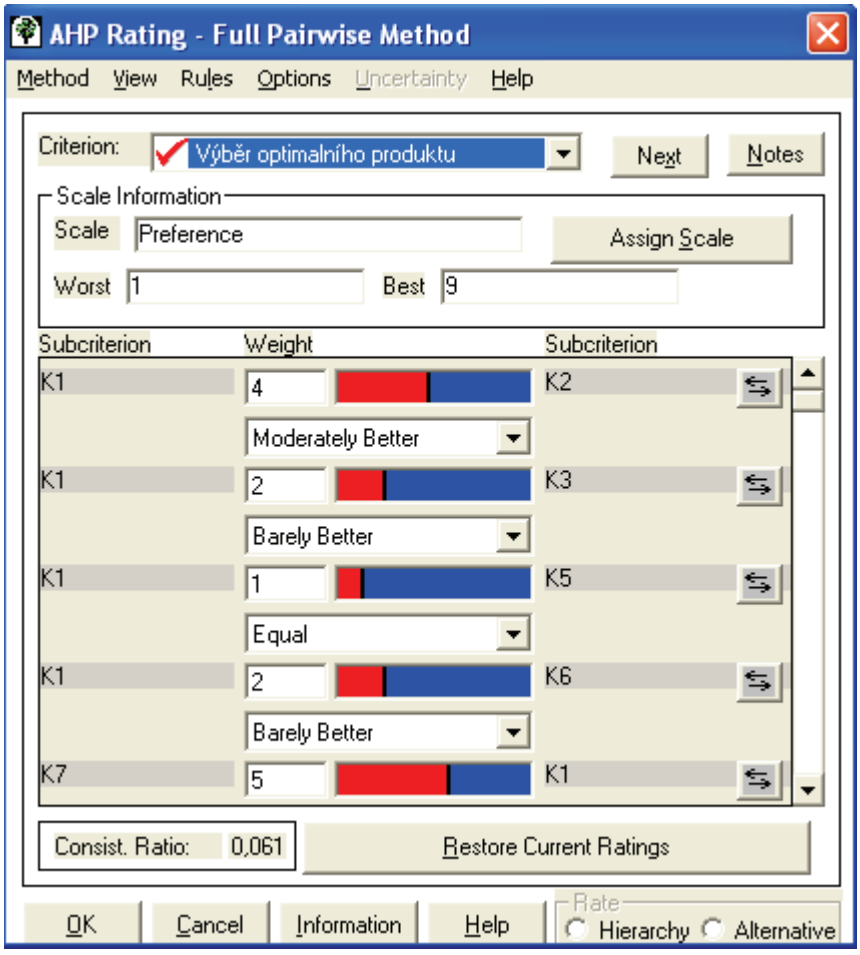
Tabulka 4 - Saatyho matice párového porovnávání kritérií

	K1	K2	K3	K5	K6	K7	K8	S_i	R_i	v_i
K1	1	4	2	1	2	1/5	7	22,400	1,559	0,158
K2	1/4	1	1/5	1/3	1/4	1/7	1	0,001	0,346	0,035
K3	1/2	5	1	1/2	3	1/5	5	3,750	1,208	0,123
K5	1	3	2	1	2	1/3	5	20,000	1,534	0,156
K6	1/2	4	1/3	1/2	1	1/5	5	0,333	0,855	0,087
K7	5	7	5	3	5	1	7	18375,000	4,066	0,413
K8	1/7	1	1/5	1/5	1/5	1/7	1	0,000	0,288	0,029

Zdroj: vlastní

Tuto matici jsem sestavila pro kontrolu, zda získané hodnoty vah Saatyho metodou přibližně odpovídají vahám získané metodou Fullerova trojúhelníku. Z uvedeného je zřejmé, že pořadí vah je u obou metod stejné. Pro práci s nástrojem CPD není nutné vypočítat váhy, nástroj tento výpočet provede sám, přičemž zároveň také vypočte konzistenční index Saatyho matice. Konzistenční index se používá pro ověření, zda byla Saatyho matice správně sestavená. Hodnota konzistenčního indexu musí být menší nebo rovna 0,1. Obrázek 15

zobrazuje preferenční škály jednotlivých kritérií vůči druhým a zároveň také v levém dolním rohu uvádí konzistenční index roven 0,061.



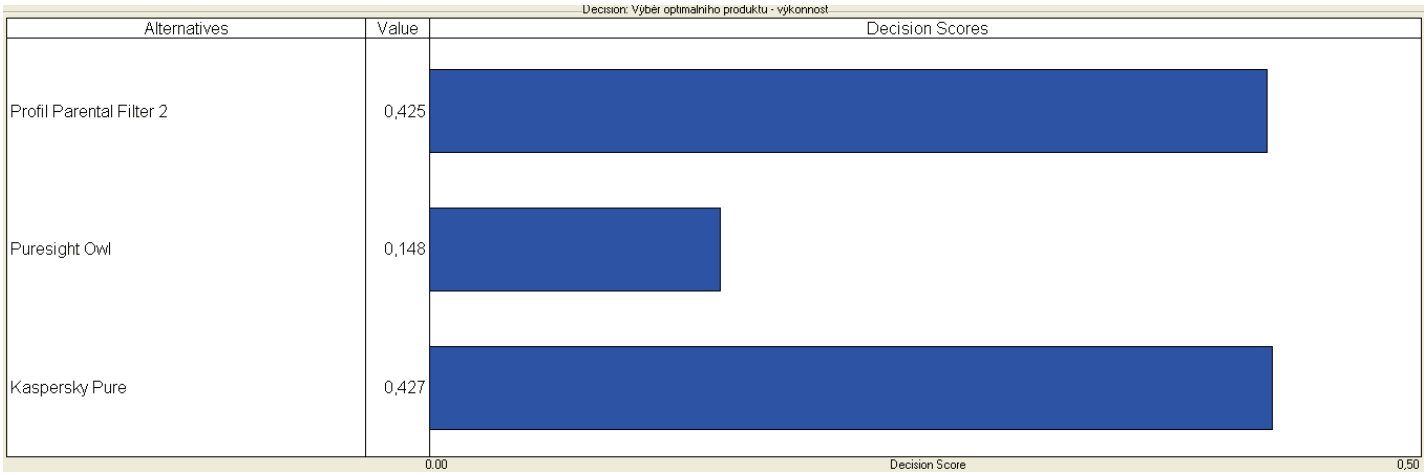
Obrázek 15 - Sestavení Saatyho matice - CDP

Zdroj: vlastní

Hodnocení výkonnosti

Obdobně, jako v případě metody Fullerova trojúhelníku, jsem prostřednictvím nástroje CDP provedla výpočet skóre jednotlivých produktů. Jako zdroj hodnocení jsem použila tabulku uvedenou v příloze C Výsledek hodnocení výkonnosti, tedy optimální variantu dle tohoto kritéria zobrazuje Obrázek 16.

Z výsledku hodnocení je patrné, že z hlediska výkonnosti je dle metody APH lépe hodnocený produkt Kaspersky Pure. Zároveň je také zřejmé, že převaha tohoto produktu je malá, tedy pouze o 0,002.

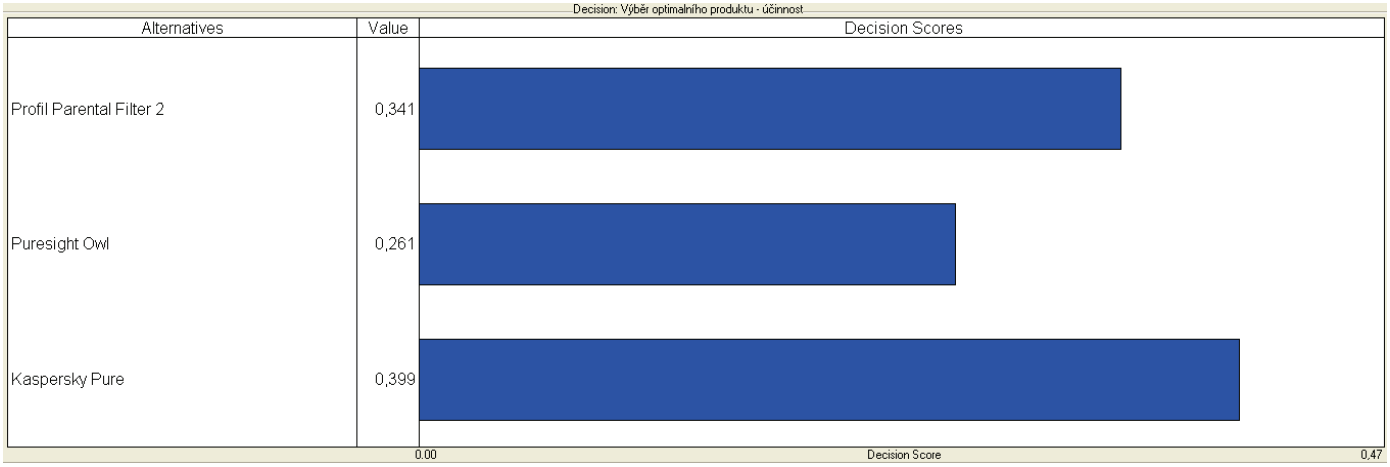


Obrázek 16 - Dosažné skóre produktů metodou AHP - výkonnost

Zdroj: vlastní

Hodnocení účinnosti

Sestavení hodnocení účinnosti probíhalo obdobně jako v případě hodnocení výkonnosti. Jako hodnocení produktů jsem využila hodnot získaných z testování produktů, které uvádí tabulka v příloze B. Výsledky metody AHP pro hodnocení variant produktů dle kritéria účinnosti zobrazuje Obrázek 17. Zde je názorně zobrazena převaha produktu Kaspersky Pure nad ostatními produkty.



Obrázek 17 - Dosažné skóre produktů metodou AHP - účinnost

Zdroj: vlastní

Z řešení rozhodovacích problémů vyplývá, že ve třech případech ze čtyř byl nejlépe hodnocen produkt Kaspersky Pure. Produkt nebyl hodnocen jako nejúspěšnější pouze v případě hodnocení výkonnosti metodou Fullerova trojúhelníku. Rozdílná pořadí produktu ve stejném hodnocení, metodou AHP, jsou způsobena velikostí preferencí vytvořenou pomocí Saatyho matice párového porovnávání kritérií. V případě metody AHP, jak zobrazuje Obrázek

16 je rozdíl mezi dosaženým skóre produktů pouze 0,002. Tato hodnota je velmi nízká, proto je možné, že při použití metody Fullerova trojúhelníku jsem díky rozdílným hodnotám vah dosáhla jiného výsledku.

Z hlediska zabezpečení ochrany dětí na Internetu větší váhu přikládám výsledkům hodnocení účinnosti, ve kterém byl jak v případě metody Fullerova trojúhelníku, tak v případě metody AHP, nejlépe hodnoceným produktem právě Kaspersky Pure. Použiji jej pro vytvoření návrhu zlepšení zabezpečení ochrany dětí.

8 NÁVRH VLASTNÍHO ŘEŠENÍ

V předchozí kapitole jsem ze získaného hodnocení produktů vybrala optimální variantu, která bude součástí návrhu zlepšení ochrany dětí v prostředí Internetu. Tato varianta a zjištěné vlastnosti a chování produktu jsou vstupem pro návrh vlastního řešení. Transformaci těchto vstupů a výstupy této kapitoly zobrazuje následující Obrázek 18.

Obrázek 18 - Schéma vstupů a výstupů pro návrh vlastního řešení

Zdroj: vlastní

Při návrhu zlepšení vycházím jak z výsledků hodnot testování, tak i ze zjištěných vlastností a chování software. Testováním jsem poznala silné a slabé stránky produktu a díky tomu mohu navrhnout účinné opatření pro ochranu dětí před nebezpečným obsahem Internetu za použití produktů rodičovské ochrany.

Jelikož produkt Kaspersky Pure měl nedostatky v oblasti filtrování blokovaných kategorií českých webových stránek, budu návrh vlastního řešení s části věnovat tomuto problému. Při návrhu zlepšení filtrování webových stránek vycházím z monitoringu produktů pro PC, které jsem provedla v kapitole 3, zejména pak produktů na úrovni integrace DNS. Produkty tohoto typu poskytují také filtrování podle kategorií obsahu webových stránek. Konkrétně využiji produkt Open DNS, který jsem v rámci monitoringu vyzkoušela a jehož filtrování českých webových stránek proběhlo úspěšně.

8.1 Popis návrhu

Návrh na zlepšení předpokládá instalaci produktu Kaspersky Pure a také zřízení účtu Open DNS. Produkt Kaspersky Pure pracuje s profily účtů vytvořených již operačním systému Windows. Před instalací tedy doporučuji, jedná-li se o sdílený počítač, nastavit účet ve Windows přímo pro dítě a heslem ochránit účet rodiče. Z účtu rodiče je pak možné nastavit požadovaná omezení. V případě filtrování webových stránek doporučuji zvolit seznam vyloučených webových stránek a vypsat seznam vyloučených webových stránek. Po zřízení účtu Open DNS je nutné změnit IP adresu DNS serveru poskytovatele Internetu na IP adresu uvedenou v účtu Open DNS. IP adresu je možné změnit přímo v počítači, což je výhodné v případě, že v domácnosti je pouze jeden počítač. Nebo je možné IP adresu DNS serveru

změnit v nastavení routeru, je-li domácí počítačová síť připojena k Internetu prostřednictvím tohoto aktivního prvku. Výhodou nastavení IP adresy v routeru je platnost omezení, respektive filtrování webových stránek, pro všechna zařízení připojená prostřednictvím tohoto routeru k Internetu. Jedná-li se o tzv. Wi-fi access point, tedy bod k připojení prostřednictvím bezdrátové sítě, je toto omezení platné i pro smartphone.

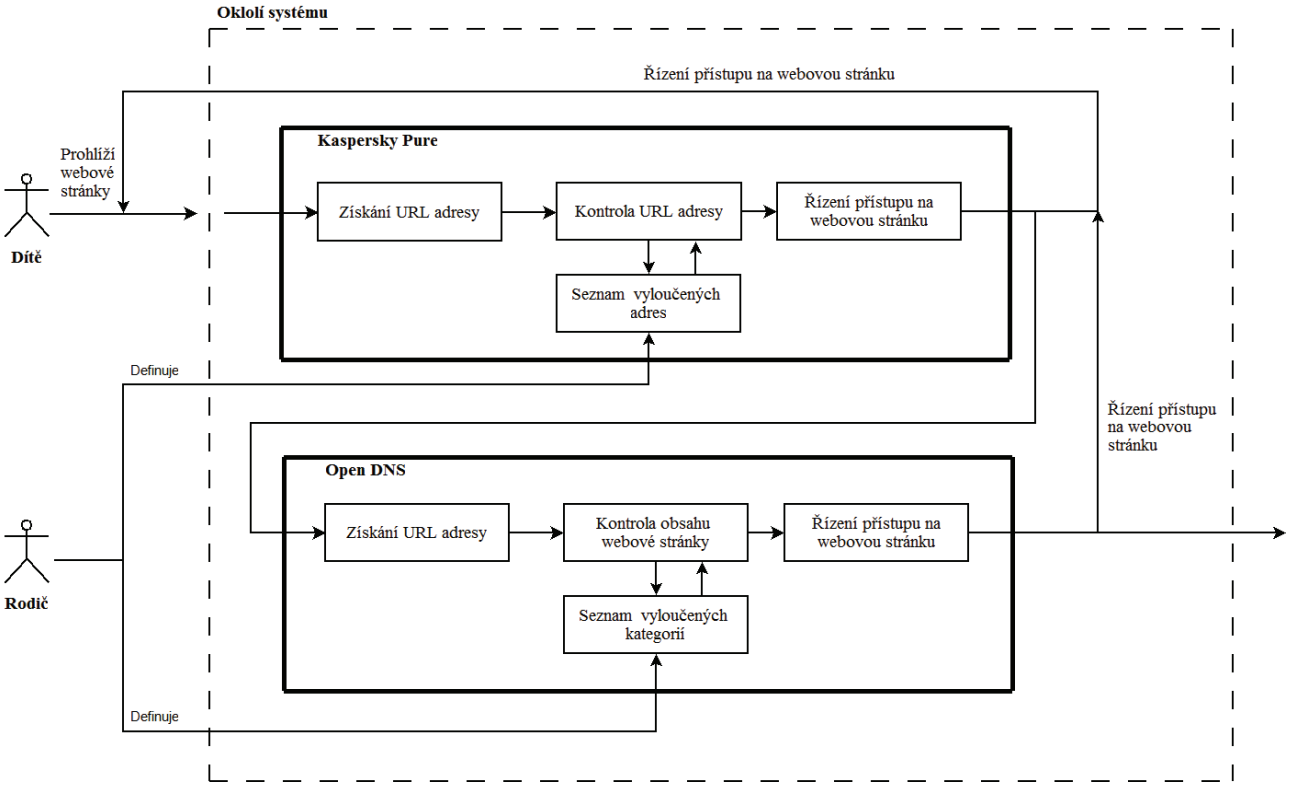
V účtu Open DNS je nutné nastavit blokované kategorie webových stránek, na které nebude mít dítě přístup. Jak jsem uvedla v kapitole 3.4, Open DNS nabízí přednastavené úrovně filtrování dle stupně ochrany, i možnost volby vlastního nastavení filtrování kategorií webových stránek.

8.2 Model návrhu

Model návrhu jsem znázornila jako systém, ve kterém jsou produkty Kaspersky Pure a Open DNS subsystémy. Návrh modelu představuje komunikaci produktů při prohlížení webových stránek dítětem. Při filtrování webových stránek může dojít ke dvěma situacím. Rozdíl mezi těmito situacemi je v pořadí akcí produktů. Z důvodu nedostatečné znalosti procesů filtrování webových stránek, zde uvedu obě situace.

Situace č.1

Předpokladem této situace je předem zvolený seznam vyloučených webových stránek, respektive jejich URL adres v produktu Kaspersky Pure a zvolené kategorie webových stránek, které mají být blokovány. Pokud si dítě chce prohlédnout požadovanou webovou stránku, jako první na požadavek zobrazení webové stránky bude reagovat produkt Kaspersky Pure. Tento produkt provádí filtrování webových stránek pouze u seznamu vyloučených webových stránek, respektive jejich URL adres. URL adresu nejprve získá z požadavku prohlížeče. Získanou adresu porovná se svým seznamem vyloučených adres. V případě, že se požadovaná URL adresa nachází v seznamu adres, Kaspersky Pure zablokuje přístup na tuto stránku. V opačném případě přístup na webovou stránku povolí. V tomto okamžiku na požadavek prohlížeče zareaguje Open DNS a porovná obsah webové stránky se zvolenými kategoriemi. Pokud stránka svým obsahem nespadá do zvolených kategorií, produkt povolí prohlížeči zobrazit webovou stránku dítěti. Naopak, pokud stránka spadá do alespoň jedné kategorie, Open DNS zablokuje přístup na tuto webovou stránku. Celý tento proces zobrazuje následující Obrázek 19.

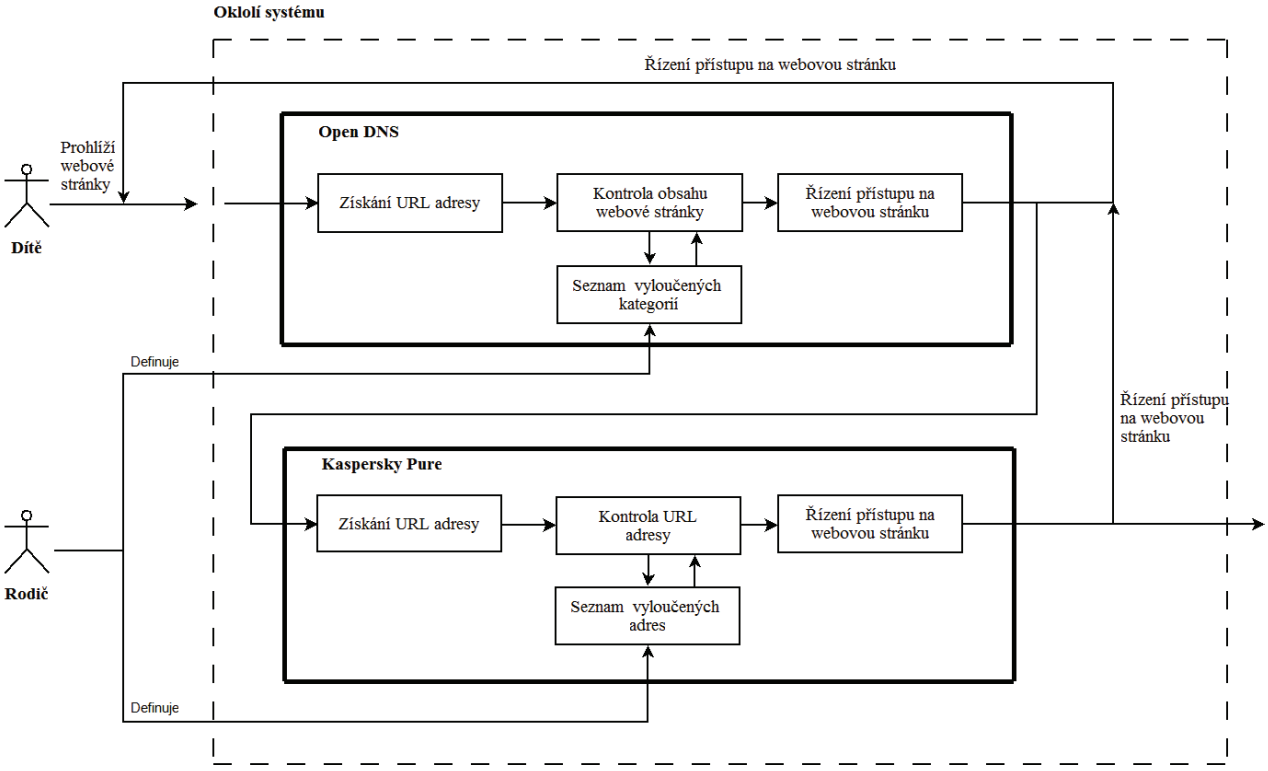


Obrázek 19 - Model návrhu filtrování webových stránek - Situace č. 1

Zdroj: vlastní

Situace č.2

V této situaci také předpokládám, že rodič předem zvolil seznam vyloučených webových stránek, jejich URL adres, v produktu Kaspersky Pure a také seznam vyloučených kategorií webových stránek v produktu Open DNS. V této situaci na požadavek zobrazení webové stránky reaguje jako první produkt Open DNS. Produkt z prohlížeče získá URL adresu požadované webové stránky. Její obsah porovná s kategoriemi, které rodič zvolil jako vyloučené. V případě, že webová stránka svým obsahem spadá alespoň do jedné z vyloučených kategorií, produkt zablokuje prohlížeči přístup na tuto webovou stránku. V opačném případě umožní prohlížeči webovou stránku zobrazit. V následujícím kroku Kaspersky Pure získá z webového prohlížeče URL adresu požadované webové stránky a porovná ji se svým seznamem vyloučených webových stránek. V případě, že se URL adresa shoduje s adresou uvedenou v seznamu, zablokuje prohlížeči přístup na požadovanou webovou stránku. V opačném případě, tedy, není-li URL adresa uvedena v seznamu vyloučených adres, povolí prohlížeči přístup na tuto stránku. Výše popsaný proces zobrazuje Obrázek 20.



Obrázek 20 - Model návrhu filtrování webových stránek - Situace č. 2

Zdroj: vlastní

Uvedené modely návrhu zlepšují filtrování webových stránek, které se při testování tohoto produktu jevilo jako problematické. Mimo ochrany před nebezpečným obsahem webových stránek, produkt Kaspersky Pure umožní také zabezpečení komunikace prostřednictvím služeb IM, řízení času stráveného jak v prostředí Internetu, tak v rámci samotného počítače. Produkt také poskytne informace o činnostech dítěte a umožní tak rodiči získat přehled o činnostech, které dítě provádí jak v prostředí Internetu, tak v počítači.

Využitím produktu Open DNS mohou rodiče také v rámci domácí Wi-fi sítě ovlivnit blokování kategorií webových stránek zobrazovaných pomocí mobilních zařízení, jako je například smartphone.

Produkt ovšem neumožní filtrování a sledování emailové komunikace, či komunikace prostřednictvím sociálních sítí. Tyto nedostatky produktu jsou vhodným podnětem k diskusi jak rodičů s dětmi, tak i tvůrci produktů jako je právě Kaspersky Pure.

ZÁVĚR

Cílem této práce bylo navrhnout vlastní řešení pro ochranu dětí v prostředí Internetu. Abych byla schopna navrhnout vlastní řešení zlepšení ochrany, definovala jsem ohroženou skupinu a nebezpečí, která jí v prostředí Internetu hrozí. Také jsem popsala stávající situaci ochrany dětí v oblasti Internetu a organizace, které se daným tématem zabývají. Provedla jsem monitoring produktů pro zabezpečení přístupu na nevhodné www stránky a rozdělila je tematicky na produkty pro platformy PC a smartphone. V další části jsem provedla testování produktů pro ochranu dětí před nebezpečným obsahem Internetu. Na základě výsledku testování jsem provedla hodnocení produktů, z nichž jsem metodami vícekriteriálního rozhodování vybrala jeden produkt, Kaspersky Pure, pro který jsem navrhla zlepšení ochrany dětí v prostředí Internetu. Zlepšení ochrany jsem navrhla v oblasti filtrování webových stránek. Tento návrh jsem vyjádřila formou modelu, který v sobě kombinuje použití produktů Kaspersky Pure a Open DNS

Účelem práce bylo navrhnout zlepšení ochrany dětí, z čehož vyplývá, že současná ochrana dětí v prostředí Internetu není bezchybná. Ani prostřednictvím návrhu zlepšení, rizika číhající v Internetu, není možné zcela eliminovat. Návrh zlepšení pouze toto riziko zmírní. Nejlepším možným způsobem ochrany dětí je forma dialogu s jejich rodiči. Pokud si budou vzájemně důvěřovat a děti budou mít jistotu, že se rodičům mohou se svými zkušenostmi v prostředí Internetu svěřit, rizika mohou omezit. Rodiče by měli se svými dětmi mluvit o těchto rizicích, varovat je a vysvětlit jim jaké důsledky mohou tato rizika mít. Zároveň je důležité, aby rodiče s dětmi mluvili odpovědnosti za jejich jednání v prostředí Internetu. Internet je totiž důležitý pomocník i mocná zbraň.

Osobní přínosem této práce pro mne bylo získání širšího nadhledu nad možnými riziky v prostředí Internetu a utvrzení v nutnosti chránit děti před těmito riziky. Díky možnosti pracovat s produkty, které mají sloužit na ochranu dětí v Internetu, jsem získala přehled, jakým způsobem je možné děti chránit a také jakými nedostatky tyto produkty trpí. Práce mi přinesla možnost uvažovat nad změnami a vylepšeními, která by zmírnila rizika ohrožující děti při pohybu v síti Internetu.

POUŽITÁ LITERATURA

[1] Bezpečnější internet pro všechny. GOOGLE. *Google* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.google.com/goodtoknow/protection/internet/

[2] CENTRE FOR THE PREVENTION OF RISKY VIRTUAL COMMUNICATION PEDAGOGICAL FACULTY OF PALACKÝ UNIVERSITY IN OLOMOUC. *Our mission* [online]. © 2010-2013 [cit. 2013-07-20]. Dostupné z: http://www.prvok.upol.cz/

[3] CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE PEDAGOGICKÉ FAKULTY UNIVERZITY PALACKÉHO V OLOMOUCI. *Projekt E-bezpečí* [online]. (c) 2008 - 2013 [cit. 2013-07-20]. Dostupné z: http://www.e-bezpeci.cz/

[4] Co je to DNS?. CZECHIA.COM. *Nápověda CZECHIA.COM* [online]. 2013 [cit. 2013-05-01]. Dostupné z: http://help.czechia.com/clanek/co-je-to-dns/

[5] Co je to GSM (slovník). *ITBIZ: Vaše jednička mezi nulami* [online]. 2013 [cit. 2013-06-02]. Dostupné z: http://www.itbiz.cz/slovnik/telekomunikace/gsm

[6] Co je to WiFi - úvod do technologie. HW SERVER S.R.O. *HW.cz | Vše o elektronice a programování* [online]. 21. Červen 2003 [cit. 2013-04-01]. Dostupné z: http://www.hw.cz/produkty/ethernet/co-je-to-wifi-uvod-do-technologie.html

[7] Cyberbully Help. AGATSTON, Patti. *Cyber Bullying Guide for Parents* [online]. 2010, 8.11.2010 [cit. 2013-06-25]. Dostupné z: http://www.cyberbullyhelp.com/Cyber%20Bullying%20Guide%20for%20Parents.pdf

[8] Česká republika. Zákon č. 101/2000, o ochraně osobních údajů. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, p. o., 2000.

[9] Česká Republika. Zákon č. 480/2004 Sb.: o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In: *Sbírka Zákonů*. Praha: Tiskárna Ministerstva vnitra, p. o., 2004.

[10] Česká republika. Zákon trestní zákoník. In: *40/2009*. Praha: Tiskárna Ministerstva vnitra, p. o., 2009, 11.

[11] ČSN ISO/IEC 14598-1. *Informační technologie - Hodnocení softwarového produktu: Část 1: Všeobecný přehled*. Praha: ČESKÝ NORMALIZAČNÍ INSTITUT, 2000.

[12] DOČEKAL, Daniel. Česko a sociální sítě v číslech. INTERNET INFO, s.r.o. *Lupa.cz: server o českém Internetu* [online]. 5. 8. 2011 [cit. 2013-01-26]. Dostupné z: http://www.lupa.cz/clanky/cesko-a-socialni-site-v-cislech/

[13] EU Kids online - Research: Department of Media and Communications. THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE. *LSE - The London School of Economics and Political Science* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

[14] EUROPEAN COMMISSION. *SIP-Benchmark II* [online]. 2011 [cit. 2013-01-01]. Dostupné z: http://www.sipbench.eu/

[15] Filtr SmartScreen. MICROSOFT.. *Microsoft Windows* [online]. © 2013 [cit. 2013-04-27]. Dostupné z: http://windows.microsoft.com/cs-cz/internet-explorer/products/ie-9/features/smartscreen-filter

[16] FOTR, Jiří, Lenka ŠVECOVÁ, Jiří DĚDINA, Helena HRŮZOVÁ a Jiří RICHTER. *Manažerské rozhodování: postupy, metody a nástroje*. Vyd. 1. Praha: Ekopress, 2006, 409 s. ISBN 80-869-2915-9.

[17] F-Secure Mobile Security: Aplikace pro Android ve službě Google Play. GOOGLE INC. *Google Play* [online]. © 2013 [cit. 2013-06-29]. Dostupné z: https://play.google.com/store/apps/details?id=com.fsecure.ms.dc&hl=cs

[18] FUNAMO.COM. *Funamo!: Best Mobile Parental Control for Android Cell Phones, Tablets* [online]. 2013 [cit. 2013-06-30]. Dostupné z: http://www.funamo.com/user/registration

[19] Google Chrome is a mixed bag for Apple. WEINTRAUB, Seth. *Computerworld Blogs* [online]. 2008 [cit. 2013-05-02]. Dostupné z: http://blogs.computerworld.com/google_chrome_is_a_mixed_bag_for_apple_users

[20] Hledáte funkce pro filtrování webu a sestavy činností v Rodičovské kontrole systému Windows?.MICROSOFT. *Microsoft Windows* [online]. 2013 [cit. 2013-05-03]. Dostupné z: http://windows.microsoft.com/cs-cz/windows7/looking-for-web-filtering-and-activity-reports-in-windows-parental-controls#section_1

[21] Children's Privacy: BCP Business Center. FEDERAL TRADE COMMISION. *BCP Business Center* [online]. 1.7.2013 [cit. 2013-07-05]. Dostupné z: www.business.ftc.gov/privacy-and-security/childrens-privacy

[22] Chronium. *The Chronium Projects* [online]. 2013 [cit. 2013-05-02]. Dostupné z: http://www.chromium.org/Home

[23] INHOPE ASSOCIATION. *INHOPE* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.inhope.org/gns/home.aspx

[24] *Instant messaging systems*. New York, NY: Wiley Pub., c2002, xv, 684 p. ISBN 07-645-4953-7.

[25] Internetový obchod Chrome: avast! Online Security. *Internetový obchod Chrome* [online]. 2013 [cit. 2013-05-02]. Dostupné z: https://chrome.google.com/webstore/detail/avast-online-security/gomekmidlodglbbmalcneegieacbdmki/details?hl=cs

[26] Internetový obchod Chrome: Bloksi – Web filtering and parental control!. *Internetový obchod Chrome* [online]. 2013 [cit. 2013-05-02]. Dostupné z: https://chrome.google.com/webstore/detail/blocksi-web-filtering-and/pgmjaihnmedpcdkjcgigocogcbffgkbn?hl=cs

[27] ISO/IEC 9126-4. *Software engineering -- Product quality: Part 4: Quality in use metrics*. 3. vydání. Tokyo: Waseda University, 2013.

[28] ISO/IEC/IEEE 29119-1 - Software and systems engineering -- Software testing: Part 1: Concepts and definitions. THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO: International Organization for Standardization* [online]. 2013 [cit. 2013-05-04]. Dostupné z: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45142

[29] Jak se chránit před malwarem. GOOGLE INC.. *Nápověda AdWords* [online]. © 2013 [cit. 2013-04-27]. Dostupné z: https://support.google.com/adwords/answer/2375413?hl=cs

[30] Jak se určují kategorie obsahu webu?. MICROSOFT. *Microsoft Windows* [online]. 2013 [cit. 2013-05-01]. Dostupné z: http://windows.microsoft.com/cs-cz/windows-live/family-safety-web-content-categories-how-ui

[31] JSV 6(3) NewGen print.vp - Hinduja and Patchin: Journal of School Violence. SAMEER, Hinduja a Justin W. PATCHIN. *USC School of Social Work* [online]. 2007 [cit. 2013-01-24]. Dostupné z: http://socialwork.usc.edu/~rastor/Israel%20flight/Hinduja%20and%20Patchin%20-%20Journal%20of%20School%20Violence.pdf

[32] K čemu slouží SSL certifikáty. ZONER SOFTWARE, a.s. *SSL certifikáty THAWTE* [online]. 2013 [cit. 2013-03-15]. Dostupné z: http://www.ssl-thawte.cz/ssl/co-je-to-ssl/

[33] Kaspersky Lab ZAO. Kaspersky PURE 3.0 [počítačový program]. Ver. 3.0. [Rusko], 1998 [cit 2013-05-12]. Dostupné z: http://www.kaspersky.com/pure

[34] Kaspersky Pure 2. KASPERSKY LAB ZAO. *Kaspersky Lab Technical Support.* [online]. © 1997 – 2013 [cit. 2013-03-07]. Dostupné z: http://support.kaspersky.com/pure_2#requirements

[35] Kaspersky Pure: Ultimate PC Protection. KASPERSKY LAB ZAO. *Kaspersky Lab | Antivirus Protection | Internet Security.* [online]. © 1997 – 2013 [cit. 2013-03-07]. Dostupné z: http://www.kaspersky.com/pure

[36] KOPECKÝ, Kamil. *Moderní trendy v e-komunikaci*. Olomouc: Hanex, 2007, 98 s. ISBN 978-808-5783-780.

[37] KŘUPKA, J., M KAŠPAROVÁ a R. MÁCHOVÁ. Metody stanovení vah kriterií. *Rozhodovací procesy* [online]. 2011 [cit. 2012-12-20]. Dostupné z: http://www.rozhodovaciprocesy.cz/vicekriterialni-rozhodovani/2-1-metody-stanoveni-vah-kriterii.html

[38] KŘUPKA, J., M KAŠPAROVÁ a R. MÁCHOVÁ. Rozhodování jako systém. *Rozhodovací procesy* [online]. 2011 [cit. 2013-06-20]. Dostupné z: http://www.rozhodovaciprocesy.cz/uvod-do-teorie-rozhodovani/1-2-rozhodovani-jako-system.html

[39] KŘUPKA, Jiří. *Teorie systémů I: pro kombinovanou formu studia*. Vyd. 1. Pardubice: Univerzita Pardubice, 2006, 140 s. ISBN 80-719-4923-X.

[40] KUBÁTOVÁ, Kateřina. SmartPhone. *Západočeská Univerzita* [online]. 2013 [cit. 2013-04-28]. Dostupné z: http://home.zcu.cz/~kubatovk/

[41] Kurzy devizového trhu: Česká národní banka. ČESKÁ NÁRODNÍ BANKA. *Česká národní banka* [online]. 26. 6. 2013 [cit. 2013-06-26]. Dostupné z: http://www.cnb.cz/cs/financni_trhy/devizovy_trh/kurzy_devizoveho_trhu/denni_kurz.jsp

[42] LANGMEIER, Josef a Dana KREJČÍŘOVÁ. *Vývojová psychologie*. 2., aktualiz. vyd. Praha: Grada, 2006, 368 s. Psyché (Grada). ISBN 80-247-1284-9.

[43] Licenční smlouva koncového uživatele. ICQ LLC. *Stáhněte si aplikaci ICQ Messenger a přejděte od placených zpráv SMS k bezplatnému zasílání zpráv!* [online]. 1996 [cit. 2013-06-14]. Dostupné z: http://www.icq.com/legal/eula/cz

[44] LIVINGSTONE, S., HADDON, L., GÖRZIG, A. and OLAFSSON, K., (2011). *Risks and safety on the internet. The perspective of European children. Full Findings*, LSE, London: EU Kids Online. ISSN 2045-256X

[45] LIVINGSTONE, Sonia M a Leslie HADDON. *Kids online: opportunities and risks for children*. Portland, OR: Policy Press, 2009, xix, 272 s. ISBN 978-184-7424-389.

[46] MACÍCH ML., Jiří. Microsoft Messenger „mává uživatelům na rozloučenou". INTERNET INFO, s.r.o. *Lupa.cz* [online]. 8. 4. 2013 [cit. 2013-05-24]. Dostupné z: http://www.lupa.cz/clanky/microsoft-messenger-mava-uzivatelum-na-rozloucenou/

[47] Messenger přešel na Skype: Nápověda pro Microsoft Windows. MICROSOFT. *Microsoft Windows* [online]. 2013 [cit. 2013-07-10]. Dostupné z: http://windows.microsoft.com/cs-cz/messenger/messenger-to-skype

[48] MITNICK, Kevin. *Umění klamu*. Vyd. 1. Gliwice: Helion, 2003, 348 s. ISBN 83-736-1210-6.

[49] Mobile Security – Antivirus - Android - Windows Mobile - Symbian - Free Trial. F-SECURE. *Internet Security - Antivirus - Online backup - Mobile Security - Anti-Virus for Mac: F-Secure* [online]. 2013 [cit. 2013-07-01]. Dostupné z: http://www.f-secure.com/en/web/home_global/mobile-security

[50] Mozilla Public License. *Mozilla: Home of Mozilla project* [online]. 2012 [cit. 2013-05-02]. Dostupné z: http://www.mozilla.org/MPL/

[51] NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Bezpečně online* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.bezpecne-online.cz/

[52] NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Horká linka.cz* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.horkalinka.net

[53] NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz: Aktuality* [online]. 2013 [cit. 2013-07-20]. Dostupné z: http://www.saferinternet.cz/

[54] Nastavení služby Zabezpečení rodiny: Nápověda systému Microsoft Windows. MICROSOFT. *Microsoft Windows* [online]. 2013 [cit. 2013-05-01]. Dostupné z:

http://windows.microsoft.com/cs-cz/windows/set-up-family-safety#set-up-family-safety=windows-7

[55] *O nás: NCBI* [online]. 2012 [cit. 2013-07-20]. Dostupné z: http://www.ncbi.cz/

[56] O službě Google Play. *Nápověda Google Play* [online]. 27. červen 2013 [cit. 2013-06-30]. Dostupné z: https://support.google.com/googleplay/answer/2490014?hl=cs&p=play_faq&rd=1

[57] OPENDNS, Inc. *Internet Security or DNS Service for your Business or Home - OpenDNS* [online]. 2012 [cit. 2013-02-28]. Dostupné z: http://www.opendns.com/

[58] Operating Systems. *Gemius Ranking CZ* [online]. 2000 [cit. 2013-02-01]. Dostupné z: http://www.rankings.cz/en/rankings/operating-systems.html

[59] P. Holub. Jak na streamované video?. Zpravodaj ÚVT MU. ISSN 1212-0901, 2002, roč. XII, č. 3, s. 9-13. [cit. 2013-04-15]. Dostupné z: http://www.ics.muni.cz/bulletin/articles/238.html

[60] PATTON, Ron. *Testování softwaru*. Vyd. 1. Praha: Computer Press, 2002, xiv, 313 s. Programování. ISBN 80-722-6636-5.

[61] Phising. SEZNAM A.S.. *Seznam Nápověda* [online]. © 1996–2013 [cit. 2013-04-26]. Dostupné z: http://napoveda.seznam.cz/cz/phishing.html

[62] Podmínky použití produktů společnosti Skype. MICROSOFT. *Bezplatná internetová volání Skype a levná volání na telefonní čísla online – Skype* [online]. 2013 [cit. 2013-06-20]. Dostupné z: http://www.skype.com/cs/legal/tou/#1

[63] POLESNÝ, David. ICQ: pokus o vzkříšení pionýra sociálních sítí. *Živě.cz: O počítačích, IT a internetu* [online]. 2010 [cit. 2013-06-10]. Dostupné z: http://www.zive.cz/clanky/icq-pokus-o-vzkriseni-pionyra-socialnich-siti/sc-3-a-150547/default.aspx

[64] Požadavky sady Windows Essentials 2012 na systém. MICROSOFT. *Microsoft Windows* [online]. 2013 [cit. 2013-05-01]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/windows-essentials-2012-system-requirements

[65] ProCon Latte Content Filter: Doplňky aplikace Firefox. *Doplňky aplikace Firefox* [online]. 2011 [cit. 2013-05-03]. Dostupné z: https://addons.mozilla.org/cs/firefox/addon/procon-latte/?src=search

[66] Profil Technology. Profil Parental Filter 2 [počítačový program]. Ver. 2.4.3. [Francie], 1998 [cit 2013-05-10]. Dostupné z: http://www.profiltechnology.com/en/home/parental-filter2

[67] Profil Technology: Home solutions – Parental Filter 2. PROFIL TECHNOLOGY. *Profil Technology, digital content analysis and filtering for families, companies and schools* [online]. 2013 [cit. 2013-03-01]. Dostupné z: http://www.profiltechnology.com/en/home/parental-filter2#

[68] Prohlášení o právech a povinnostech. *Facebook* [online]. 2012 [cit. 2013-05-02]. Dostupné z: https://www.facebook.com/legal/terms

[69] Prohlášení o právech a povinnostech. FACEBOOK. *Facebook* [online]. aktualizováné 11. prosince 2012 [cit. 2013-04-12]. Dostupné z: https://www.facebook.com/legal/terms

[70] Přehled podílů vyhledávačů a PPC systémů. ATAXO CZECH S.R.O. *Ataxo – internetová reklama a SEO optimalizace pro vyhledávače* [online]. 2010 [cit. 2013-04-20]. Dostupné z: http://www.ataxo.cz/informace/vyhledavace-katalogy/prehled-podilu-vyhledavacu

[71] Puresight © Technologies Ltd.. PureSight Owl [počítačový program]. Ver. 2012.3.9081. [Izrael], 2012 [cit 2013-05-15]. Dostupné z: http://www.puresight.com

[72] PureSight Owl 2012. PURESIGHT © TECHNOLOGIES LTD. *Parental Control | PureSight.* [online]. 2013 [cit. 2013-03-05]. Dostupné z: http://onlinechild.puresight.com/onlinehelp/1/en/index.html

[73] PureSight Owl 2012. PURESIGHT © TECHNOLOGIES LTD. *Parental Control | PureSight.* [online]. 2013 [cit. 2013-03-05]. Dostupné z: http://onlinechild.puresight.com/Support/support_im?brandId=1&langName=en

[74] PureSight Owl Features and Benefits. PURESIGHT © TECHNOLOGIES LTD. *Parental Control | PureSight.* [online]. 2013 [cit. 2013-03-05]. Dostupné z: http://www.puresight.com/Features/puresight-owl-features-and-benefits.html

[75] Různé webové prohlížeče. JANOVSKÝ, Dušan. *Jak psát web* [online]. 2010 [cit. 2013-05-01]. Dostupné z: http://www.jakpsatweb.cz/prohlizece.html

[76] ŘÍČAN, Pavel a Pavlína JANOŠOVÁ. *Jak na šikanu*. Vyd. 1. Praha: Grada, 2010, 155 s. Pro rodiče. ISBN 978-802-4729-916.

[77] SEZNAM.CZ, a.s. *Jsou děti na internetu v bezpečí?* [online]. © 1996 - 2011 [cit. 2013-07-20]. Dostupné z: http://seznamsebezpecne.cz

[78] ŠMAHEL, David. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton, 2003, 158 s. Psychologická setkávání, sv. 6. ISBN 80-725-4360-1.

[79] The Internet Standards Process. HARVARD UNIVERSITY. *RFC-Editor Webpage* [online]. 1996 [cit. 2013-04-26]. Dostupné z: http://www.rfc-editor.org/rfc/rfc2026.txt

[80] *The perspective of European children: Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries* [online]. 2011, Poslední aktualizace 12.1.2011[cit. 2013-01-20]. Dostupné z: www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

[81] TOPlist - Historie. *TOPlist - audit návštěvnosti webových stránek zdarma:* [online]. 2013 [cit. 2013-04-21]. Dostupné z: http://toplist.cz/stat/?a=history&type=4

[82] UČEŇ, Pavel. *Metriky v informatice: jak objektivně zjistit přínosy informačního systému*. 1. vyd. Praha: Grada, 2001, 139 s. ISBN 80-247-0080-8.

[83] UZEL, Radim. *Pornografie, aneb, Provokující nahota*. Vyd. 1. Praha: Ikar, 2004, 197 s. ISBN 80-249-0351-2.

[84] VÁGNEROVÁ, Marie. *Vývojová psychologie*. Vyd. 1. V Praze: Karolinum, 2005, 467 s. ISBN 978-802-4609-560.

[85] VÍT, Svatopluk. Když se řekne repozitář. INTERNET INFO, s.r.o. *Root.cz: informace nejen ze světa Linuxu* [online]. 3. 8. 2008 [cit. 2013-05-01]. Dostupné z: http://www.root.cz/clanky/kdyz-se-rekne-repozitar/

[86] WAIC, Vlastimil. Opera, Firefox, Chrome a Safari součástí Windows? Utopie? Realita!. MLADÁ FRONTA A. S. *Živě.cz* [online]. 25. 2. 2009 [cit. 2013-05-24]. Dostupné z: http://www.zive.cz/clanky/opera-firefox-chrome-a-safari-soucasti-windows-utopie-realita/sc-3-a-145837/default.aspx

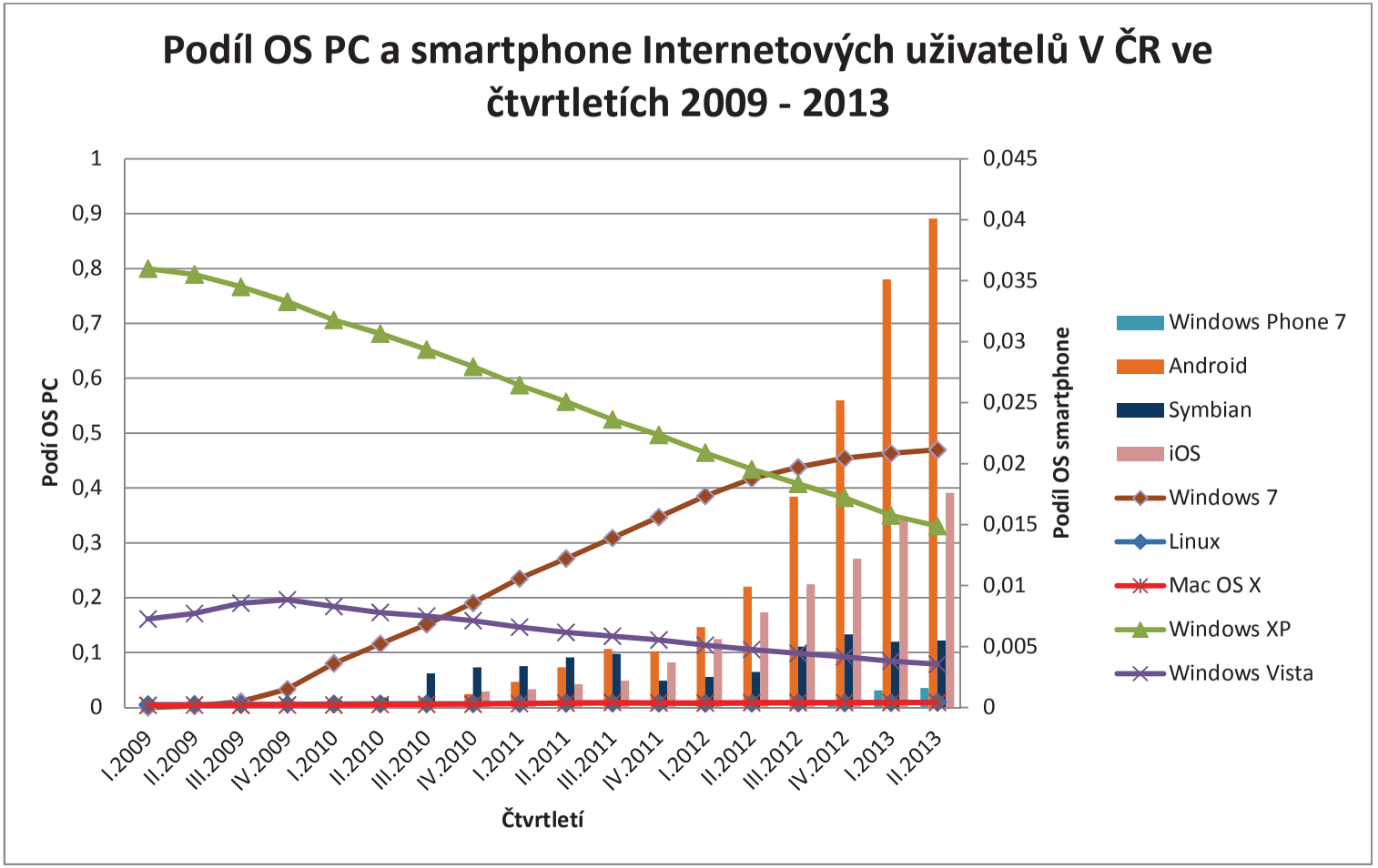
[87] W-CDMA. ETSI. *3GPP* [online]. © 2013 [cit. 2013-04-21]. Dostupné z: http://www.3gpp.org/Technologies/Keywords-Acronyms/article/w-cdma

[88] Web browsers – groups. *Gemius Ranking CZ* [online]. 2000 [cit. 2013-05-10]. Dostupné z: http://www.rankings.cz/en/rankings/web-browsers-groups.html

[89] WILLARD, Nancy E. *Cyberbullying and cyberthreats: responding to the challenge of online social aggression, threats, and distress*. Champaign, Ill.: Research Press, c2007, v, 311 p. ISBN 978-087-8225-378.

SEZNAM PŘÍLOH

Příloha A - Graf podílu OS PC a smartphone Internetových uživatelů V ČR ve čtvrtletích 2009 – 2013



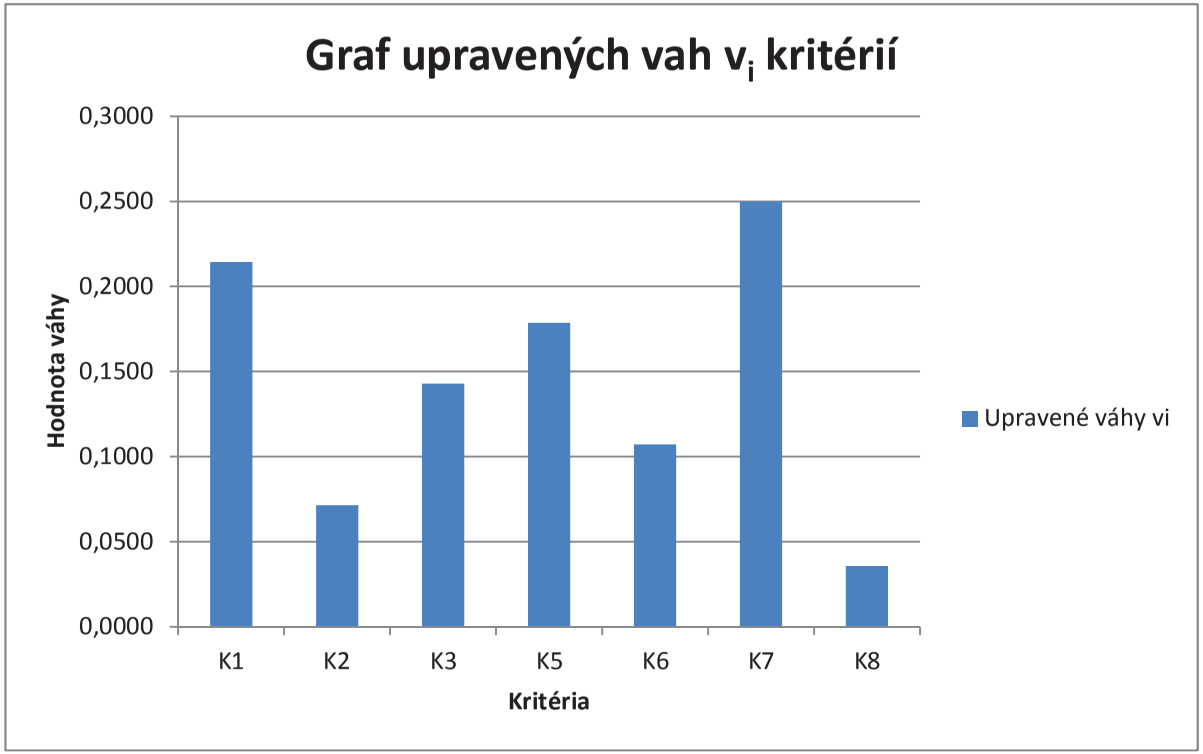
Příloha B - Tabulka hodnocení účinnosti produktů

Kritérium / Produkt	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2
Filtrování, omezení přístupu na nevhodné stránky (K1)	0	0,1	0,9
Zabezpečení emailové komunikace (K2)	0	0	0
Zabezpečení komunikace prostřednictvím IM (K3)	0	1	0
Monitoring a reporting činností a času stráveného na Internetu (K5)	0,7	0,7	0,1
Řízení času stráveného na Internetu (K6)	1	1	1
Zabezpečení produktu (K7)	1	1	1
Cena produktu (K8)	€ 46,06	€ 61,38	€ 39,99

Příloha C - Tabulka hodnocení výkonnosti produktů

Kritérium / Produkt	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2
Filtrování, omezení přístupu na nevhodné stránky (K1)	78	107	98
Zabezpečení emailové komunikace (K2)	49	35	35
Zabezpečení komunikace prostřednictvím IM (K3)	154	84	130
Monitoring a reporting činností a času stráveného na Internetu (K5)	296	79	67
Řízení času stráveného na Internetu (K6)	85	87	83
Zabezpečení produktu (K7)	293	63	67
Cena produktu (K8)	€ 46,06	€ 61,38	€ 39,99

Příloha D – Graf upravených vah v_i kritérií



Příloha E – Tabulky párového porovnávání alternativ metodou Fullerova trojúhelníku dle výkonnosti

Kritéritum K1	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	1	2	0,666667	0,5
Kaspersky Pure	0		0	0	0	0,166667
Profil Parental Filter 2	0	1		1	0,333333	0,333333

Kritéritum K2	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		0,5	1,5	0,666667	0,416667
Profil Parental Filter 2	1	0,5		1,5	0,333333	0,416667

Kritéritum K3	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		1	2	0,666667	0,5
Profil Parental Filter 2	1	0		1	0,333333	0,333333

Kritéritum K5	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		0	1	0,333333	0,333333
Profil Parental Filter 2	1	1		2	0,666667	0,5

Kritéritum K6	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	0		0	0	0	0,166667
Profil Parental Filter 2	1	1		2	0,666667	0,5

Kritéritum K7	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		1	2	0,666667	0,5
Profil Parental Filter 2	1	0		1	0,333333	0,333333

Kritéritum K8	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	0		0	0	0	0,166667
Profil Parental Filter 2	1		1	2	0,666667	0,5

Příloha F – Tabulky párového porovnávání alternativ metodou Fullerova trojúhelníku dle účinnosti

Kritéritum K1	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		0	1	0,333333	0,333333
Profil Parental Filter 2	1	1		2	0,666667	0,5

Kritéritum K2	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	1		0	1	0,333333	0,333333
Profil Parental Filter 2	0	1		1	0,333333	0,333333

Kritéritum K3	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	0	0	0	0,166667
Kaspersky Pure	1		1	2	0,666667	0,5
Profil Parental Filter 2	1	0		1	0,333333	0,333333

Kritéritum K5	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		0	1	1	0,333333	0,333333
Kaspersky Pure	1		1	2	0,666667	0,5
Profil Parental Filter 2	0	0		0	0	0,166667

Kritéritum K6	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	0		1	1	0,333333	0,333333
Profil Parental Filter 2	1	0		1	0,333333	0,333333

Kritéritum K7	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	0		1	1	0,333333	0,333333
Profil Parental Filter 2	1	0		1	0,333333	0,333333

Kritéritum K8	PureSight Owl	Kaspersky Pure	Profil Parental Filter 2	Počet preferencí	Výsledné váhy v_i	Upravené váhy v_i
PureSight Owl		1	0	1	0,333333	0,333333
Kaspersky Pure	0		0	0	0	0,166667
Profil Parental Filter 2	1	1		2	0,666667	0,5

Příloha G – Hierarchická struktura H rozhodovacího problému, metoda AHP