

Rodičovská kontrola v informačních technologiích

Jan Pavelka

Bakalářská práce
2019



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Jan Pavelka**
Osobní číslo: **A15025**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Informační technologie v administrativě**
Forma studia: **prezenční**

Téma práce: **Rodičovská kontrola v informačních technologiích**

Téma anglicky: **Parental Control in Information Technologies**

Zásady pro vypracování:

1. Provedte literární rešerši na téma IT hrozeb u dětí, kyberšikany apod.
2. Zaměřte se na možnosti rodičovské kontroly.
3. Prozkoumejte současné možnosti rodičovské ochrany na různém hardware a software.
4. Otestujte vybrané možnosti rodičovské ochrany.
5. Vytvořte sadu doporučení k vhodné implementaci rodičovské ochrany.



Rozsah bakalářské práce: -

Rozsah příloh:

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

Seznam odborné literatury:

1. ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.
2. ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Vyd. 1. Praha: Grada, 2014. 183 s. Psyché.
3. HOLLÁ, Katarína. Sexting a kyberšikana. Vydanie: prvé. Bratislava: Iris, 2016. 165 s.
4. Internetem bezpečně [online]. Karlovy Vary: you connected, c2018 [cit. 2018-11-24]. Dostupné z: <https://www.internetembezpecne.cz>
5. Bezpečně online [online]. Praha: Národní centrum bezpečnějšího internetu, c2017 [cit. 2018-11-24]. Dostupné z: <https://bezpecne-online.saferinternet.cz>

Vedoucí bakalářské práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**

Ústav řízení procesů

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 27.05.2019

Jan Pavelka, v. r.

ABSTRAKT

Předkládaná bakalářská práce na téma: „Rodičovská kontrola v Informačních technologiích“ se zabývá problematikou spojenou s bezpečím dětí na Internetu. V teoretické části se tato práce zabývá hrozbami, které v dnešní době mohou na dítě v IT prostředí čekat a jejich rozdělením do 5 skupin. V praktické části jsou poté obsaženy možnosti rodičovské kontroly a samotná rodičovská kontrola, která se zaměří na nejpoužívanější zařízení u dětí. Na závěr se práce věnuje otestování vybraných aplikací/programů na jednotlivých IT zařízeních s následným vyhodnocením. Hlavním cílem práce je proto navrhnout několika otestovaných možností zabezpečení domácí sítě spolu se zabezpečením a kontrolou zařízení dětí.

Klíčová slova: Rodičovská kontrola, IT, Internet, software, hardware, aplikace, Wi-Fi router, DNS server.

ABSTRACT

This bachelor thesis: "Parental Control in Information Technologies" deals with issues related to children's safety on the Internet. In the theoretical part, this thesis deals with the current threats that can wait for a child in the IT environment and dividing them into 5 groups. The practical part includes the possibilities of parental control and the parental control itself, which will focus on the most used devices in IT. In conclusion, the thesis deals with testing of selected applications/programs on individual IT devices with subsequent evaluation. The main goal of this work is to suggest several tested home network security options along with the security and control of children's devices.

Keywords: Parental Control, IT, Internet, software, hardware, applications, Wi-Fi router, DNS server.

Velmi rád bych chtěl touto cestou poděkovat vedoucímu své bakalářské práce panu doc. Ing. Jiřímu Vojtěškovi, Ph.D. za ochotu, cenné rady, poznatky a odborný přehled, ale také za trpělivost při zpracovávání bakalářské práce. V neposlední řadě bych chtěl také poděkovat své rodině, která mě po celou dobu studia podporovala a také samotné Univerzitě Tomáše Bati za možnost studia na Fakultě aplikované Informatiky.

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

OBSAH

ÚVOD.....	8
I TEORETICKÁ ČÁST.....	9
1 HROZBY INFORMAČNÍ TECHNOLOGIE	10
1.1 KOMUNIKAČNÍ HROZBY	11
1.1.1 Kyberšikana.....	11
1.1.2 Kyberstalking	12
1.1.3 Kybergrooming	12
1.1.4 Sexting.....	13
1.2 OBSAHOVÉ HROZBY	15
1.2.1 Pornografie	15
1.2.2 Násilí	16
1.3 ZÁVISLOST	17
1.3.1 Hraní her.....	17
1.3.2 Netholismus.....	18
1.3.3 Sociální sítě	19
1.4 ŠKODLIVÝ SOFTWARE	21
1.4.1 Malware.....	21
1.4.2 Virus	21
1.4.3 Trojský kůň	22
1.4.4 Ransomware	22
1.4.5 Adware	22
1.4.6 Spyware.....	23
1.4.7 Keylogger.....	23
1.4.8 Rootkit.....	24
1.4.9 Hoax	24
1.4.10 Sociální inženýrství	25
1.4.11 Spam.....	27
2 SOCIÁLNÍ SÍTĚ	28
II PRAKTICKÁ ČÁST	30
3 MOŽNOSTI RODIČOVSKÉ KONTROLY	31
3.1 OBECNÉ RADY A TIPY	31
3.2 POMOCÍ SOFTWARE	33
4 RODIČOVSKÁ KONTROLA	35
4.1 POČÍTAČE (PC), NOTEBOOKY	35
4.1.1 Rodičovská kontrola Windows	35
4.1.2 OpenDNS	38
4.1.3 WebLocker	40
4.1.4 PC Screen Watcher	41
4.1.5 ManicTime	44
4.2 MOBILNÍ TELEFONY	46
4.2.1 Obchod Google Play	46
4.2.2 Google Family Link	47
4.2.3 SecureKids	49
4.2.4 Kids Zone	52

4.2.5	Spyzie	53
4.3	WI-FI ROUTERY	54
4.3.1	Tenda F3 (F303) Wireless-N	54
4.3.2	Mikrotik RB952Ui-5ac2nD-TC	56
5	TESTOVÁNÍ A VYHODOCENÍ RODIČOVSKÉ KONTROLY	62
5.1	TEST APLIKACÍ NA PC	62
5.2	TEST APLIKACÍ NA MOBILNÍCH ZAŘÍZENÍCH	64
5.3	TEST NA WI-FI ROUTERU	66
	ZÁVĚR	68
	SEZNAM POUŽITÉ LITERATURY	69
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	71
	SEZNAM OBRÁZKŮ	72
	SEZNAM TABULEK	73
	SEZNAM PŘÍLOH	74

ÚVOD

Určitě si každý, hlavně rodiče a starší lidé, všimli, že každým rokem se vývoj civilizace posunuje a s tím také souvisí vývoj vyrůstání. Pokud se zaměřím na vývoj dětí v době před 30 lety a teď, tak zjistíme, že se doba za těch několik let posunula ohromně dopředu. Zatímco kdysi si děti hráli převážně venku a rodiče museli své děti nahánět, aby je dostali domů nebo jim dávat domácí vězení jako tresty, tak v dnešní době je tomu převážně naopak. Děti se musí vyhánět ven, aby celé dny neseděli u počítačů, mobilů nebo třeba před televizí. Dostat domácí vězení je dnes spíše odměnou než trestem, dítě tak může čas trávit na počítači, mobilu, u televize nebo u herní konzole jako je Play Station nebo Xbox. Stejným trestem jako bylo kdysi domácí vězení by bylo pro dnešní děti zakázání použití jejich chytrých zařízení, jako jsou mobilní telefony nebo třeba počítače.

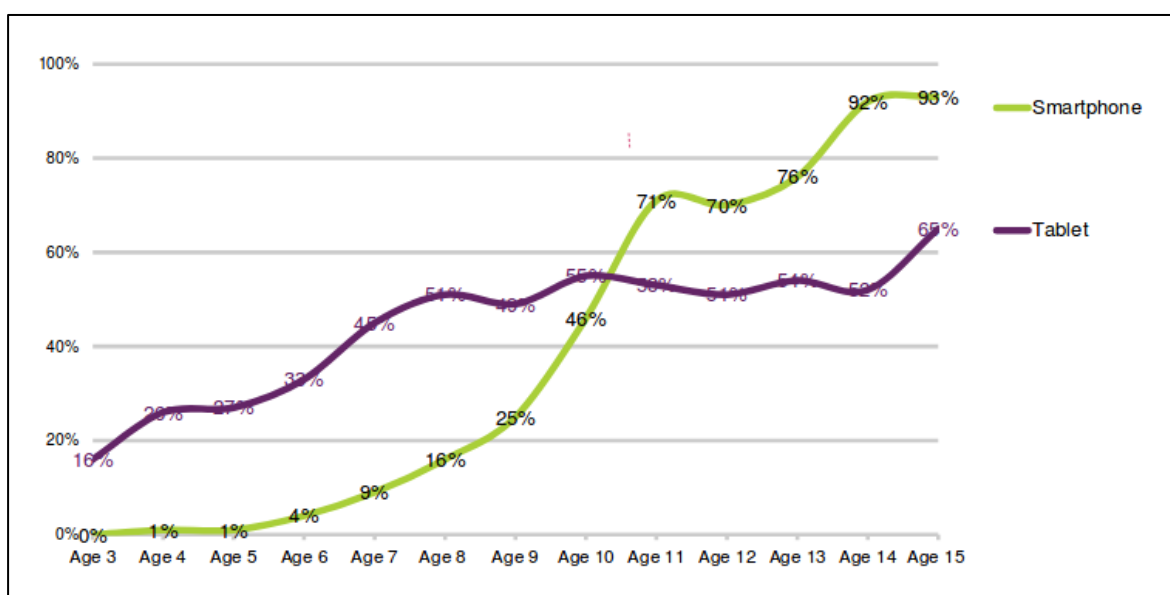
Dá se říci, že novodobé děti se narodili do světa digitálních technologií, a tak je pro ně vývoj přirozený než naopak pro jejich rodiče, kteří se s touto technologií seznamovali v průběhu svého dospívání. Zatímco dospělí byli zvyklí se bavit, seznamovat, řešit problémy a celkově komunikovat ve svých mladistvých letech z očí do očí, tak v dnešní době děti převážně komunikují pomocí počítačů, mobilů, tabletů a podobných novodobých technologiích. Vše má své výhody a nevýhody, práce se ale zaměří hlavně na nevýhody, a to konkrétně na rizika, které přináší tato nová doba informačních technologií (dále jen IT) pro vývoj každého dítěte, které je s touto technologií v kontaktu. Práce by měla upozornit všechny rodiče a nejen je, ale i samotné dospívající a děti na hrozby, které představuje informační technologie a jak těmto hrozbám předcházet nebo se jim vyvarovat.

Je důležité, aby rodiče měli zájem o to, co jejich děti dělají v tzv. online světě a mohli tak předcházet případným nebezpečím. Existuje spousta hrozeb od kyberšikany, pornografie až po závislost na hraní her nebo na IT obecně, kterým se práce bude věnovat více v dalších kapitolách a upozornit tak na jejich dopad ve vývoji dítěte. Každému nebezpečí jde více méně zamezit, a to jak upozorněním dítěte na danou hrozbu nebo využitím speciálních funkcí či aplikací, které se zabývají snížením rizika těchto hrozeb a dávají tak větší kontrolu rodičům nad tím, co jejich děti na zařízeních dělají. Důležité ale je, aby se rodiče chtěli naučit těmto novým věcem a uměli tak nastavit potřebná omezení pro své děti.

I. TEORETICKÁ ČÁST

1 HROZBY INFORMAČNÍ TECHNOLOGIE

Doba se mění, a to platí také v oblasti IT neboli informační technologie a dospívání. Každým rokem prakticky přibývá nová technologie, začalo to počítači, na začátku 21. století to byly mobilní telefony, k dnešnímu dni tu máme smartphony, tablety, chytré hodinky a spousta dalších vymožeností. To vše má ovšem dopad také na vývoj dětí a dospívání mladistvých. Na Internetu se objevila studie telekomunikační společnost Ofcom [8], ve které byl zveřejněn následující graf (Obr. 1), který ukazuje kolik procent dětí vlastní smartphone neboli chytrý telefon a kolik tablet [1][8].



Obr. 1. Procentuální znázornění dětí vlastníci telefonů podle věku [8].

Z výše uvedeného grafu je patrné, že dítě se už ve 3 letech dostane do kontaktu s IT konkrétně s tabletem a to hned 16 % dětí. Naopak mobilní telefony se na stejné procento dostanou až v osmém roku dítěte, zatímco tablety se nám v tomto věku vyšplhaly na něco málo přes 50 %. Od 11 let už poté vlastní smartphone až 71 % dětí, zatímco tablety se drží pořád kolem 50 %. V patnácti už máme mobilní telefony na 93 % a tablety na bezmála 70 %. Z těchto údajů si lze všimnout, že děti se nejprve dostávají do styku s tablety, a to už v útlém věku. Zlomovým rokem nastává 10.-11. rok, ve kterém tablety stíhají chytré telefony, které v tomto období zaznamenaly největší procentuální nárůst [8].

Existuje spousta hrozeb, které tato technologie vytváří, a proto je dobré si tyto hrozby nějak roztřídit, proto se zde vytvořilo několik skupin, do kterých se rozdělily nejznámější a nejvíce rozšířené hrozby na které může uživatel v online světě narazit. Jedná se o následující rozdělení:

1.1 Komunikační hrozby

Jak už název napovídá, budou zde patřit hrozby spojené s komunikací a je jedno zda to bude s osobou známou nebo ještě hůře neznámou, v obou případech se totiž může jednat o hrozbu. Tato skupina je ve vývoji dítěte asi tou nejvíce zásadní, jelikož zde může narazit na osoby, které ho mohou poznamenat na hodně dlouhou dobu a tím ohrozit jeho vývoj. Mezi komunikační hrozby se zařadilo několik pojmů, mezi ty nejznámější a nejdůležitější patří: [1]

1.1.1 Kyberšikana

Není tajemstvím, že děti na sebe můžou být hodné, ale taky zlé. V tom druhém případě se jedná o šikanu, která na světě existovala ještě před samotným vznikem IT. Jedná se vlastně nejen o fyzické, ale i psychické omezování nebo týrání jedince v kolektivu. S dobou IT se ale tento problém zvětšil a přenesl také do digitálního prostředí, kde se tento problém označuje jako kyberšikana. V podstatě se jedná o to samé jako je šikana, jen se vše odehrává v online světě a může se lišit v pár věcech. To znamená, že přes nějaký komunikační kanál je osoba napadnuta psaným projevem. Stejně jako u šikany jsou zde agresori, oběť a publikum.

Důležité je si taky uvědomit, kdy se jedná o kyberšikanu a kdy už ne. Například pokud si na sociální síti přečteme nějaký nelichotivý příspěvek a tím to končí, musíme to brát pouze jako názor. Pokud by se však v tomto pokračovalo dalšími a dalšími projevy či útoky, jednalo by se poté o kyberšikanu.

Kyberšikana může být v několika pohledech horší než šikana samotná, například v anonymitě. Agresor může stejně jako u šikany vystupovat pod svým pravým jménem, ale jde taky zaútočit na oběť v anonymitě, pomocí vytvořeného falešného účtu na sociální síti nebo e-mailu. Zařadit se zde může i čas nebo místo útoku, které na rozdíl od klasické šikany může přijít kdykoliv ať je to ráno, večer, o půlnoci, na dovolené nebo doma v pokoji a také kdekoliv třeba na sociální síti, pomocí SMS, e-mailu, zveřejněním videa apod.

Mezi kyberšikanu patří široká škála projevů, těmi vůbec nejčastějšími je ponižování, pomlouvání, nadávání, napadání, zesměšňování, vydírání, odhalování tajemství nebo Happy Slapping. Většina pojmů je jasná z šikany, jenom poslední pojem je novinkou, který se pojí pouze s kyberšikanou. U Happy Slappingu se jedná se o natáčení fyzického útoku na šikanovanou oběť a následné zveřejnění pořízeného videa na Internetu.

Bohužel kyberšikana je poměrně rozšířená, jelikož se snad každé dítě s tímto problémem setkalo, a to ať už v roli agresora, oběti či jako publikum. Ve většině bývá šikanovaným dítětem někdo, kdo se odlišuje od ostatních dětí, kteří si ho následně dobírají. Jde převážně o děti ze slabších sociálních rodin nebo děti z neúplných rodin.

Pro dítě kyberšikana představuje jednu z největších hrozeb, která může poznamenat celý jeho vývoj, a tak není radno si s tímto problémem zahrávat a rodič by se tak o tuto problematiku měl zajímat [1][3][6].

1.1.2 Kyberstalking

Kyberstalking neboli nebezpečné pronásledování vychází ze stalkingu, kde je oběť sledována, omezována nebo obtěžována. V IT tak je k tomuto využíván například mobilní telefon k rozesílání SMS zpráv nebo telefonátů, dále také Internet pro zasílání e-mailů nebo pro špehování a sledování na sociálních sítích.

Nejčastěji se kyberstalking objevuje například při ne zrovna vydařeném vztahu, přičemž je následně oběť, většinou dívka, sledována například pomocí sociální sítě. Jak bylo řečeno, využít se může i mobilní telefon k zasílání zpráv nebo opakovaných telefonátů. Může se taky stát, že útočník použije citlivé fotky, které mu byly zaslány obětí v průběhu jejich vztahu.

Často se taky stává, že útok je mířen na blízké okolí oběti, kdy se útočník snaží pomluvit oběť. Bohužel kyberstalking nezůstane většinou pouze v online prostředí, ale bývá podporován taky pronásledováním v reálném životě. V případě, že si dívka najde nového přítele, tak se snaží tohoto přítele od ní dostat pomluvami, fyzickými útoky nebo vydíráním [1][6].

1.1.3 Kybergrooming

Co by si měl každý pod kybergroomingem představit je manipulace s obětí. V podstatě se jedná o situaci, kdy na Internetu nějaká osoba vystupuje v roli pachatele, který se snaží na Internetu vytipovat jinou osobu neboli oběť. Cílem je získat její důvěru, která by měla vést k osobnímu setkání a následnému zneužití této osoby, nejčastěji se jedná o sexuální zneužití.

Do takové situace a se může dostat jak dospělá osoba, tak i dítě u kterého to jde snadněji, jelikož dnešní děti tráví spoustu času na Internetu a rády se seznamují s novými kamarády, je proto pro pachatele jednodušší si takovou oběť vyhlédnout a získat si ji. Z pravidla se obětí nejčastěji stávají dívky, a to ve věku mezi 11-17 lety [4], které nejsou tak oblíbené a můžou být třeba i obětí šikany, a tak při správném zvolení komunikace, mohou být lehkou kořistí pro útočníka.

Útočníci se ve většině případů vydávají za jinou osobu, než ve skutečnosti jsou, například o pár let staršího chlapce, než je vytipované dívce. Pro takové osoby je taky důležité vydržet si s obětí psát dlouhou dobu, tedy mít trpělivost a tím si získat její důvěru a informace o ní, díky kterým přizpůsobí konverzaci a další postup. Mohou také využít i dárky nebo podplácení k získání důvěry.

Kybergrooming je velmi nebezpečný, a to i ve chvíli, kdy si myslíte, že dítěti se nemůže nic stát nebo si to dokonce myslí samo dítě. Je to proto, jelikož k takové situaci může dojít doma, kdy je rodič rád, že má dítě pod dohledem. Dítě totiž může rodiči argumentovat, že si píše se svým kamarádem nebo kamarádkou, rodič se ale nemusí dále zajímat o jakého kamaráda jde a zda ho vůbec dítě zná, tím veškeré bezpečí mizí. Takzvanému kamarádovi poté stačí získat důvěru dítěte a následně ho vylákat na schůzku, proto by se rodič měl zajímat o to s kým si dítě píše a zda ho vůbec zná.

Typický průběh kybergroomingu:

- Vzbuzení důvěry a snaha izolovat oběť od okolí.
- Podplácení dárky, penězi, budování přátelského vztahu.
- Získání nebezpečných materiálů k případnému vydírání.
- Emocionální závislost oběti na útočnickovi.
- Osobní schůzka.
- Sexuální obtěžování, zneužití [4][6][12].

1.1.4 Sexting

Každým rokem je u dětí a mladých lidí stále více oblíbenější tzv. sexting, jedná se o složeninu slov sex a textování. Jak už název napovídá, jedná se o elektronické rozesílání nejen textových zpráv, ale převážně fotografií či videí se sexuální tematikou. Dost často poté bývají tyto záznamy jako jsou videa nebo fotografie zveřejněny na Internetu, nejčastěji se tak stává hlavně u mladistvých, když dojde k rozchodu neboli ukončení vztahu, kdy se následně jedna z osob uchýlí ke zveřejnění těchto citlivých záznamů za účelem zesměšnění či ponížení protějška.

Jedny z rizik, které sexting přináší jsou také případné rozpory se zákonem, pokud na takových záznamech je vyobrazena osoba mladší 18 let. V té chvíli se jedná o trestní čin šíření sextingu neboli pornografie, která je celosvětově zakázána, a tak se osoba, která zveřejní takový obsah dopouští protiprávního chování.

Sexting je nebezpečný hlavně z toho hlediska, kdy jsou potencionálnímu útočníkovi poskytnuty citlivé záznamy, které mohou být v budoucnu kdykoliv zneužity. Jedná se tak o takovou časovanou bombu, která může osobě, která je zveřejněna na takových materiálech, zadělat na problémy či ji vystavit posměškům okolí. Ve světě je zaznamenáno několik případů takového zneužití, v krajních případech některé události končí i tragédií, kdy zneužitá osoba nevydrží nátlak, sexuální útoky či posměšky, například ve škole nebo na Internetu a rozhodne se, že spáchá sebevraždu.

Je také důležité si uvědomit, že takový materiál může kolovat a šířit se na Internetu desítky let a je prakticky nemožné poté takové záznamy zcela odstranit. Děti a mladiství se většinou rozhodnou pro sexting z několika důvodů, přičemž si ale nedokáží uvědomit nebo připustit vysoká rizika spojená s tímto pojmem. Mezi nejčastější důvody, které vedou k sextingu rozhodně patří získání pozornosti nějaké konkrétní osoby (k seznámení, zalíbení), pocit povinnosti zaslat takový záznam za účelem udržení si vztahu či jeho vytvoření a v neposlední řadě může být dítě k takovému materiálu i donuceno (např. může být dívka donucena zaslat takový materiál pod nějakou výhružkou nebo ukončením vztahu).

Sexting ale neznamená pouze zaslání a zveřejnění fotografie nebo videa, ale zahrnuje také textovou formu komunikace, což může být flirtování, sexuální komentáře na sociálních sítích, zaslání sexuální nabídky, erotické SMS zprávy apod.

Prakticky jedinou a tím i nejúčinnější obranou proti sextingu je takové záznamy vůbec nevytvářet a už vůbec ne je zasílat druhým osobám, jelikož nikdy nevíte, co může se snímky třeba za několik let udělat [3][6][13].

1.2 Obsahové hrozby

Mezi další hrozby patří určité obsahové, pod kterými by si člověk měl představit fotografie, videa, články nebo nějaké určité stránky. Pro detailnější představu se jedná například o nepřístupné webové stránky určené pro osoby starší 18 let, dále se může jednat o fotografie nebo videa ve kterých se může objevit násilí. Obecně se bude jednat o problematiku zahrnující pojmy jako je pornografie nebo násilí [1].

1.2.1 Pornografie

V dnešní době je na Internetu možné narazit na spousty věcí, tím jsou také materiály nebo stránky, které se zabývají pornografií. Pornografie je velmi blízká sextingu, jelikož zde vystupují v hlavní roli také lechtivé materiály s tím rozdílem, že se tyhle materiály vytváří primárně za účelem jejich následného zveřejnění širokému spektru, kdežto u sextingu se tyto záznamy posílají určité osobě, například svému příteli/přítelkyni. V podstatě se dá tvrdit, že sexting je podkapitolou pornografie, jelikož za pornografií se považuje všechen materiál, který má za úkol vyvolat sexuální vzrušení.

Už dnes však pornografie tvoří nemalou část Internetového obsahu, a tak není vůbec těžké, aby se kdokoliv i děti k takovému obsahu bez problémů dostaly. V době před 20 lety se k takovým materiálům lidé mohli dostat jenom na specializovaných místech, v době Internetu se ale tomuto oboru mohou věnovat nejen specializované organizace, ale prakticky každý uživatel Internetu, který může takové materiály vytvořit a následně zveřejnit, což rozšiřuje Internetový obsah pornografie.

I když je pornografie přístupná osobám starší 18 let, dostat se k takovému obsahu na Internetu není problém, jelikož ve většině případů se webové stránky zabývající těmito materiály uchýlí pouze k pouhému upozornění, že je obsah stránek přístupný uživatelům starší 18 let. Takové opatření, i když je vloženo před samotnou stránkou je však pochopitelně velice slabé, jelikož uživateli/dítěti stačí aby v takovém upozornění pouze odsouhlasil, že jeho věk dosáhl 18 let, bez jakéhokoliv dalšího ověření.

Dítě se však může k takovému obsahu dostat také neúmyslně, například když mu vyskočí reklama na nějakých nezabezpečených stránkách na právě zmíněné tzv. pornostránky. Může také odkliknout nějaké upozornění, které bude v cizím jazyce a nebude mu rozumět, čímž neúmyslně potvrdí věk starší 18 let, aniž by to věděl.

Na takových webových stránkách specializujících se pornografií je také větší riziko nakažením zařízením některým škodlivým softwarem neboli malwarem, o kterém bude více napsáno v dalších kapitolách [1][2][5].

1.2.2 Násilí

Na Internetu však může dítě narazit také na materiály na kterých je vyobrazeno násilí jakéhokoliv druhu ať už se jedná o nenávistný obsah, pro-anorexii (jedná se o obsah který propaguje anorexii), sebepoškozování, týrání nebo dokonce vraždy. U filmů, videí či fotografií které se zveřejňují v TV se většinou uvádí, jestli se jedná o obsah, který je nebo není vhodný pro děti a mladistvé či je doporučeno sledovat pořad od určitého věku. V některých případech může rodič podle názvu pořadu či filmu poznat, zda se jedná o záznamy, které by dítě nemělo vidět, většinou jde o pořady s obsahem násilí označený například hvězdičkou.

Násilí na Internetu se může objevit prakticky kdekoliv i na sociálních sítích, kde bylo zaznamenáno už několik takových případů. Ne jednou se mohli lidé na Internetu dočíst nebo v TV slyšet o případech, kdy se na sociální síti Facebook zveřejnil živý přenos sebevraždy, k jeho odstranění došlo až po několika minutách či hodinách, a tak takové video mohlo shlédnout i několik tisíc uživatelů včetně těch mladistvých. Bohužel takovým videím na FB nejde zabránit, pouze je jde nahlásit a věřit v co nejkratší zablokování a odstranění takového záznamu.

Narazit se ale dá i na videa, která zaznamenávají vraždy, šikanu nebo také týrání zvířat, přičemž může dojít i k jejich usmrcení. Děti by před takovými materiály měly být varovány, a hlavně by se jim mělo dostat upozornění na existenci takových videí a poučení, jak v takových chvílích jednat. Takový násilný záznam může vystavit citlivější dítě klidně traumatu a poznamenat tak jeho výchovu nebo naopak se může v takových věcech začít vyžívat. Na Internetu existují i takové webové stránky, které takové videa nebo fotografie zaznamenávají a lze je shlédnout, i u těchto stránek sice vyskočí na uživatele upozornění s následným potvrzením jeho věku jako je u pornostránek, ale i zde se pravdivost tvrzení neověřuje [1].

1.3 Závislost

I když to může někoho překvapit, tak i v online světě IT se může člověk setkat se závislostí. Dříve si děti běžně hrály s míčem na hřišti, jezdily na kolech nebo hrály na schovávanou. Dnešní trend je takový, že děti se zabaví spíše svým mobilním zařízením, počítačem, herní konzolí nebo tabletem. Bohužel nadměrné používání těchto zařízení může vést k následné závislosti, a to bývá nejčastěji u dětí na: [1]

1.3.1 Hraní her

Podle všeho, je hraní her pro děti asi největší lákadlo, protože se u toho můžou zabavit na několik hodin denně, a navíc je to hrozně baví. Počítačové hry se každoročně více vyvíjí a stávají se rok od roku populárnější, a to nejen pro mladistvé a děti, ale také pro dospělé. Bohužel děti na rozdíl od dospělých neví, kdy mají přestat, a tak se u nich může projevit závislost na hrách i když si to samo dítě neuvědomuje.

Dítě si může vybrat ze široké škály her od sportovních, strategických až po RPG (dobrodružné hry, v překladu hry na hrdiny), online hry nebo v dnešní době hodně oblíbené hry ve kterých se za použití střelných zbraní snažíte usmrtit nepřátele a zůstat co nejdéle naživu. Jedná se o tzv. akční hry, které se často označují jako střílečky. Asi nejvíce lákavý žánr her jsou již zmínění střílečky, i když pro děti mladšího věku nejsou vůbec vhodné, a to z prostého důvodu a tím je zabíjení a střílení. Velmi oblíbenými jsou také RPG hry neboli dobrodružné hry, ve kterých se hraje za postavu neboli hrdinu, s kterou se prozkoumává rozsáhlá oblast mapy, kde se plní všelijaké úkoly a tím svoji postavu postupně vylepšuje.

V posledních letech jsou velmi oblíbené i online hry neboli multiplayerové, ve kterých nehraje hráč sám, ale jsou zde i další hráči. Děti tak zde mohou hrát se svými přáteli, ale také se mohou seznámit se i s novými a komunikovat spolu při hraní. Mezi nejznámější a nejoblíbenější online hru patří rozhodně „World of Warcraft“ neboli WoW.

Počítačové hry jsou a budou běžnou součástí vývoje většiny dětí a teenagerů. Rodiče, ale i samotné děti by měli pochopit, že nic se nemá přehánět nebo se z pouhé zábavy volného času může stát závislost. Existují samozřejmě příznaky závislosti na počítačových hrách, řada odborníků tvrdí, že problém se závislostí nastává, pokud se projeví aspoň 3 z následujících 7 příznaků závislosti [1][2][5].

Hlavní příznaky závislosti na hraní her:**Ztráta zájmů**

Problém nastává ve chvíli, kdy je pro hráče důležitější ne-li nejdůležitější hraní her, a proto se jeho myšlenky i v reálném světě točí kolem hraní.

Hraní jako řešení problémů

Jestliže se hraní nepoužívá jako zabavení, ale použije se k řešení nebo zapomenutí nějakých problémů, frustrace či zbavení negativních emocí.

Posouvání tolerance

V takovém případě závislému hráči nestačí určitá rozumná doba na hraní her, ale má potřebu si tento čas stále zvětšovat a rozšiřovat také portfolio svých her, aby se u něj objevili uspokojující a příjemné pocity z hraní.

Abstinenční příznaky

Důležitým příznakem je také abstinence, stejně jako například u alkoholismu to znamená, že pokud závislá osoba nemá zrovna možnost hrát nebo dlouho nehraje, tak se u takového člověka objeví abstinенční příznaky jako je nervozita, podrážděnost, v krajních případech i pocení nebo třesení.

Ztráta kontroly

Dost často dochází k nedodržení stanoveného času nebo herní doby, kdy takový hráč smí nebo nesmí zrovna hrát, a tak i přes vyčerpání svého času hraní přesto dále pokračuje. Patří sem i recidiva, kdy se hráč rozhodne úplně přestat s hraním, ale bohužel se mu to nepovede dodržet a k hraní se znovu vrátí.

Dopad na běžný život

Posledním příznakem je situace, kdy má hraní her přímý dopad na běžný život. Najednou pro takového hráče ztrácí význam škola, popřípadě práce, kamarádi, záliby a počítačové hry jsou pro něho přednější, což může mít za následek spory s okolím [1][2][5].

1.3.2 Netholismus

Závislost se však může projevit také na samotném Internetu, které má označení netholismus. V podstatě jde o závislost na všem, co je spojené s Internetem, od hraní online her, surfování po webových stránkách až po sledování videí nebo trávení času na sociální síti. Samozřejmě

závislým není každý, kdo využívá Internet, ale stává se jím jen ten, kdo ho využívá prakticky non-stop.

Rodiče mohou tuhle závislost u dětí snadno podcenit, jelikož vidí své dítě, jak si čte nejruznější články, sleduje videa, či chatuje s přáteli. Díky tomu jsou v přesvědčení, že si nemusí dělat vrásky na obličejích, když mají dítě doma v bezpečí a berou to tak, že se normálně baví na Internetu nebo se pomocí Internetu zlepšuje a zdokonaluje. Pokud však bude dítě trávit enormní množství času na internetu, může se na něm stát závislé.

Závislost na internetu má dost podobné příznaky jako je u hraní her nebo u závislosti obecně, proto zde budou uvedeny jednoduché otázky, na které se dá odpovědět buď ANO nebo NE. Čím více se dostane odpovědi kladných, tím spíše se jedná o závislého jedince. Otázky se mohou použít také na závislost u hraní her nebo sociálních sítích, kde se slovo Internet nahradí právě zmíněnými slovy.

- Zanedbáváte kvůli Internetu důležité věci ve svém životě?
- Narušuje Internet vztahy s významnými lidmi vašeho okolí?
- Bráníte se nebo jste rozrušení, když někdo kritizuje váš Internetový život?
- Vyčetl vám někdo pro vás důležitý váš Internetový život a byl při tom rozrušený?
- Zjistili jste někdy, že skrýváte před ostatními váš Internetový život?
- Snažil jste se toho nechat, ale nešlo to?
- Myslíte často na on-line záležitosti, i když jste off-line?
- Cítíte se nepokojný a rozzuřený, když se máte odpojit od Internetu?

Velmi typickým příznakem u těchto závislostí je zanedbaný spánek, kdy v tomto případě dá dítě přednost trávení času na Internetu před spánkem. Takže místo toho, aby šlo spát v 10 hodin, tak ulehne až po půlnoci, nejčastěji ještě s mobilním zařízením v ruce [2][4][9].

1.3.3 Sociální sítě

Kromě závislosti na Internetu obecně se může závislost také projevit na sociální síti. Může za to hlavně sociální síť Facebook (dále jen FB), která přišla s tím mít své přátele na této stránce, a tak s nimi komunikovat. Jelikož kromě kontaktu s přáteli nabízí FB také celou řadu dalších možností jako je hraní her, přidávání do skupin či uskutečňování obchodů, přidávání příspěvků apod., tak se tato sociální síť stala dnešním fenoménem a jedná se bezesporu o jednu z nejnavštěvovanějších stránek na světě. Narazit na někoho, kdo nemá založený účet na FB je dneska spíše rarita než normální věc.

Sociální sítě ale mohou potencionálně představovat mnoho rizik hlavně pro děti a mladistvé. Pro spousty lidí, hlavně u osob do 18 let, je důležitější budování vztahů a komunikace na sociálních sítích než ve skutečném životě. Pokud má dítě nutkání být neustále na Facebooku a sledovat, kdo co přidal nového, který přítel kde je, co dělá nebo co sdílel, dá se už pomalu mluvit o závislosti. Pokud se k tomu ještě přidá snaha neustále své přátele zásobovat novými příspěvky o tom co dělá, co se mu přihodilo, fotkami, počítáním „to se mi líbí“ tzv. lajků nebo komentářů, tak se jedná o závislost.

Stejná závislost jako na FB se může projevit na kanálu YouTube, kde dítě může být závislé na sledování videí svých oblíbených youtuberů. V poslední době se taky do popředí dostal Instagram, který slouží pro nahrávání převážně fotografií, které jsou sdílené se světem a přidáváním tzv. „My Stories“, což jsou fotografie nebo videa, která jsou zveřejněné pouze na 24 hodin. I na těchto sítích se může dítě stát závislé, pokud na něm tráví enormní množství času a má potřebu neustále komentovat, přidávat či dávat příspěvkům „to se mi líbí“ což se mezi uživateli této sítě označuje jako lajkování [2][4][6].

1.4 Škodlivý software

Velmi důležitou kapitolou je také škodlivý software, který se snaží infikovat zařízení nejčastěji počítače a tím je tak přimět dělat co útočník přikáže. V dnešní době se s počítačovým virem či malwarem obecně uživatel setká a ani o tom nemusí mít vůbec ponětí, jelikož tento škodlivý software se vyvíjí a díky tomu se dnes dokáže maskovat.

Obecně se škodlivému softwaru říká malware, pod tento pojem spadají všechny počítačové viry, které se snaží získat kontrolu nad zařízením a využít ho tak pro své vlastní účely. Proto se také tyto viry v dnešní době snaží být co nejhůře odhalitelné, aby tak mohli co nejdéle a nejlépe sloužit svým tvůrcům tedy útočníkům. Ti se následně přes tyto zařízení snaží rozesílat dále svůj nebezpečný kód ukrytý v softwaru a napadat tak další stovky nic netušících lidí na jejich počítačích. Jakmile se takový malware dostane do zařízení, tak začíná ihned s tzv. hackováním, což je činnost nabourávání se do systému počítačů za účelem získání informací. To může mít za následek rozesílání nevyžádané pošty, spamů, získávání informací nebo také odposlouchávání zařízení.

Existuje spousta škodlivých softwarů, přičemž se každý zabývá napadením něčeho jiného. Práce se pokusí vyjmenovat a popsat vůbec ty nejčastější termíny spojené se škodlivým softwarem, jednoznačně sem budou patřit tyto pojmy jako je malware, virus, Trojský kůň nebo například Spyware [1][10].

1.4.1 Malware

Malware vznikl ze dvou anglických slovíček „malicious“ a „software“, při čemž prvně zmíněné slovo znamená v překladu zlomyslný či škodlivý. Jak již bylo zmíněno výše, malware je veškerý škodlivý neboli nebezpečný software, obecně se tedy jedná o takovou kapitolu, do které patří všechny dále zmíněné softwary jako podkapitoly. V zásadě se jedná o nějaký kus kódu, který byl vytvořen za účelem infikování zařízení, nejčastěji počítače nebo mobilního zařízení a tím jej přimět dělat co si útočník bude přát [10].

1.4.2 Virus

Za počítačový virus je v zásadě označován software nebo část programového kódu, která se spustí bez vědomí uživatele. Cílem takového viru je získání kontroly nad počítačem nebo nějaké jeho části a následné šíření do dalších zařízení. K šíření využije již infikované zařízení, které využije jako prostředek pro své další šíření. Na počítačový vir dnes uživatel narazí

jen zřídka, jelikož je vytlačován a nahrazen daleko sofistikovanějšími formami útoků, jelikož si s takovým virem dokáže již dnes poradit praktický každý antivirový program [10].

1.4.3 Trojský kůň

Trojský kůň získal své pojmenování podle dřevěného koně, který sehrál hlavní roli při dobytí bájně Troje, tento dřevěný kůň zprvu představoval jakýsi dar, ve skutečnosti ale bylo v útrobách ukryto několik válečníků, kteří se posléze zmocnili města. Podobné je to také i u trojského koně, kde je kus škodlivého kódu ukryt v programu, který zprvu vypadá užitečně, většinou se jedná o legitimní programy, ve kterých bývá tento kód skryt a následně propagován do zařízení.

Cílem je získání možnosti ovládnutí zařízení uživatele útočníkem, manipulování a mazání dat, získání hesel apod. Na rozdíl od počítačového viru se zpravidla nesnaží o další šíření z napadnutého zařízení [4][10].

1.4.4 Ransomware

Ransomware je dalším druhem malwaru, který když se dostane do zařízení, tak má za úkol zpravidla zablokovat uživateli počítače přístup k nějaké jeho části v systému, například k fotografiím, souborům, videím atd. Dnes se již spíše snaží zašifrovat nějaké vybrané soubory na zařízení, následně se pokouší jejich uživatele vydírat. V tomhle případě se jedná o tzv. kryptovirální vydírání, kdy se neplatí převodem reálných peněz, ale je vyžadována virtuální měna Bitcoin.

Dříve bylo pravidlem, že po zaplacení se vám soubory zpřístupnily, dnes tomu tak již spíše není, a tak se nedoporučuje platit. I na tento malware totiž už existují spousty aplikací, které jsou schopny odšifrovat napadené soubory a uvést je zpět do původního stavu [4][10].

1.4.5 Adware

Adware není nijak nebezpečný, ale bezesporu jde o velice otravnou a nepříjemnou věc. Jednoduše se jedná o takový software, který se po zabydlení v počítači postará o to, aby vyskakovaly reklamní okna nebo aby při brouzdání po Internetu bylo vidět daleko více reklam či takové reklamy, které tvůrci adware chtějí. Naštěstí adware nepředstavuje žádné větší nebezpečí, existují ale takové programy, které se snaží shromažďovat osobní informace nebo sledovat historii, což určitě nikdo nechce.

Jelikož dnes jsou často vyměňovány pouze reklamy na Internetu za jiné, tak je adware kolikrát těžko zjištělný. Pokud však uživatel zaregistruje, že se mu na PC objevuje daleko více reklam než dříve, byla změněna domovská stránka nebo se zobrazuje reklama, i když neprochází žádnými webovými stránkami, tak dost pravděpodobně má v počítači adware [4][10].

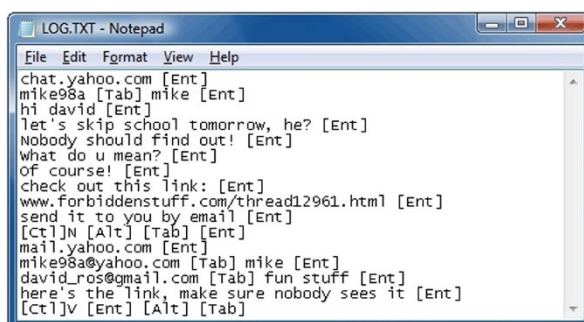
1.4.6 Spyware

V tomto případě se jedná o tzv. špionský program, který má za úkol špehovat a sbírat informace o uživateli ze zařízení. Jde o velice těžko odhalitelný malware, který může shromažďovat snímky obrazovek, bankovní nebo osobní údaje, osobní soubory a fotografie nebo historii prohlížení. Následně tyto informace rozesílá třetím stranám bez vašeho vědomí.

Stejně jako většina malware se i tento software dostane do zařízení pomocí jiného programu nebo při otevření infikované přílohy. Jak bylo napsáno, velice těžko se spyware odhaluje, ale pár znaků existuje. Pokud se například objeví v hlavním panelu nějaké nové, a ještě k tomu neznámé ikony programů, vyhledávací dotazy jsou přesměrovány do jiného vyhledávače nebo při provádění běžných operací vyskakují podivné chybové hlášky je to náznak toho, že se v zařízení objevil spyware [4][10].

1.4.7 Keylogger

Jedná se o jeden z typů spywaru, který je pro uživatele dost nebezpečný, jelikož keylogging dokáže odposlouchávat a zaznamenávat všechny znaky, které se na klávesnici zapíší. Program následně tyto znaky pošle na předem určený server, kde se k těmto informacím dostanou hackeri. Útočníci tak můžou například zjistit hesla, přihlašovací údaje, čísla platebních karet, emailové zprávy apod. a tím se tak dostat na vaše účty.



Obr. 2. Výstupní data z keylogeru [4].

Keyloggery se ale také využívají jako legitimní monitorovací prostředek pro monitorování činnosti uživatele, např. kontrola dítěte rodiči. Na Obr. 2 jsou vyobrazeny výstupní data z keyloggeru, ze kterých se dá jednoduše zjistit co daný uživatel na zařízení dělal a co psal.

Hned z prvního řádku lze vyčíst, že sledovaný uživatel navštívil webovou stránku „chat.yahoo.com“. Druhý řádek potom ukazuje, jaké uživatelské jméno zadal, v tomhle případě se jedná o „mike98a“ a také jaké použil heslo „mike“. Na dalších řádcích poté lze vyčíst, co v chatu napsal a poslal [4][10].

1.4.8 Rootkit

Dalším dosti nebezpečným a nepříjemným malwarem je Rootkit, který byl hackery sestaven a navržen tak, aby pomocí tohoto programu získal přístupová práva administrátora na zařízení. Odhalení tohoto malwaru je velice obtížné, jelikož antivirové programy musí prohledávat všechny programy a zároveň sledovat všechny procesy a jejich závislosti [10].

1.4.9 Hoax

Hoax se do češtiny dá přeložit jako výmysl, poplašná neboli falešná zpráva. Většinou se jedná o nějakou zprávu, která varuje před neexistujícím nebezpečím nebo virem a je sestavena tak, aby se tato zpráva mohla šířit dále pomocí přeposílání nebo sdílení. Právě ono zmíněné sdílení/přeposílání je takovým základním a nejhlavnějším znakem hoaxu.

Proč vůbec takový hoax vznikl a k čemu slouží? Primárně se snaží vyvolat strach pomocí popsaného neexistujícího nebezpečí. Dále se snaží šířit falešné zprávy, dělat si legraci z důvěřivých lidí, manipulovat s názory lidí, přilákat pozornost nebo dokonce poškodit nějakou značku, firmu nebo třeba výrobek.

Existuje několik druhů hoaxu, kterým se věnuje specializovaná stránka hoax.cz, která ve své databázi uvádí nejčastější hoaxy, které jsou zaměřené na:

- Varování před smyšlenými viry a různými útoky na počítač.
- Varování před reálnými hrozbami mimo IT.
- Falešné prosby o pomoc.
- Petice a výzvy.
- Pyramidové hry a různé snadné výdělky.
- Řetězové dopisy štěstí (pověřivost).
- Žertovné zprávy [11].

1.4.10 Sociální inženýrství

Sociální inženýrství v IT znamená způsob manipulace lidí neboli uživatelů za účelem získání důvěrných informací nebo k přesvědčení určitého jednání. K tomu útočníkům vystačí využít lidské hlouposti, nebezpečnosti a naivity a má prakticky vyhráno.

Sociální inženýrství má několik metod jak lidi tzv. obalamutit (oklamat) a získat od nich důležité informace, mezi nejznámější a nejpoužívanější patří: [4][10].

Pharming

Pharming je podvodný útok, jehož úkolem je infikovat počítačový systém tak, že když se bude chtít uživatel přihlásit přes tento infikovaný PC do svého Internetového bankovníctví, tak ho speciální programy přesměrují na falešné Internetové bankovníctví. Tyto programy totiž umí napadnou DNS, což je doménový server a přepsat tak IP adresu a tím uživatele mohou přesměrovat tam, kde si to útočníci přejí. Na této falešné stránce je poté uživatel donucen zadat své přihlašovací údaje spolu s heslem v domnění, že se dostane do svého zabezpečeného bankovníctví, místo toho ale poskytne své údaje útočníkům.

Každá taková podvodná stránka má své charakteristické rysy. Lze tak poznat, zda se jedná o falešnou stránku, a to následovně podle:

- Nestandardního chování Internetového bankovníctví, jako je zobrazení formuláře pro zadání důvěrných údajů apod.
- V adresním řádku je adresa, která je podobná, nepatrně změněná nebo diametrálně zcela odlišná, než jsou oficiální stránky napodobené organizace nebo banky.
- Komunikace probíhá na nezabezpečeném protokolu `http://` místo zabezpečeném `https://` a označeném symbolem visacího zámku, který používá drtivá většina dnešních webových stránek, díky jejich zabezpečenému přenosu [4].

Phishing

Phishing jsou podvodné e-mailové útoky za účelem získání důvěrných informací nejčastěji přihlašovacích údajů, hesla, PINy apod. Útočníci se snaží nejčastěji získat přístup k bankovnímu účtu, ale není to pravidlem, jelikož se také mohou pokusit získat přístup k PayPalu (jedná se o Internetový platební systém), Googlu nebo třeba eBay, kde dochází k manipulaci s penězi nebo jednoduše lze zneužít jejich služeb. V dnešní době k založení bankovního účtu nezletilých osob stačí pouze souhlas rodičů a registrace na jiných stránkách není kolikrát ani podmíněna věkem, proto se tento problém může týkat i dětí.

Phishingové zprávy se snaží vyvolat dojem, aby si příjemce této zprávy myslel, že jde opravdu o zprávu z důvěryhodných zdrojů jako je PayPal, banka uživatele, Česká pošta apod. Jelikož zpráva je velice dobře graficky napodobena, tak neobezřetný uživatel nepozná, že se jedná o podvod. Většinou se v takové zprávě píše, že je potřeba aktualizovat či potvrdit informace a byl tím nucen zadat své přihlašovací údaje. K tomu se využívá ve zprávě odkaz neboli link na webové stránky organizace (banky), který na první pohled opět vypadá věrohodně, ale při bližším prozkoumání lze zjistit, že se jedná o odkaz odkazující na podvodnou stránku, která díky zadání přihlašovacích údajů získá tyto údaje.



Obr. 3. Příklad phishingu neboli podvodného e-mailu od České spořitelny.

Na Obr. 3 si lze všimnout základních charakteristik podvodného e-mailu, které byly zmíněny na začátku kapitoly. Phishing obsahuje odkaz na přihlášení, který uživatele přesměruje na podvodnou stránku, dále vypadá graficky velmi věrohodně a v neposlední řadě si lze všimnout, že odesílatel se sice jmenuje SERVIS 24, ale jeho e-mailová adresa není věrohodná.

Obecně si stačí zapamatovat, že banky takové zprávy, ve kterých by žádaly uživatele (svého klienta) o přihlášení přes odkaz ve zprávě neposílají a jedná se tedy v takovém případě vždy o phishing.

Nejlepší obranou proti phishingu je neklikat na odkazy v e-mailech, které mají uživatele údajně přesměrovat na webové stránky organizace, raději by si měl uživatel danou stránku

vyhledat sám pomocí ručního zadání do vyhledávače. Není také na škodu si dát pozor na překlepy při psaní adresy, jelikož podvodníci mohou zaregistrovat adresu podobnou té oficiální, například místo mBank je uživatelem zadáno nBank, která může vizuálně vypadat naprosto stejně jako pravá stránka, a tak si uživatel nemusí všimnout své chyby, a přitom bude na falešné webové stránce. I v tomhle případě jde použít stejný postup pro zjištění, zda se jedná opravdu o podvodnou stránku jako u pharmingu [10][11][12].

1.4.11 Spam

Spam je ve většině případů pouze velice otravný, ale může uživateli nadělat také problémy, pokud na takový spam naletí. Jednoduše si pod spamem lze představit hromadné rozesílání nevyžádané elektronické pošty, nejčastěji přes e-maily většinou jako reklamy.

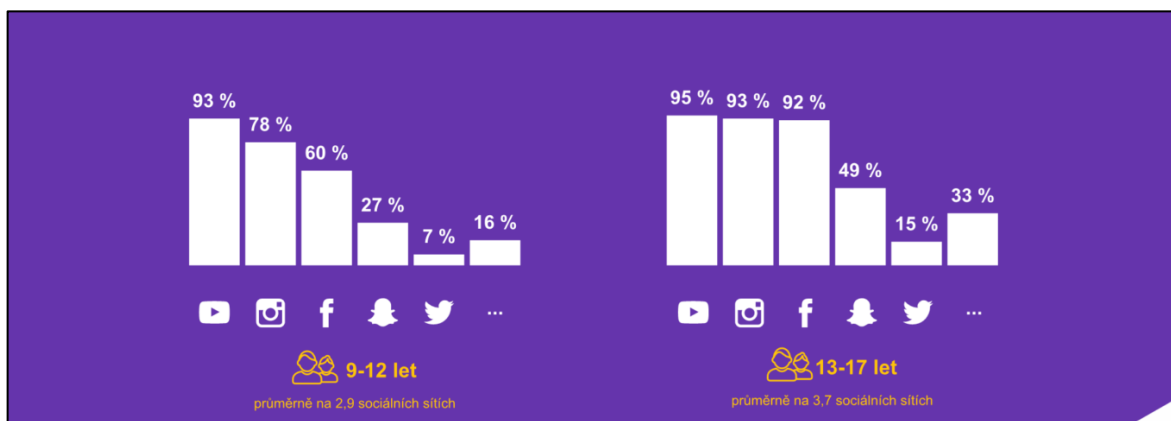
Bohužel v dnešní době nezůstalo pouze u zasílání reklamního sdělení, ale pomocí spamů se také rozesílá různý malware, který se vám po otevření takové zprávy dostane do zařízení. Pomocí spamu se také rozesílá, již zmíněný phishing pro získání citlivých údajů.

Jak proti takovému spamu bojovat? Prvním krokem je nezasílat a nezveřejňovat své emailové adresy všude, kde si o to stránky řeknou. Pokud však má uživatel podezření, že mu došel spam, doporučuje se takovou zprávu raději ihned smazat. Dnešní emailoví klienti drtivou většinu takových zpráv rozpoznají a automaticky je přesouvají do složky SPAM, která smaže všechny zprávy, které se zde nacházejí déle jak 30 dní [10][12].

2 SOCIÁLNÍ SÍTĚ

Poslední popsanou skupinou hrozeb jsou sociální sítě, které v posledních letech zažívají obrovský boom, který se projevuje ve změně společnosti, hlavně u dětí a mladých uživatelů těchto sítí. Proto taky snad neexistuje dítě, které by právě sociální síť nemělo, i když věková hranice pro založení účtu na FB je 13 let. S tím jsou spojené nejen výhody používání těchto sítí, ale také se zde objevuje velké množství rizik, které si je třeba uvědomit.

A co to vlastně sociální síť je? Jedná se o Internetovou službu, která svým uživatelům umožňuje vytvořit svůj vlastní profil, díky kterému lze komunikovat s přáteli, sdílet své osobní údaje, fotografie, videa, nálady apod. Právě zveřejňování věcí a komunikace představuje pro mladistvé největší riziko, které může někdo zneužít [1][2][4].



Obr. 4. Využívání sociálních sítí podle věkových skupin [7].

Z výše uvedeného grafu (Obr. 4) z roku 2018, který vytvořil Avast je patrné, které sociální sítě využívají děti jednotlivých věkových skupin. Ve věkové skupině od 9 do 12 let je nejvíce oblíbený kanál YouTube (90 %), který slouží pro sledování videí v dnešní době oblíbených tzv. Youtuberů. Největší riziko ovšem představují sítě umístěné na dalších místech a tím je Instagram (78 %), Facebook (60 %) a také Snapchat (27 %). Ve věkové skupině od 13 do 17 let využívá první 3 sociální sítě více než 90 % uživatelů [7].

Facebook

Nejvíce nebezpečnou sociální sítí tak může být Facebook, který toho uživatelům nabízí nejvíce a tím pádem se zde vyskytuje také více potenciálního nebezpečí. Facebook je v zásadě nejpopulárnější sociální sítí, a to nejen v České republice, ale i ve světě společně s YouTube. V České republice je registrováno 4,2 milionu aktivních uživatelů, z nichž 11 % je ve věku 13–17 let [6].

Jelikož je Facebook určený pro osoby starší 13 let, tak se lze setkat i s případy, kdy si účet na této síti založí dítě mladšího věku, což ukázal i graf výše, který vykazoval, že až 60 % dětí ve věku 9-12 let využívá Facebook. Už tím, že se tak mladé dítě na danou síť zaregistruje, tak se vystavuje zbytečnému nebezpečí.

Jedním z největších rizik je vyplnění osobních informací a údajů v profilu uživatele. Tyto údaje totiž mohou být zneužity, proto bychom měli vyplňovat pouze údaje, které jsou povinné. Vyplněním více informací, dává uživatel možnost všem dalším členům se podívat do jeho vlastního soukromí a dát jim informace týkající se například zálib, adresy bydliště, věku, práce, rodiny, fotek, událostí apod., které mohou být zneužity. Mladí se také často snaží spíše o ochranu svých dat před rodiči než před cizími lidmi, kteří se mohou stát potenciálními hrozbami. Dělají tak z toho důvodu, aby zabránili rodičům v případném špehování, jelikož by mohli uvidět fotky nebo komunikaci mezi kamarády, ale že je může sledovat někdo cizí už na zřetel neberou, protože si nedokáží uvědomit potenciální nebezpečí.

Další nevýhodou Facebooku je také to, že se zde může dítě či mladistvý setkat s hrozbami, které byly pojmenovány a vysvětleny výše, jako je kyberšikana, kybergrooming, kyberstalking, sexting apod. V tomto případě je zde Facebook jako takový nástroj těchto hrozeb, které můžou dítě potkat.

Děti, ale vůbec všichni uživatelé Facebooku by si měli dávat pozor a více uvažovat také nad tím co zveřejňují, protože je může zveřejněný příspěvek, názor či nějaká fotografie přijít v budoucnu pěkně draho. Jako příklad se zde uvede třeba hledání zaměstnání, kdy v dnešní době se stává pomalu zcela běžným, že si personální pracovníci prověřují uchazeče i pomocí Internetu, a ne jenom podle zaslaného životopisu či pohovoru [2][4][6].

II. PRAKTICKÁ ČÁST

3 MOŽNOSTI RODIČOVSKÉ KONTROLY

V zájmu každého rodiče je předejít výše zmíněným hrozbám nebo alespoň učinit kroky k jejich předcházení. Existuje spousta programů, které dokáží kontrolovat, zakazovat a povolovat určité věci, které rodič požaduje na zařízeních dětí nebo ke kterým mají přístup. Možnosti rodičovské kontroly neboli jak předejít výše popsáním problémům by šlo rozdělit na 2 velké skupiny:

1. Obecné rady a tipy.
2. Kontrola pomocí softwarů.

Rodič by se měl věnovat oběma skupinám, aby tím zvýšil pravděpodobnost vyhnout se nežádoucím problémům, které může jejich dítě potkat v online světě. Některým hrozbám jde velice účinně předcházet, jiným zase hůře, nicméně v obou případech je důležité se o to pokusit a zmenšit tím riziko hrozeb IT pro dítě.

3.1 Obecné rady a tipy

Rodič se od narození svého potomka snaží své dítě vychovávat, jak nejlépe umí a předávat mu své zkušenosti a postřehy. Stejně tak by to mělo fungovat i v online světě ve kterém se používají zařízení jako jsou mobilní telefony, počítače nebo tablety. V první řadě by si měl každý rodič uvědomit a rozhodnout, kdy je podle nich ten správný čas začít dítě seznamovat s IT, jelikož dnešní doba se bez těchto vymožeností jen těžko obejde a v budoucnu by se na těchto zařízeních mohla stát doslova závislá. Pokud se začne dítě dostávat do kontaktu s informační technologií jako je například mobilní telefon nebo tablet už v útlém věku, hrozí zde hned několik rizik. Naopak pokud se mu bude tato technologie zakazovat a oddalovat, může hrozit, že se nesžije tak rychle a úplně s dnešní dobou, což může mít za následek pomalejší rozvoj v IT a třeba i posměšky od ostatních dětí apod.

Velice často rodiče v dnešní době využívají mobilní telefony nebo tablety k uklidnění svého neposlušného nebo zrovna plačícího dítěte, jelikož se jedná o nejjednodušší způsob, jak docílit klidu a pokoje od svých dětí alespoň na chvíli. Rodič by si ale měl uvědomit, že dítě je v tomhle věku ve vývoji, ve kterém začíná poznávat svět a okolí a že to může mít za následek i zdravotní potíže. Odborníci se shodují, že by se dítěti do 3 let neměla v rukou objevit žádná elektronika, časté používání IT zařízeních totiž může mít za následek poškození zraku, nespavost nebo může také zpomalit růst svalů [14]. Dále se také shodují, že by dítě nemělo vlastnit mobilní telefon dříve než s nástupem do 3. třídy, tedy kolem 10. roku života, mělo

by se postupně seznamovat s touto technikou až do chvíle, než na ni bude připraveno [14]. První rada tedy zní: rozhodnout se a zvážit, kdy je vhodné začít dítě seznamovat s IT a kdy jim pořídit jejich vlastní mobilní telefon nebo tablet.

Není také od věci si s dítětem, které začíná používat PC nebo mobilní telefon spolu s Internetem promluvit o tom, jak by se na takovém zařízení měl chovat, a dále ho varovat před hrozbami s kterými se může setkat. Pokud se vezmou v potaz komunikační hrozby, které byly rozebrány na začátku práce, mělo by se dítěti vysvětlit, jak by se při komunikaci s kamarády měl chovat, případně se s vyskytnutými problémy svěřit rodičům. To samé platí i při komunikaci s cizími lidmi či s uživateli, které na Internetu poznalo. Mělo by se jim dostat upozornění, že s takovými lidmi by se do komunikace dávat neměli a když už, tak velice opatrně a v žádném případě jim nezasílat žádné osobní či jiné důležité informace. To platí také na zasílání fotografií obličeje nebo intimnějších snímků, které by se neměli vůbec vytvářet.

Upozornit by se také mělo na hrozby spojené s obsahem, které se mohou na Internetu objevit, o jaké hrozby jde se už psalo v kapitole 1.2 Obsahové hrozby. Děti by měli mít povědomí o webových stránkách, ke kterým by měli mít přístup pouze dospělé osoby tj. starší 18 let a v případě, že se na takovou stránku dostanou nebo budou požádáni o potvrzení věku 18 let, tak aby okamžitě takové stránky opustili. To samé se dá říci i o falešných reklamách, například o falešných vyskakovacích oknech, které hlásí, že jste se stali výhercem mobilního telefonu. Dítě by mělo vědět, že by takovým reklamám nemělo věřit a klikat na ně.

Nemělo by se také zapomínat omezit čas, má se tím na mysli dobu používání zařízení ať už na něm dělá cokoli. V první řadě by se rodiče měli zajímat o to, co dítě dělá v online světě, ale také omezit čas strávený v tomto prostoru. Stejně jako se kdysi omezovala dětem televize, by se měla omezovat dnešní technika v podobě mobilů, tabletů, herních konzolí nebo počítačů. Rodič by si měl jednoznačně ujasnit pravidla, za jakých podmínek, může dítě využívat IT nebo alespoň omezit tento čas na nějakou únosnou hodnotu. Nejběžnějšími podmínkami jsou dobré známky ve škole, plnění povinností, poslouchání, dobré chování, u takového dítěte by s omezováním neměl být problém. Pokud by však dítě vykazovalo opačné výsledky, je namístě takovému dítěti používání moderních zařízení zakázat nebo alespoň omezit. Jestli však rodič se svým dítětem žádné takové pravidla nemá, měl by se alespoň zajímat o to, zda dítě nežije pouze Internetem nebo hraním her, pokud ano, bylo by na místě zakročit a zdravě zakázat nebo omezit pobyt na zařízeních, aby se předešlo případné závislosti, jelikož nic se nemá přehánět a u IT to platí dvojnásob.

Dítě by mělo dostat zároveň i povědomí o škodlivých softwarech, které mohou nakazit zařízení a o tom, jak k takovému malwaru mohou přijít. Nejlepší volbou je dítěti zakázat stahování ať už se jedná o filmy, programy, hudbu nebo hry, a to bez svolení rodiče, čímž se může předejít stažení nějakého pofigidního souboru, který by mohl obsahovat malware. Upozornit by se určitě mělo i na sociální inženýrství, spam či hoax a neuvádět důvěrné informace všude, kde si o to řeknou, ale pouze na důvěrných a ověřených stránkách.

Pokud jde o sociální sítě jako je Facebook, Instagram nebo Twitter a děti, není od věci, aby rodič účet svého dítěte sledoval nebo si ho přidal do přátel, a měl tak aspoň přehled o tom, co jeho dítě zveřejňuje a sdílí. Upozornit by se tak před založením a používáním sociální sítě mělo na to, že co se zveřejní zůstane na Internetu navždy [14][15].

3.2 Pomocí softwaru

Druhou kategorií, jak by rodič mohl mít kontrolu nad tím co jeho dítě dělá na chytrém zařízení, je využití nějakého programu/aplikace, který má určité funkce pro kontrolu nad tím, co dítě na zařízení dělá. Dneska již existuje spousta speciálních aplikací, které mají možnosti, jak upravovat rodičovskou kontrolu a ovlivňovat tak částečně pobyt dítěte v online prostředí.

Jednu takovou aplikaci obsahuje také samotný operační systém Windows, který nese název Rodičovská kontrola Windows, ve kterém může rodič nastavit určitá pravidla. Aplikace jdou ale také stáhnout z Internetu, takže výběr je opravdu veliký. Drtivá většina domácností v dnešní době využívá také Wi-Fi routery, díky kterým se mohou připojit k Internetu další zařízení používající službu Wi-Fi. Z tohoto zařízení se tak lze připojit k Internetu bezdrátově (mobily, tablety, notebooky), tak i drátově (počítače), a proto se také dají nastavit určitá opatření už v těchto zařízeních, jako je zamezení určitých webových stránek nebo omezení času.

A o jaké omezení se vlastně jedná? Jelikož na Internetu existují nebezpečné nebo nevhodné stránky, které by mohly děti navštívit, jednou z možností těchto aplikací je nastavení, které stránky budou dětem nepřístupné. Zakázat se tak mohou konkrétní stránky nebo se zakáží pouze určitá slova, které se na stránce mohou objevit, čímž vlastně může rodič ochránit své dítě nejčastěji před pornografií a násilím. Není špatné také dětem vysvětlit, proč jim jsou některé stránky zablokovány nebo proč nemohou hrát určité online hry.

Dalším omezením, může být nastavení, kdy se dítě může připojit k Internetu, tím tak může rodič zakázat, že se Internet nesmí používat mezi zadanými hodinami například, když je

rodič zrovna v práci. Tato metoda nastavení se využívá na internátech neboli na ubytovacích zařízeních pro středoškoláky, kde je jim odepřen přístup k Internetu nejčastěji od 22:00 hod večerních do 6:00 hod ranních. Omezit se také může pouze čas bez ohledu na to kolik je zrovna hodin. Má se tím na mysli třeba omezení po dvou hodinách činnosti na Internetu, kdy je následně přístup k Internetu odepřen.

Některé aplikace také dokáží monitorovat co dítě na mobilním zařízení nebo počítači dělá, tzn. že sbírá data o používání zařízení, které následně rodiči poskytne, ten tak může shlédnout, co vše dítě dělá nebo dělalo na sledovaném zařízení, sledovat tak může s kým telefonoval, posílal si SMS zprávy nebo co dělal na Internetu či jakou hru hrál. Spravovat se také mohou i aplikace, které dítě používá, což znamená že rodič může schvalovat nebo blokovat aplikace, které si chce dítě stáhnout do mobilu. Zaznamenávat se také mohou stisknuté klávesnice na počítači nebo náhodné snímání obrazovky což je takzvaný screenshot.

V takových speciálních aplikacích, které se věnují rodičovské kontrole jde v podstatě již dneska zakázat, blokovat nebo sledovat prakticky vše, tato práce se proto v dalších kapitolách bude věnovat právě rodičovské kontrole pomocí nejrůznějších aplikací a jejich nastavení.

4 RODIČOVSKÁ KONTROLA

Vzhledem k tomu, že v dnešní době děti vlastní nebo alespoň mají přístup k širokému spektru chytrých zařízení, měla by se rodičovská kontrola týkat právě těchto zařízení jako jsou mobilní telefony, počítače nebo tablety. Práce je zaměřená na zařízení, na kterých budou vyzkoušeny nejrůznější softwary, zaměřené na kontrolu dětí v online světě, které jsou dostupné zdarma a následně se vyberou ty aplikace, které budou shledány nejvíce účinnými či vhodnými. Seznam všech použitých aplikací se najde v Příloze PI – Programy PC a PII – aplikace mobil, které obsahují názvy aplikací/programů spolu s využitou verzí a odkazem ke stažení těchto softwarů, pokud je to zapotřebí.

4.1 Počítače (PC), notebooky

Jako první se práce bude věnovat zabezpečení PC se kterým přijde dítě do styku ať už doma, u kamaráda nebo třeba ve škole. Většinou má PC své dané místo v domácnosti, pokud se ovšem nejedná o notebook, což je zjednodušeně řečeno přenosný PC. Nejpoužívanějším operačním systémem (OS) na světě je Windows, který v současnosti drží podíl 86,2 % ze všech operačních systémů PC, z čehož pouze Windows 10 si z tohoto podílu připisuje 39,22 % a je tak nejpoužívanějším OS i Windows na světě [16]. Z tohoto hlediska se rodičovská kontrola v této práci bude věnovat právě zmíněné verzi OS.

Pokud se rodič rozhodne pro kontrolu svého dítěte na PC, měl by toto zařízení obstarat zabezpečením a programy, které dokáží omezit čas, zablokovat nevhodné webové stránky, blokovat určité aplikace, programy, hry a v neposlední řadě také zvládnout zjistit, co vlastně dítě na PC dělá neboli jak na něm tráví čas.

Dále tato práce doporučuje obstarat každý PC v domácnosti nebo alespoň ta zařízení, která jsou v kontaktu s dětmi antivirovým programem. Na světě existuje spousta antivirových programů, mezi nejznámější patří například ESET, Avast nebo Kaspersky.

4.1.1 Rodičovská kontrola Windows

OS Windows disponuje softwarem, který se věnuje rodičovské kontrole a lze tak nastavit určitá opatření pro dítě bez použití dalších programů zabývajících se kontrolou dětí na PC. V první řadě je potřeba dítě přidat v nastavení jako člena rodiny, a to přes „Nastavení Windows“, následně se vybere „Účty“, kde se zvolí „Rodina a jiní uživatelé“. V této chvíli přes tlačítko „Přidat člena rodiny“ může rodič zvolit, zda se jedná o dítě nebo dospělou osobu,

v tomto případě se vybere dítě a zadá se nebo vytvoří jeho emailový účet, na který bude dítěti zaslána pozvánka do rodiny, kterou musí potvrdit, aby se následně mohla spravovat jeho oprávnění.

Rodič může rozhodnout o typu účtu dítěte, kde by měl zvolit standartní účet nikoli správce, který by dítěti dával všechna oprávnění. Jako druhá možnost nastavení se objevuje povolení nebo blokování přihlášení k zařízení, čímž může rodič kdykoliv odeprít nebo povolit přístup dítěte k PC. Dalším krokem je následné „Spravování nastavení rodiny online“ což umožní rodiči po přihlášení k účtu na stránkách Microsoftu další možnosti nastavení. Nastavit lze oprávnění týkající se aktivity, času u obrazovky, omezení obsahu a dalších možností [20].

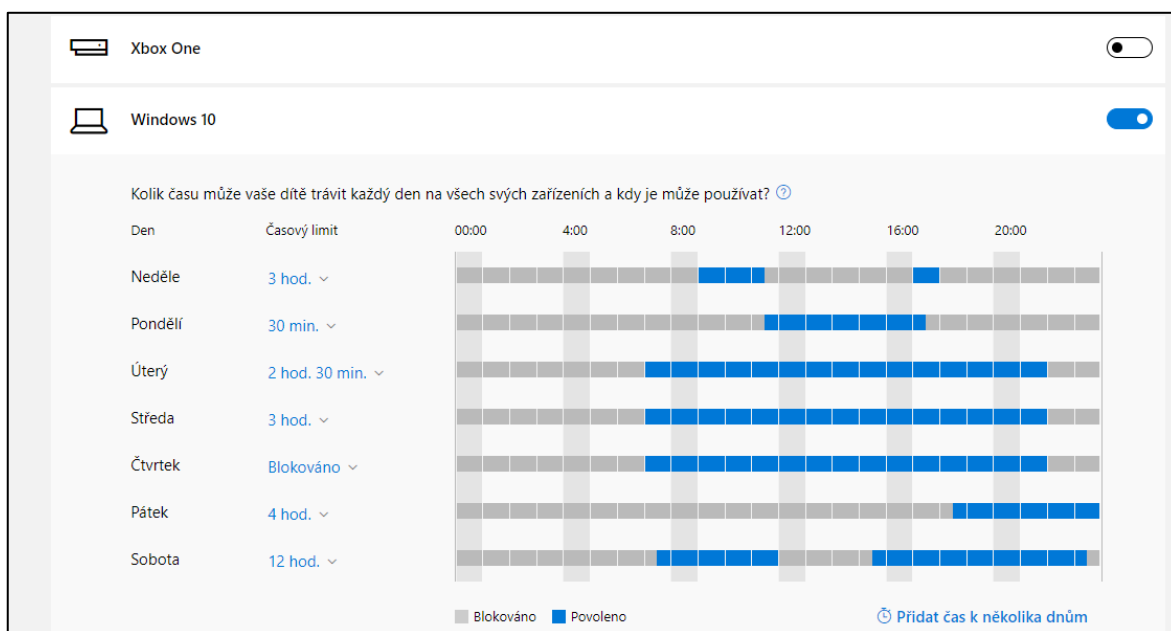
Aplikace a hry (5)			
> Microsoft Edge	2 min.		Nejde zablokovat
> originthinsetupinternal	2 min.		Blokovat
> Origin	1 min.		Blokovat
> Obchod Google Play	1 min.		Nejde zablokovat
> UI systému	1 min.		Nejde zablokovat
Prohlížení internetu			
Pokusy o návštěvu zablokovaných webů Když se vaše dítě pokusí navštívit blokové webové stránky, uvidíte je tady.			
Navštívené weby (7)			
> microsoft.com	ne 19:12	Návštěvy: 18	Blokovat
> msn.com	ne 19:12	Návštěvy: 6	Blokovat
> onlinovky.cz	so 18:27	Návštěvy: 4	Blokovat
> alza.cz	so 18:27	Návštěvy: 1	Blokovat
> albi.cz	so 18:27	Návštěvy: 1	Blokovat
Zobrazit všechno			
Vyhledávání			
Web (20)			
online hry erotické, erotické hry, online hry, pornohub, porno, sex, pornovka, porno, erotické hry online, https://www.erotické-hry.bing.com/search?q=porno , porno, porno, microsoft,			

Obr. 5. Sekce Aktivita.

V sekci **Aktivita** je na rodiči, aby se rozhodl, zda chce získávat týdenní přehledy o aktivitách dítěte na všech zařízeních s Windows 10, zařízeních Xbox One, ale také na zařízeních s Androidem, na kterých musí být nainstalována aplikace Microsoft Launcher. Pokud se rozhodne pro sledování, budou se rodiči na stránkách zobrazovat všechny aplikace, které byly použity s ukazatelem stráveného času jednotlivých aplikací. Je zde také na výběr, zda danou aplikaci zablokovat nebo nechat povolenou. Zobrazovat se také budou vyhledávací výrazy (po kliknutí na výraz se zobrazí okno v prohlížeči s totožným obsahem, jako mělo dítě, lze

tak zjistit, zda omezení obsahu funguje), navštívené webové stránky za jednotlivé dny spolu s počtem navštívení a volbou, zda danou stránku zablokovat. Jako poslední se rodič může dozvědět čas strávený u obrazovky v minutách za každý jednotlivý den v týdnu.

V sekci **Čas u obrazovky** lze nastavit časové limity týkající se doby strávené na zařízení, a to pro každý den zvlášť. Rodič může nastavit jak časový limit, což znamená maximální dobu, kterou může dítě strávit na zařízení za určitý den nebo rovnou zvolit časový harmonogram, kde je povoleno nebo blokováno používání zařízení. Tyto limity jdou nastavit pouze pro Windows 10 nebo pro Xbox One, přičemž nastavení může i nemusí být pro obě zařízení stejné. Časový limit i harmonogram jde nastavovat pouze v délkách po 30 minutách, přičemž maximální doba, kterou lze povolit je 12 hodin denně, což si lze všimnout na Obr. 6.



Obr. 6. Nastavení časového plánu.

Další možností Microsoft přináší v sekci **Omezení obsahu**, kde lze nastavit, jestli je zapotřebí souhlas rodiče, když si chce dítě něco koupit v Microsoft Storu nebo také jestli má být zasílán email pokaždé, když si dítě něco stáhne. Je tu možnost také zapnout blokování nevhodných webů, pro které děti ještě nemají věk, ovšem toto nastavení funguje jenom za předpokladu, že dítě použije jeden z webových prohlížečů od Microsoftu (Microsoft Edge nebo Internet Explorer) navíc na zařízeních s Windows 10. Blokovat zde jdou také nevhodné aplikace, hry nebo multimédia, přičemž se můžou povolit aplikace a hry s hodnocením pro libovolný věk. Automaticky jsou zde blokovány standartně používané webové prohlížeče, pro jejich používání se musí zrušit jejich blokování nebo může dítě zaslat e-mail o povolení používat tento prohlížeč.

V dalších možnostech stojí za zmínku zjištění polohy dítěte, k čemuž je potřeba mít zařízení s Windows 10 nebo s Androidem a nainstalovanou aplikací Microsoft Launcher Toto nastavení se proto týká hlavně mobilů, tabletů nebo notebooků [17].

Výhody:

- Předinstalovaný a v češtině.
- Odepření či omezení přístupu k PC.
- Přehled o aktivitách a stráveného času.
- Zobrazení navštívených www stránek.
- Blokování či omezení webů a aplikací.

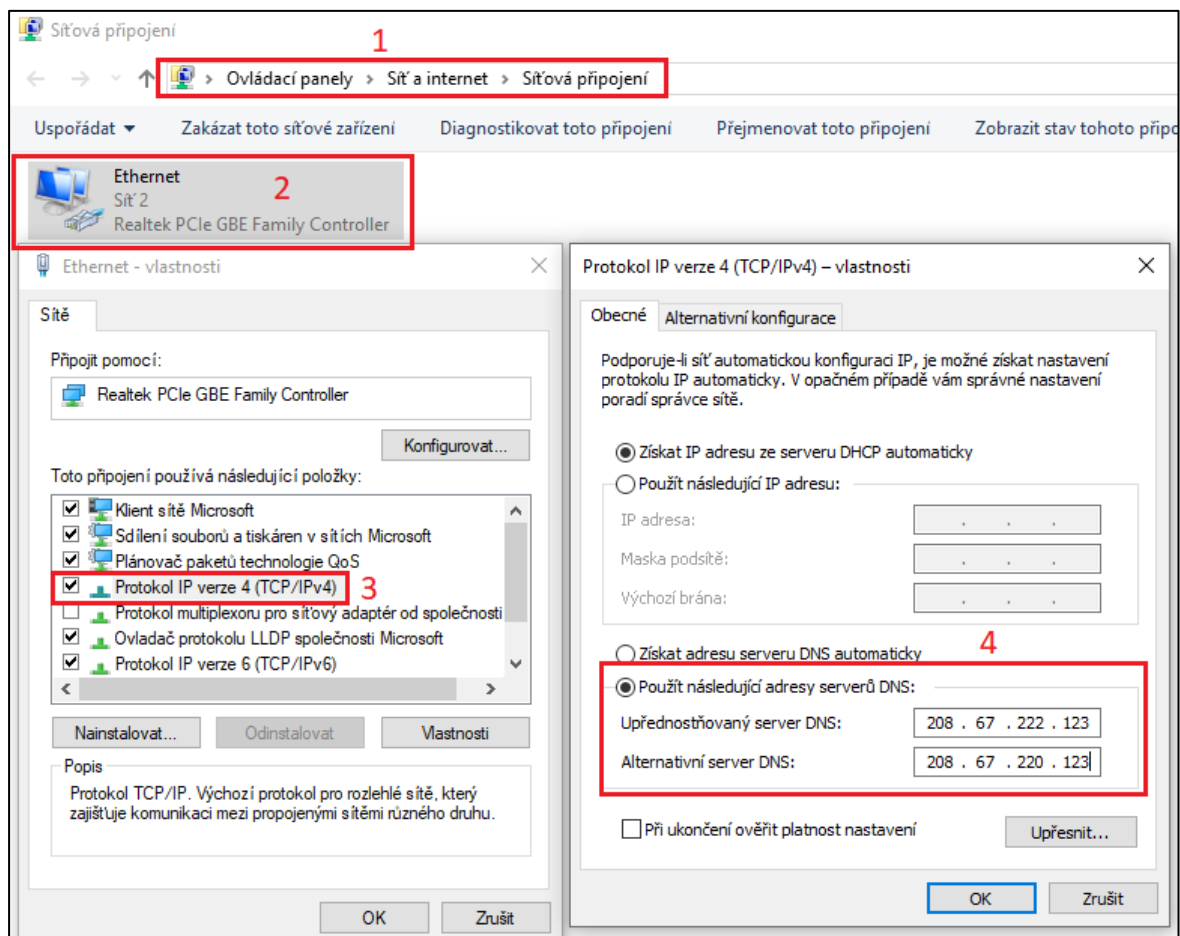
Nevýhody:

- Nastavení po 30 minutách a maximálně 12 hodin denně.
- Funkčnost pouze při použití webových prohlížečů od Microsoftu.
- Určené pro Windows.

4.1.2 OpenDNS

Pokud je snaha rodiče primárně to, aby se dítě nedostalo na nepřístupnou stránku nebo jinou nebezpečnou doménu, určitou alternativou je FamilyShield od OpenDNS, jelikož tato služba automaticky blokuje všechny nevhodné a nebezpečné stránky, které už jsou v jejich seznamu. Na rozdíl od rodičovské kontroly Microsoftu, zde není blokování podmíněno použitím určitého webového prohlížeče, ale je automaticky použito na všech prohlížečích, což je jistě lepší variantou. Nastavení je opravdu jednoduché a rodič nepotřebuje stahovat žádný software, stačí pouze provést následující kroky, které jsou vidět na Obr. 7:

- Přes nastavení si vyhledat Síť a Internet (1. bod na obrázku).
- Následně vybrat možnost Změnit možnosti adaptéru.
- Pravým tlačítkem myši kliknout na Ethernet a následně zvolit Vlastnosti (2. bod).
- Zvolit Protokol IP verze 4 (TCP/IPv4) a zvolit Vlastnosti (3. bod).
- Zadat upřednostňovaný server DNS (208.67.222.123) a Alternativní server DNS (208.67.220.123) a potvrdit (4. bod).



Obr. 7. Nastavení DNS serveru.

Pokud by se nyní někdo snažil dostat na stránku zabývající se pornografií, tak se okamžitě zobrazí stránka, která informuje o tom, že byla daná stránka zablokována. Nevýhodou OpenDNS je, že neblokuje tyto výrazy již při hledání, ale až se nevhodná stránka vybere, tím pádem se dítěti ukáží všechny vyhledané stránky související s hledaným výrazem. To samé platí i u zobrazení obrázků, kdy se tyto obrázky ukáží jako vyhledané, ale až po přejití na stránky, kde se nachází, dojde k zablokování [18].

Výhody:

- Blokování automaticky vygenerovaných nebezpečných a nevhodných stránek.
- Není potřeba instalace.
- Lze použít i na Wi-Fi routeru.

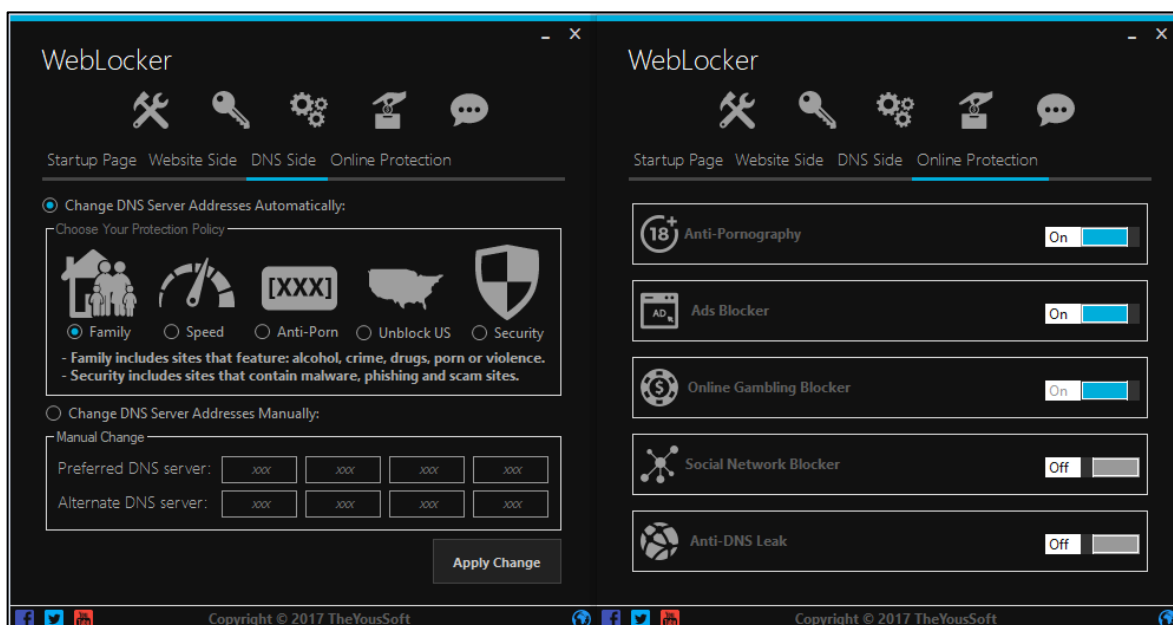
Nevýhody:

- Nejde přidat další blokovanou stránku nebo naopak některou odebrat.
- Blokuje pouze nevhodné webové stránky nikoliv výrazy při hledání.

4.1.3 WebLocker

Pokud by rodič hledal něco opravdu spolehlivého v blokování nepřístupných stránek, výrazů apod. existuje software WebLocker, který má jednoduché nastavení s kvalitním provedením práce v blokování webových stránek. Na rozdíl od předchozích dvou variant se tento program musí stáhnout a nainstalovat na zařízení, aby se rodič mohl dostat k nastavení. Hned ze začátku se rodič zaregistruje a zvolí si přihlašovací jméno spolu s heslem, čímž získá jako jediný kontrolu nad tímto softwarem.

Po přihlášení se objeví úvodní stránka, která informuje o tom, zda jsou na PC aktivovány základní funkce jako je blokování reklam nebo výrazů s pornografickou tematikou a také jakou DNS adresu uživatel používá. Pokud by rodič přešel na nastavení DNS Side, může si zde zvolit mezi automatickým nebo manuálním nastavením adresy. Pro rodiče se doporučuje vybrat automatické nastavení, kde je na výběr z 5 variant ochrany: Family, Speed, Anti-porn, Unblock US a Security. Pokud se zvolí Security, dojde k blokování stránek, kde by se mohl objevovat malware, phishing nebo podvodné stránky. Unblock US je zase nastavení, které je určeno převážně pro americké občany a jejich specifikace. Anti-Porn už podle názvu blokuje všechny stránky spojené s pornografií, a to už při vyhledávání těchto výrazů, předposlední volbou ochrany je Speed, který je zaměřen na rychlost vyhledávání.



Obr. 8. Vzhled WebLockeru a jeho nastavení.

Práce ale doporučuje zvolit poslední volbu ochrany Family, která blokuje alkohol, kriminalitu, porno nebo násilí. Tohle nastavení je ve výsledku podobné tomu jako bylo u Family-Shieldu od OpenDNS, bohužel se stejně toto nastavení týká jenom blokování stránek a ne vyhledávání, proto se nabízí jít do nastavení Online Protection. V tomto nastavení může rodič povolit hned několik online ochran, které se týkají například pornografie, reklam, hazardních her nebo sociálních sítí. Doporučuji opět povolit ochranu týkající se pornografie, čímž se vyřeší problém s vyhledáváním, a tak budou pojmy týkající se pornografie už blokovány při hledání, dále doporučuji povolit blokování reklam a také hazardních her. Pokud by bylo potřeba, jde zde nastavit i blokování sociálních sítí jako je Facebook nebo Instagram.

Může se také stát, že rodič bude chtít zablokovat nějakou určitou stránku nebo ji povolit pouze v nějaký den či hodinu. Pro tyto případy je tu nastavení Website Side, kde se může přidat libovolná stránka, která má být blokována, přičemž se může určit, jestli má být blokována natrvalo nebo pouze v určitý den, dny nebo hodiny. Jde zde také odblokovat stránky, které naopak tento program zablokoval a tím znemožnil jejich používání.

Výhody:

- Blokování nevhodných webových stránek již při vyhledávání.
- Výběr mezi několika DNS servery a online ochran.
- Možnost přidání/odebrání libovolných webových stránek.
- Nastavení časového omezení pro určité webové stránky.

Nevýhody:

- Zaměření pouze na blokování stránek.
- Není podporován český jazyk.

4.1.4 PC Screen Watcher

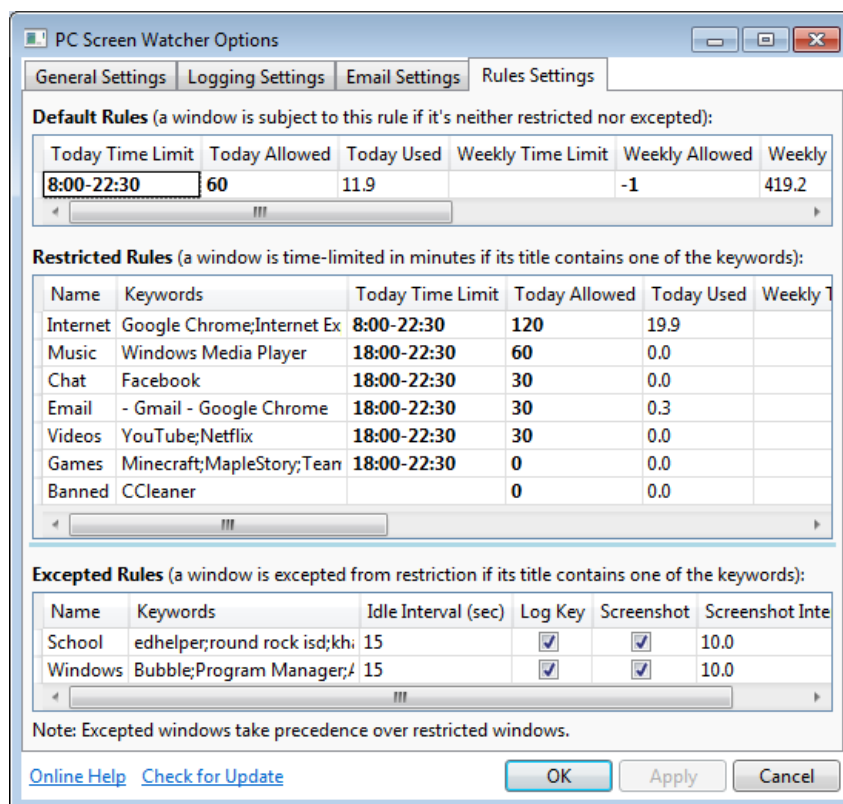
Velice užitečným může být program PC Screen Watcher pro ty, kteří by chtěli hlavně omezovat určité aplikace. Jelikož tento program nedisponuje češtinou a celkově může některým rodičům trvat déle, než zjistí, jak co pracuje, může být pro rodiče nastavení obtížnější. Nejzajímavější sekcí tohoto softwaru je nastavení pravidel (Rules Setting), kterou určitě využije nejeden rodič. Tento program stejně jako WebLocker vyžaduje stažení a instalaci na zařízení.

Po instalaci si rodič nastaví pouze heslo, čímž získá možnost upravovat nastavení pouze on sám, jelikož při každém otevření, ukončení nebo odinstalování bude program vyžadovat toto

heslo. Po přihlášení se objeví okno se 4 nastaveními a to: General Setting, Logging Setting, Email Setting a Rules Setting. Za zmínku stojí hlavně nastavení pravidel, tedy Rules Setting na který se práce podívá blíže, u ostatních sekcí jde spíše o běžné nastavení.

Rules Settings

Jak už se psalo výše, dle všeho asi nejzajímavější a také hlavní nastavení celého softwaru. Jde zde o nastavení pravidel, které jsou navíc už předem více méně předvyplněné. Program má předvyplněna ty nejčastější pravidla, například pod pojmem Internet se schovávají klíčová slova všech webových prohlížečů, pod videi je zase YouTube a pod hrami jsou vypsány některé hry. Všechny tyto klíčová slova jsou poté nastaveny v dalších sloupcích, jako je povolení denního/týdenního limitu (v minutách), nastavení denního/týdenního času používání, zda se mají zaznamenávat snímky obrazovky či stisknuté klávesy apod. Na Obr. 9 jdou vidět hodnoty, které byly nastaveny pro tuto práci, například Facebook je nastaven tak, že se smí používat mezi 18:00 až 22:30, při čemž denně má povoleno pouze 30 minut, dále třeba u her jako Minecraft je nastaven čas od 18:00 do 22:30, ale dnešní limit je nastaven na 0, takže se hra nespustí. Rodič tak může omezit a nastavit prakticky jakoukoliv aplikaci, dokument či hru, musí ovšem klíčové slovo zapsat tak, jak ho používá Windows. Jako příklad se opět využije obrázek s nastavením, na kterém si lze všimnout, jaké klíčová slova se použila, pro FB se musí uvést celý jeho název Facebook nebo celé názvy webových prohlížečů jako je Google Chrome nebo Internet Explorer.



Obr. 9. PC Screen Watcher – nastavení pravidel.

Naopak mohou se také zadat výjimky, které by se mohly týkat třeba školy nebo vzdělání, v takovém případě by dítě nebylo nijak časově omezeno i když by překročilo povolený limit pro používání webového prohlížeče, pokud by sloužil pro zadanou výjimku [19].

Výhody:

- Odinstalace i každá změna vyžaduje heslo.
- Omezení vybraných aplikací podle několika možností.
- Povolení výjimek pro aplikace.
- Možnost sledovat emailový účet dítěte (Email Settings) nebo nastavení pořizování snímků obrazovky či stlačených kláves (Logging Settings).

Nevýhody:

- Klíčové slova musí být zadaná tak, jak ho používá Windows.
- Pro někoho složitější nastavení.
- Není podporován český jazyk.

4.1.5 ManicTime

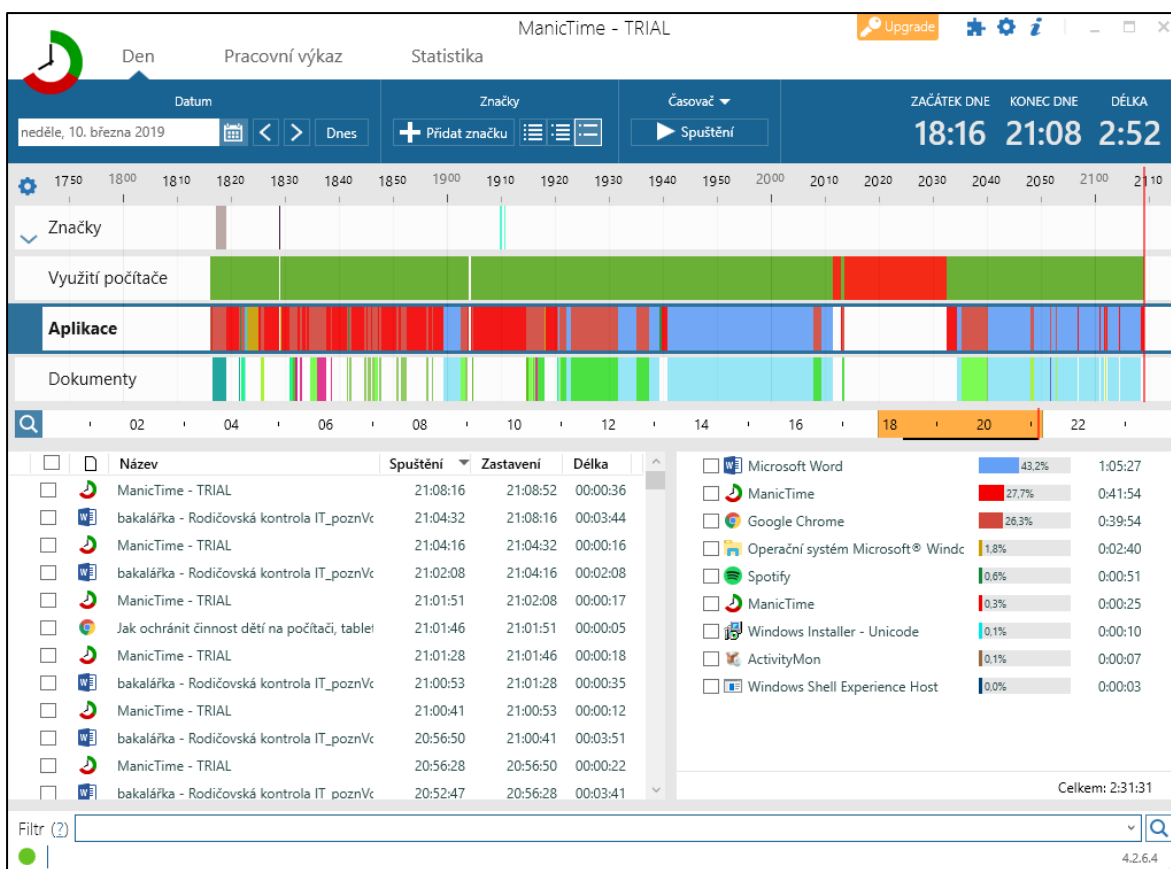
Pro sledování se nabízí program ManicTime, který se specializuje na monitorování toho, co dítě provádí na PC a zároveň vše ukazuje v přehledných statistikách. Pokud se tedy rodič zajímá a zároveň hledá software, který by sledoval každý krok, který byl vykonán na zařízení a přehledně ho také následně ukazoval, určitě by se měl využít právě tento program. Stejně jako u posledních dvou aplikací je potřeba si stáhnout instalační balíček. Po spuštění se doporučuje v nastavení vytvořit heslo, čímž se může předejít smazání těchto údajů dítětem. Velkým plusem je určitě podpora českého jazyka, což určitě uvítají rodiče, kteří zrovna neovládají cizí jazyk, ale i bez této podpory by se jednalo o velice jednoduchou aplikaci s prostým vzhledem i ovládáním. ManicTime je rozložen do 3 záložek: Den, Pracovní výkaz a Statistika. Rodiče ale budou zajímat hlavně záložky Den a Statistika, ve kterých se dozví vše o tom, co bylo prováděno na PC [20].

Den

Jedná se o jednoduše vytvořené prostředí, které rodičům poskytne všechny informace týkající se pobytu dítěte na PC, což je ostatně vidět na Obr. 10. V horní části lze jednoduše přepínat mezi určitými dny, které zrovna chce rodič kontrolovat. Dále se jde dozvědět přesný čas, kdy byl PC poprvé zapnut a kdy byl také naposledy použit, přičemž se hned vedle dozví celkovou dobu chodu zařízení v tomto případě PC.

V další části si lze všimnout rozdělení do skupin: Využití počítače (jedná se o ukazatele, který uvádí, v jaký čas přesně byl PC aktivní, neaktivní nebo byl vypnutý), Aplikace, Dokumenty a Značky. Na Obr. 10 je zobrazena skupina Aplikace, která rodiči poskytne všechny informace týkající se všech využívaných aplikací v požadovaném datu a čase. Stojí za povšimnutí, že program ukazuje přesný čas na vteřiny, ve kterém se s určitou aplikací začalo pracovat a kdy skončilo, přičemž každé vyjetí z dané aplikace se považovalo za jeho zastavení, a naopak každé vrácení za jeho spuštění. Proto ta samá aplikace byla spuštěna několikrát. Má to za následek přepínání například mezi různými aplikacemi nebo mezi aplikací a prohlížečem či dokumentem. Informaci taky rodič dostane nejen o jakou aplikaci či program se jedná, ale také co přesně se v takové aplikaci použilo, například u programu Microsoft Word si lze všimnout toho, jak se jmenoval otevřený soubor, nebo u webového prohlížeče název webové stránky. Každé aplikaci se navíc počítá celkový čas používání, který je zároveň zobrazen procentuálním podílem. Pokud by se kurzorem myši najelo na barevný

proužek, který se zobrazuje u výše zmíněných skupin, zobrazí se snímky obrazovky, které se automaticky pořizují po 60 vteřinách, ale v nastavení lze nastavit jiný časový interval.



Obr. 10. Program ManicTime, záložka Den.

Statistika

Pokud by navíc rodiče zajímala statistika o tom, co jejich dítě dělá nejčastěji na PC či vidět, jestli si v poslední době oblíbilo nějakou aplikaci, stránku nebo jenom vidět průběh dne, tak na záložce Statistika se vše zaznamenává do přehledných grafů a tabulek. Na výběr je už z předem definovaných statistik jako jsou nejčastější aplikace, dokumenty nebo docházka, vytvořit se ale dá zcela vlastní statistika, třeba porovnání určitých aplikací, webových stránek, vlastních značek apod. Zvolit se dá také jestli se bude statistika vytvářet pouze za určité období tedy den, týden, měsíc či dokonce rok, určitě se jedná o velice zajímavou službu, která jednoduše dává rodiči přehled o všech aktivitách, a ještě je k tomu dokáže zobrazit v přehledných statistikách.

Výhody:

- Lze zjistit, jaké aplikace se, v který čas na vteřiny přesně používaly a naopak.
- Zjištění, k čemu sledovaná aplikace sloužila.

- Zobrazení předdefinovaných statistik, ale i vlastních za jakékoliv období.
- Zobrazení screenshotů v daný čas.

Nevýhody:

- Slouží pouze pro sledování, chybí nastavení omezení.

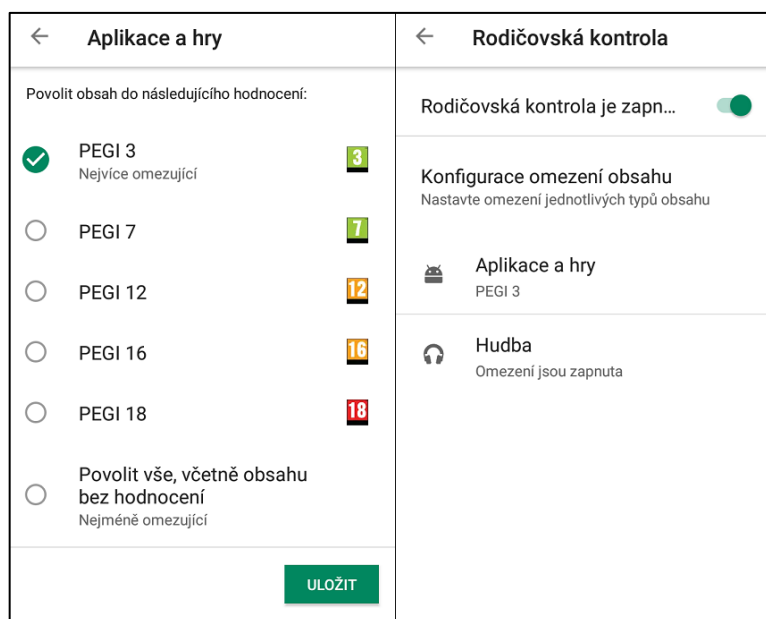
4.2 Mobilní telefony

Ještě více než na PC by se měla rodičovská kontrola zabývat mobilními zařízeními, které jak bylo na začátku práce zobrazeno v grafu, vlastní do 11. roku 70 % dětí. Stejně jako u PC by se i tady měla rodičovská kontrola zabývat omezením Internetového obsahu, blokováním či omezováním určitých aplikací, sledováním polohy nebo toho co je na zařízení vykonáváno a v neposlední řadě také omezením stahování či přístupu k mobilnímu zařízení. Pro zvolení ideální aplikace nebo aplikací pro kontrolu dítěte je také důležité vědět, jaký operační systém je v mobilním telefonu dítěte, jelikož ne všechny aplikace fungují na všech platformách. Mezi nejpoužívanější OS bezesporu patří Android, ale také iOS, který vlastní mobilní telefony od společnosti Apple. Práce se ale zaměří hlavně na kontrolu mobilních telefonů s OS Android, které jsou přeci jen u dětí více rozšířenější, hlavně kvůli pořizovací ceně a dostupnosti.

4.2.1 Obchod Google Play

V první řadě se práce zaměří na omezení stahování aplikací z Google Play, odkud se stahuje drtivá většina všech aplikací od her až po sociální sítě. V Obchodu Play lze nastavit rodičovská kontrola, která dává rodiči možnost částečně omezit obsah a stahování aplikací, pouze ale z Obchodu Play, nikoliv však z neověřených přímých zdrojů na Internetu. K nastavení se rodič dostane po spuštění aplikace a kliknutím na 3 tečky/čárky v horním rohu obrazovky. Následně je potřeba zvolit volbu Nastavení a zde se již nachází možnost Rodičovská kontrola. V nastavení lze omezit 2 možnosti: Aplikace a hry nebo Hudbu. Při zapnutí rodičovské kontroly na rodiče vyskočí okno, které žádá o zadání a vytvoření 4místného PIN kódu, čímž odepře přístup dítěti k této funkci. Jako první lze omezit Hudbu, a to pouze tak, že je rodiči poskytnuta volba omezení hudby, kterou poskytovatel označil jako explicitní obsah, což znamená že se jedná o písně, ve kterých se objevují vulgární výrazy, sexuální narážky apod. Druhou možností je omezení Aplikací a her, kde může rodič povolit obsah podle hodnocení vývojářů. Ten se značí pomocí systému PEGI (Pan European Game Information) a to následovně:

- PEGI 3 je nejnižší vhodná pro nejmenší děti (hry typu puzzle, piškvorky apod.).
- PEGI 7 jsou povoleny scény nahánějící hrůzu.
- PEGI 12 má jistou formu násilí a zobrazení nahoty.
- PEGI 16 obsahuje scény nahoty a násilí, ale s mírným projevem.
- PEGI 18 je klasifikace pro dospělé, tedy vše povoleno [21].



Obr. 11. Nastavení Obchodu Play.

Výhody:

- Omezení aplikací a her pomocí systému PEGI.
- Vnitřní nastavení – není potřeba žádné stažení aplikace.

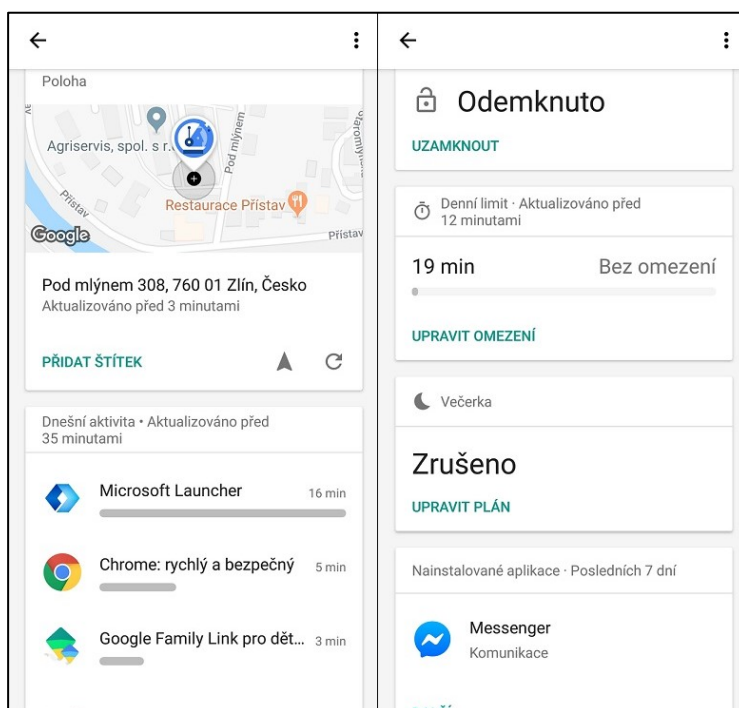
Nevýhody:

- Nezamezení stahování z neznámých přímých zdrojů.

4.2.2 Google Family Link

Společnost Google vytvořila pro zařízení s OS Android, ale i iOS rodičovskou kontrolu, která vystupuje pod názvem Google Family Link a v podstatě nabízí základ možností kontroly. Aplikace funguje tak, že si rodič stáhne aplikaci určenou pro rodiče a postupuje podle průvodce, zároveň se na zařízení dítěte stáhne Family Link, který je naopak určený pro dítě. Bohužel i zde platí určitá omezení, na mobilních telefonech rodičů funguje aplikace, pokud má zařízení Android 5.0 a vyšší, kdežto u dětí je potřeba mít zařízení s Androidem 7.0 nebo vyšší [22]. Celý proces spárování je velmi přehledný, jednoduchý a zabere kolem 5 minut

času. V nastavení lze nastavit denní limit používání zařízení (nastavení po 15 minutách a maximálně 8 hodin) a zároveň také večerka, která uzamkne zařízení ve stanovený čas na minuty přesně. Dále zde jde sledovat aktivitu posledních dnů (dnes, včera, 7 dní a 30 dní), která zobrazí jednotlivé aplikace, které byly využity a jejich čas použití. Zjistit lze také přesná poloha zařízení v danou chvíli nebo spravovat aplikace, a to až už se jedná o systémové aplikace jako je galerie, fotoaparát nebo poznámkový blok, ale také aplikace, které byly staženy, jako jsou různé hry, sociální sítě či jiné programy. Tyto aplikace lze poté povolit nebo zakázat a spravovat jejich oprávnění.



Obr. 12. Možnosti Google Family Linku.

Spravovat umožňují také ovládací prvky Obchodu Google Play, přičemž zde je stejná nabídka nastavení, jako tomu bylo u rodičovské kontroly v samotné službě Google Play, obohacená o nastavení filmů, knih, schvalování nákupů pomocí platební rodinné metody a také o zakázání instalace aplikací z jiných zdrojů, než je Google Play. Nastavit lze i filtry, jako je zablokování webů určených pro dospělé, které automaticky tato aplikace blokuje, ale rodič může tento seznam upravovat a to tak, že určité stránky může povolit nebo naopak blokovat. Další filtr lze nastavit ve vyhledávání Google, který se bude snažit o bezpečné vyhledávání. Dítě může samozřejmě požádat o povolení, stáhnout si aplikaci, která nepodléhá nastaveným pravidlům, rodič se poté může rozhodnout, zda dá svolení ke stažení takové aplikace. Pokud dítě stáhne novou aplikaci, rodiči obdrží zprávu, která ho informuje o instalaci dané aplikace,

tudíž se může hned rozhodnout k jeho zablokování či ponechání povolení danou aplikaci používat. Pokud dítě vyčerpá denní limit, automaticky dojde k uzamknutí zařízení, přičemž jediné, co bude naskytnuto na zařízení je rodičovský přístup a stav nouze. U rodičovského přístupu je zapotřebí 6místný kód, který zařízení znovu odemkne a u stavu nouze jsou povoleny pouze hovory.

Nastavení týkající se blokování Internetového obsahu se vztahuje pouze na prohlížeč Google Chrome, takže je zapotřebí zakázat všechny ostatní prohlížeče, aby dítě nemohlo obejít tato omezení vyhledávání. Všechna nastavení lze také nastavit, pouze pokud je rodič připojen online k Internetu, to samé platí i pro dítě, které až po připojení k Internetu přijme nové nastavení zařízení [22].

Výhody:

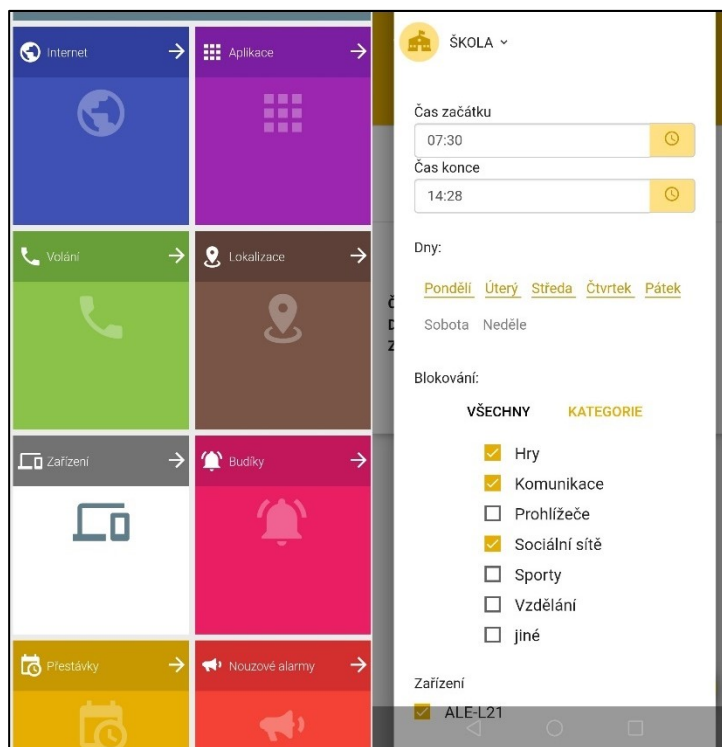
- Rozšířené omezení Google Play Obchodu se zákazem stahování z jiných zdrojů.
- Spravování aplikací ať systémových (fotoaparát...) nebo stažených (hry...).
- Online nastavení mobilního zařízení dítěte.
- Zaslání informací o nově stažené aplikaci a možností okamžitě takovou aplikaci zakázat.

Nevýhody:

- Telefonní zařízení dítěte musí mít Android 7.0 nebo vyšší.
- Nastavení denního omezení pouze po 15 minutách a maximálně 8 hodin.
- Filtry týkající se Internetového vyhledávání fungují pouze na Google Chrome.

4.2.3 SecureKids

Alternativou Google Family Linku se může klidně stát rodičovská kontrola SecureKids, která nabízí zajímavé nastavení. Stejně jako u většiny aplikací zabývajících se dohledem nad dětmi i zde se najde filtr webových stránek a vyhledávání, který je zde rozdělen do předem definovaných skupin jako je náboženství, násilí, pornografie, drogy, sportovní apod. Je pouze na rodiči, které skupiny aktivuje a zamezí tak jejich vyhledávání dítětem. Samozřejmě nechybí ani přidání výjimek, a to ať už se jedná o blokování nebo povolení webových stránek. Zároveň lze nastavit úroveň zabezpečení 1-3, přičemž nejvyšší zabezpečení 3 znamená, používání pouze skBrowser, který je nainstalován spolu s aplikací. Zlatou střední cestou je zabezpečení úrovně 2, která dovoluje využívat ověřené prohlížeče, a to Google Chrome, skBrowser a výchozí prohlížeč.



Obr. 13. Možnosti nastavení a příklad přestávky.

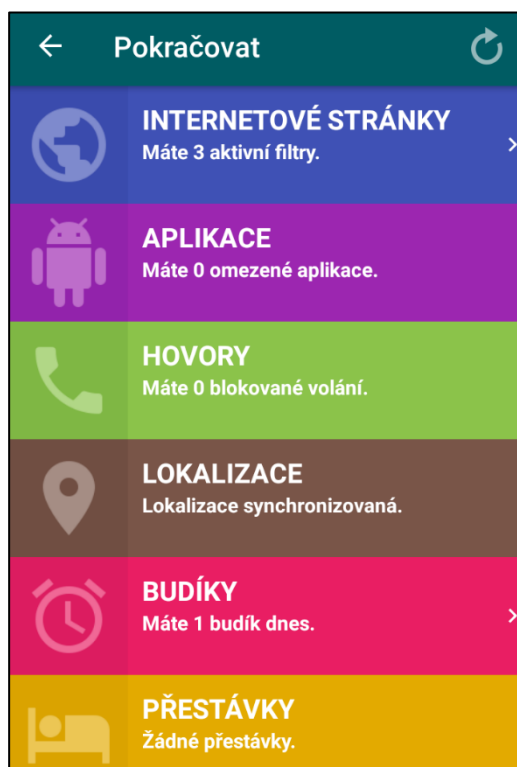
Blokovat či povolit zde lze také jednotlivé aplikace bez rozdílu, zda se jedná o systémové aplikace či nikoliv. Nechybí ani nastavení délky používání určité aplikace, která se nastavuje počtem minut na jednotlivé dny. I tady se najde rozřídění aplikací do jednotlivých skupin, přičemž každá jednotlivá skupina jde nastavit samostatně, jedná se o skupiny: hry, komunikace, prohlížeče, sociální sítě, sporty, vzdělání, jiné a všechny. Zablokovat se mohou i instalace nových aplikací, dokud rodič nenastaví jejich přístup. Nechybí ani lokalizace zařízení, která zobrazí na mapě přesné místo pobytu dítěte spolu s přesným časem kdy došlo k poslední lokalizaci zařízení.

Plusem této aplikace je správa hovorů, která dokáže blokovat hovory z neznámých čísel nebo čísla z mezinárodních zemích. Rodič si také může vybrat, které telefonní čísla mohou nebo nemohou kontaktovat zařízení dítěte, zároveň může dostávat výpisy jednotlivých hovorů. Dalším plusem je nastavení přestávek, které zablokují zařízení ve stanovený den i čas. Jelikož počet přestávek není omezen, může být na jeden den použito hned několik časů, proto je toto nastavení ideální například v době, kdy má být dítě ve škole, dělat domácí úkoly nebo když má jít spát. Navíc jde toto omezení nastavit jak na všechny kategorie aplikací, tak i na určité například na hry, sociální sítě nebo komunikace.

Velice zajímavé je také nastavení budíku, kdy rodič může nastavit ve který den i čas má zařízení zvonit. Opět se jedná o ideální nastavení, které dítě může vzbudit v den, kdy má jít

do školy nebo když mu má být něco připomenuto. Nastavit lze jak určitý den v roce, tak i opakované buzení v určité dny, přičemž se do budíku připiše i zpráva, která poskytne potřebné informace při zazvonění. Posledním nastavením je nouzový alarm, kterým může dítě dát rodiči vědět, že potřebuje pomoc. Ve zprávě jsou poskytnuty přesné souřadnice spolu se zobrazením na mapě, kde se dítě v době zaslání nouzové zprávy nachází spolu s přesným časem.

V poslední řadě jsou rodiči poskytnuty statistiky, které uvádí čas užívání zařízení, a to jak celkový, tak i rozdělený na jednotlivé aplikace, díky kterým získá přehled o stráveném čase dítěte na jeho zařízení i o které aplikace se jedná. Dítě zároveň na svém zařízení může vidět kolik je aktivních filtrů webových stránek, zablokovaných aplikací, blokových volání, zda je jeho lokalizace synchronizovaná a kolik budíku i přestávek je nastaveno. Po rozkliknutí jednotlivých možností se dítěti dostanou podrobnější informace, například o jaké aplikace jde nebo jak je nastavena přestávka.



Obr. 14. SecureKids na zařízení dítěte.

Výhody:

- Filtr Internetového vyhledávání podle skupin.
- Denní limit pro vybranou aplikací nebo skupinu aplikací podle dne (max. 999 min.).
- Správa hovorů.

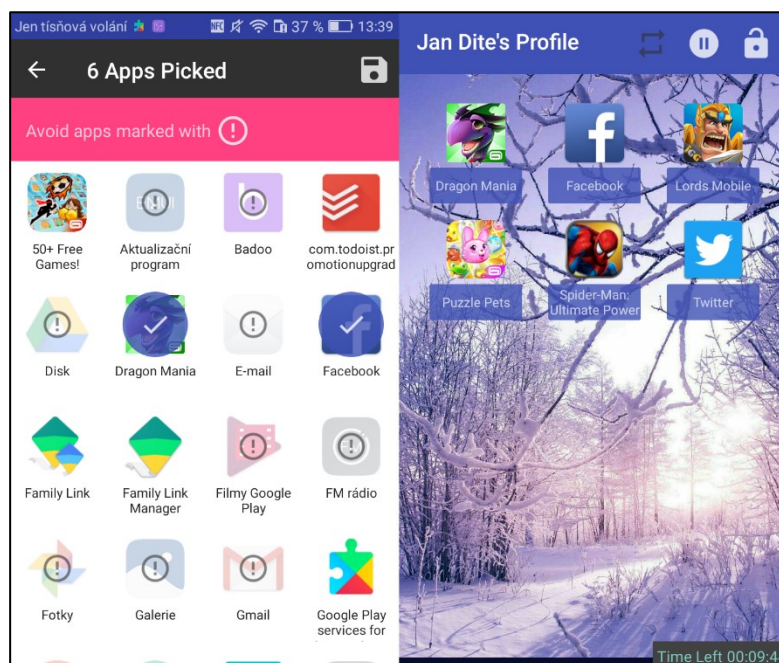
- Nastavení budíků nebo přestávek.
- Online nastavení mobilního zařízení dítěte.

Nevýhody:

- Nejvyšší zabezpečení vyhledávání je podmíněno používáním skBrowser.

4.2.4 Kids Zone

Pro ty rodiče, kteří půjčují své mobilní zařízení svému dítěti například ke hraní her je tu aplikace s názvem Kids Zone. Tato aplikace je velice jednoduchá a přitom účinná, jelikož rodič v této aplikaci vytvoří svému dítěti účet a následně povolí pouze takové aplikace, které uzná za vhodné, navíc aplikace sama upozorňuje na to, jaké aplikace by se povolovat neměly, a to pomocí zobrazení vykřičníku (!). Dítě tak dostane velice omezené možnosti ale takové, jaké si bude rodič přát. Zvolit se také může pozadí na tomto účtu a také časový limit, který je dítěti poskytnut (nastavení po 5 minutách). V posledním kroku stačí pouze přes tlačítko LOCK a vytvořením PIN kódu uzamknout zařízení a spustit tak omezený účet, který byl vytvořen pro dítě. Pokud by rodič chtěl opět využívat své zařízení pro vlastní účely stačí zadat zvolený PIN kód a tím dojde k jeho odemknutí.



Obr. 15. Povolení aplikací a náhled účtu dítěte.

Výhody:

- Vytvoření vlastního účtu dítěte na zařízení rodiče.
- Dítěti budou poskytnuty pouze takové aplikace, které budou rodiči schváleny.

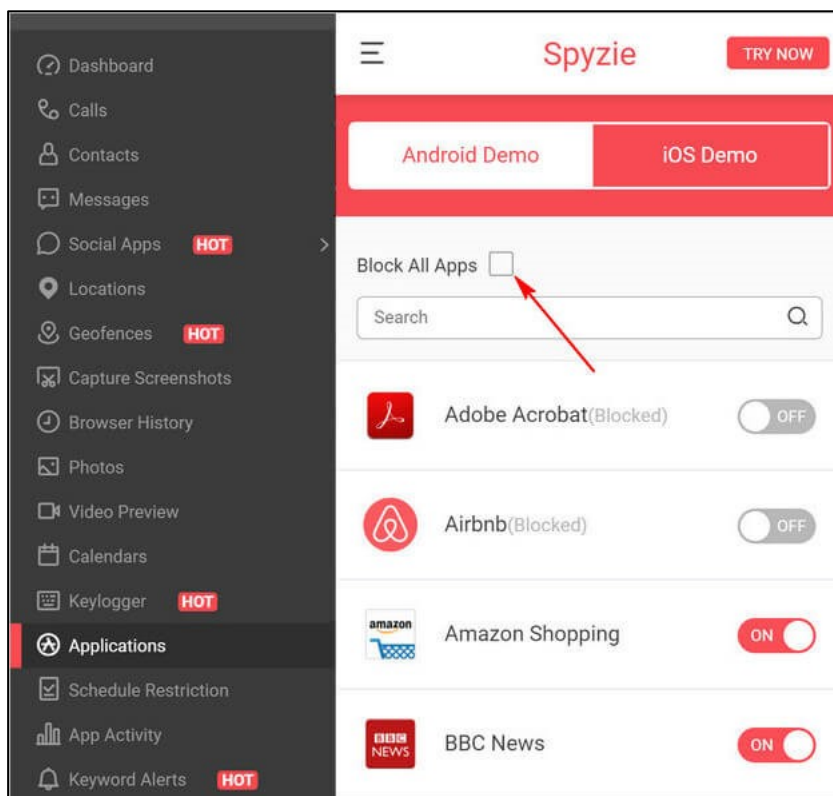
- Nastavení časového limitu poskytnutý dítěti.

Nevýhody:

- Nastavení časového limitu po 5 minutách.
- Každé spuštění účtu dítěte vyžaduje zadání nového PIN kódu.

4.2.5 Spyzie

Pro rodiče, kterým nevadí si připlatit za kontrolu jejich dítěte je vynikající aplikace Spyzie, která se věnuje kontrole zařízení dítěte, a to opravdu na vysoké úrovni. Na stránkách poskytovatele www.spyzie.com se nalezne vše potřebné, dokonce si rodič může na těchto stránkách vyzkoušet tzv. Demo verzi, která rodiči ukáže, co aplikace dokáže a jak vypadá. Nastavit lze opravdu všechno od blokování určitých aplikací, kontrolu pořízených fotografie, zaznamenávání hovorů, zobrazování jednotlivých konverzací, zjištění polohy zařízení apod. Na Obr. 16 lze vidět jaké skupiny mohou být spravovány. K tomu všemu jsou na stránkách vytvořeny tutoriály, které pomohou k rychlejšímu pochopení a nastavení jednotlivých možností. S cenou okolo 80-100 USD za rok se nemusí jednat o špatně investované peníze, jelikož aplikace dokáže nepřeberné množství nastavení kontroly dítěte. [23]



Obr. 16. Ukázka demo verze Spyzie.

Výhody:

- Široká škála možností nastavení, které bezplatné aplikace nemají.
- Poskytnuta demo verze a tutoriály pro lepší a rychlejší orientaci.

Nevýhody:

- Jedná se o placenou aplikaci.
- Není podporován český jazyk.

4.3 Wi-Fi routery

Poslední kategorií, na kterou se zaměří tato práce je rodičovská kontrola na Wi-Fi routerech, které již dnes jsou součástí mnoha domácností, ve kterých se využívají PC, chytré telefony či jiné zařízení závislé na Internetu. K nastavení těchto zařízení není potřeba (většinou) stahovat žádné aplikace, jelikož každý Wi-Fi router má své vlastní nastavení na předem stanovené adrese, která je uvedena v návodu, proto také v zásadě platí, čím dražší router máme, tím je větší pravděpodobnost většího množství možností i pro rodičovskou kontrolu. Proto se práce zaměří na nastavení dvou Wi-Fi routerů, konkrétně se bude jednat o levnější (Tenda F3 (F303) Wireless-N) a dražší (Mikrotik RB952Ui-5ac2nD-TC) variantu pro ukázkou toho, že každý Wi-Fi router má rozdílné nastavení.

4.3.1 Tenda F3 (F303) Wireless-N

Jedná se o Wi-Fi router, který se pohybuje v cenové relaci kolem 400,- Kč, čímž se řadí, jak už bylo zmíněno mezi levnější varianty, proto je taky nabídka nastavení rodičovské kontroly menší. Aby se uživatel dostal do nastavení, tak je v první řadě potřeba otevřít Internetový prohlížeč na zařízení, které je připojeno na daný router a zadat adresu 192.168.1.1. Díky tomu se uživatel dostane na stránku s nastavením připojeného routeru, který bude chtít heslo z manuálu, vlastní či žádné heslo vyžadovat nebude a rovnou uživatele přepojí na domovskou stránku nastavení. V prvním případě by si každý rodič měl nastavení svého Wi-Fi routeru zaheslovat vlastním heslem, pokud tak ještě neučinil, aby tak nedal svému dítěti nebo komukoliv, kdo by se na daný router mohl připojit možnost změnit nastavení.

Device Name	IP Address	Online Duration	Manage
PC	192.168.0.4	11h 2m 50s	<input type="checkbox"/>
Huawei P20 lite	192.168.0.3	1h 36m 51s	<input checked="" type="checkbox"/>
Huawei NOVA 3i	192.168.0.2	3h 15m 1s	<input type="checkbox"/>

Access Restrictions

Settings below will be applied to all managed devices

Allow access during: 10 : 00 ~ 23 : 00

Repeat: ☐ Everyday ☐ Mon ☒ Tue ☒ Wed ☐ Thu ☒ Fri ☒ Sat ☒ Sun

Website Restrictions: Disable

Obr. 17. Parental Controls a jeho nastavení.

Jelikož se tato práce zabývá rodičovskou kontrolou, zaměříme se proto na nastavení, která se týkají této problematiky. První nastavení najdeme v Parental Controls, kde se uživateli dostanou informace o všech zařízeních, které jsou v danou chvíli připojené k routeru a zároveň také časový údaj jejich dnešního připojení. Každé zařízení lze libovolně pojmenovat a také nastavit omezení přístupu. Samotné omezení se týká webového přístupu a jde nastavit pouze jednou a jen pro zvolená zařízení. Na výběr je ze 3 variant, a to zakázání všech stránek, povolení nebo zakázání podle specifikací webových stránek. U všech 3 variant se nastavuje čas od kdy do kdy je povolen přístup k Internetu bez omezení, a to v délkách po 5 minutách, pokud je zařízení připojeno mimo stanovený limit, platí nastavená pravidla, zároveň se také dá zvolit, pro které dny v týdnu nastavení platí. Za zmínku stojí pouze varianta Disable, ve které se nastaví, kdy má být povolen přístup k Internetu, jelikož čas se zadává jako povolený přístup a vše mimo tento povolený čas je následně díky Disable zakázáno. Jako příklad se využije Obr. 17, na kterém lze nahoře vidět zatrhnutí zařízení s názvem Huawei P20 lite a dole následně čas mezi 10:00 – 23:00 a vybrané dny v týdnu. V tomto vybraném čase je tedy povolen přístup k Internetu a mimo tento čas je odepřen, jelikož je vybraná varianta Disable. U zbylých dvou variant je potřeba zadat specifikaci webových stránek.

Další možností nastavení v tomto routeru může být nastavení DNS. Tato varianta byla již použita u PC v podkapitole 3.1.1 OpenDNS a stejně jako u PC i zde dokáže zablokovat automaticky všechny nevhodné webové stránky na všech připojených zařízeních. V tomto případě je potřeba zvolit sekci Administration a zadat upřednostňovaný server DNS (208.67.222.123), Alternativní server DNS (208.67.220.123) a následně potvrdit.

Poslední možností je blokování zařízení bez ohledu na další nastavení, jako je časové omezení. Toto nastavení se nalézá v sekci Bandwidth Control, kde se zatrhne, která zařízení mají být blokována nebo kterým má být omezen limit na stahování (No Limit, 128, 256 nebo 512 KB/s) a nahrávání (No limit, 32, 64 nebo 128 KB/s). Opět lze na Obr. 18 vidět příklad nastavení v této sekci, kde je nastaven u obou zařízení s názvem „Huawei“ limit stahování (256 a 128 KB/s) i nahrávání (32 a 128 KB/s). Zároveň se i zde nachází zařízení, kterému je odepřen přístup k Internetu, jedná se o zařízení s názvem „Mikrotik“.

Attached Devices(3)					
Device Name	Download Speed	Upload Speed	Download Limit	Upload Limit	Internet Access
PC 192.168.0.5 (Native Device)	↓ 0KB/s	↑ 1KB/s	No Limit	No Limit	Native Device
Huawei 192.168.0.2	↓ 262KB/s	↑ 12KB/s	256.00KB/s	32.00KB/s	<input checked="" type="checkbox"/>
Huawei 192.168.0.3	↓ 0KB/s	↑ 0KB/s	128.00KB/s	128.00KB/s	<input checked="" type="checkbox"/>

Blocked Devices(1)		
Device Name	MAC Address	Action
Mikrotik	B8:69:F4:DB:6B:E9	<button>Remove</button>

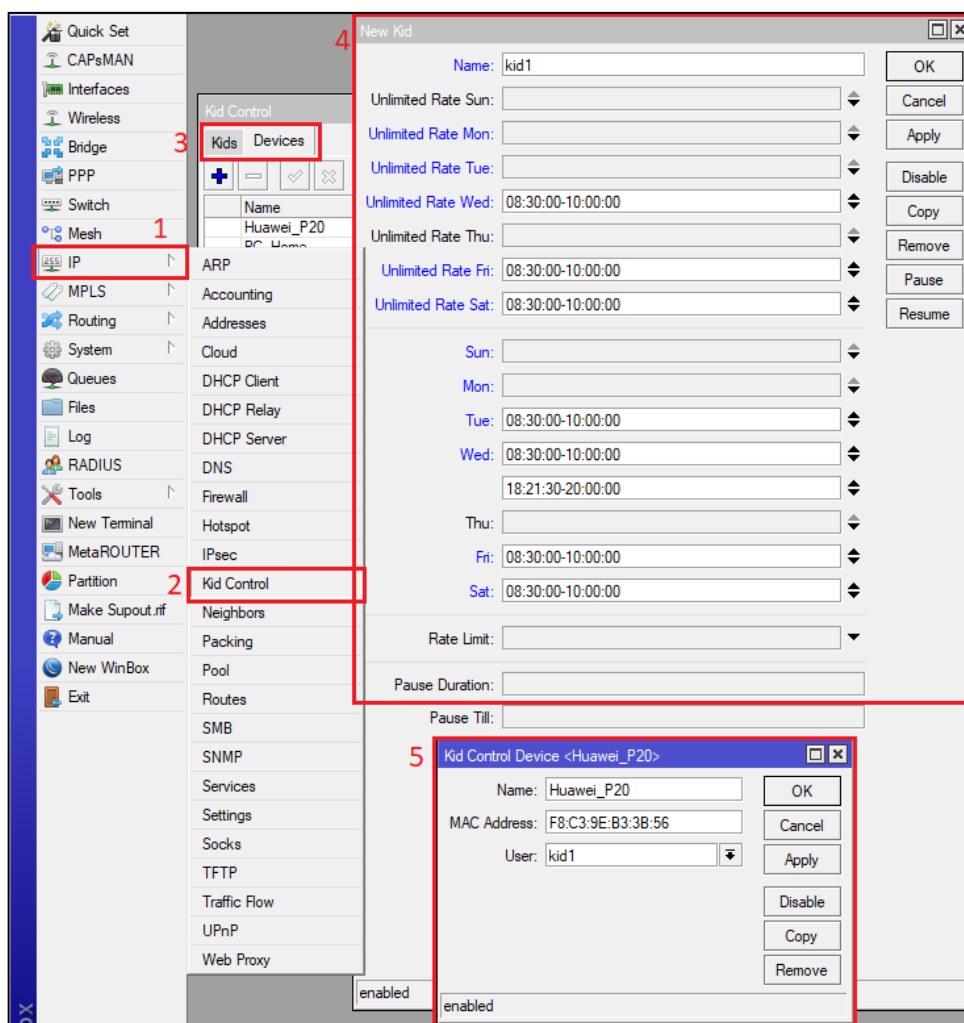
Obr. 18. Příklad nastavení v sekci Bandwidth Control.

4.3.2 Mikrotik RB952Ui-5ac2nD-TC

Jako druhé sledované zařízení se stal Wi-Fi router od Mikrotiku, který s cenou kolem 1 100,- Kč nabízí o poznání více možností nastavení, a i po technické stránce se jedná o kvalitnější zařízení. Do nastavení routeru se uživatel dostane přes IP adresu 192.168.88.1 a následně zadáním hesla. Pro správu nastavení se dá využít Webfix, což je nastavení pomocí prohlížeče, ale jde si také stáhnout aplikaci Winbox. Nastavení může být pro řadu rodičů celkem obtížné, jelikož nastavení není pro začátečníky, ale spíše pro zkušenější uživatele. Nachází se zde velké množství nastavení, a navíc je vše v cizím jazyce. Naštěstí dnešní doba a Internet poskytuje pro uživatele širokou škálu tutoriálů a článků poskytující nejrozličnější pomoc či postupy nejrozličnějších nastavení. Provádět nastavení jde také pomocí příkazového řádku, který nese název Terminal, ke kterému je poskytnut manuál na stránce www.wiki.mikrotik.com [24].

Jelikož tento Wi-Fi router nabízí mnoho nastavení a tato práce se zabývá rodičovskou kontrolou, tak zde budou rozebrána nastavení, která by mohla být užitečná při rodičovské kontrole. Budou tedy vypsány pouze jaké možnosti Wi-Fi router nabízí a co vše lze nastavit, přičemž bude vytvořena ukázka nastavení v Kid Control. V prvním případě je důležité stejně jako u všech Wi-Fi zařízení nastavit silné heslo jak pro přístup k Wi-Fi, tak k samotnému nastavení routeru.

Mikrotik nabízí uživatelům možnost nastavení zaměřenou na rodičovskou kontrolu, která nese název Kid Control. Zde jde přidat v záložce Kids časové omezení neboli lépe řečeno zde lze povolit, v který den i čas může být zařízení připojeno k Internetu. Nastavit jde pro každý den v týdnu neomezené množství časů, to znamená, že zařízení může být povoleno klidně i 10 časů denně. Zároveň jde také nastavit Rate Limit což je omezení rychlosti Internetu a zároveň jde také nastavit, v které časy i dny má být omezení uplatněno a kdy nemá. Díky tomuto postupu se vytvoří profil, který si libovolně uživatel pojmenuje a poté přiřadí ke konkrétním zařízením. Dalším krokem je tedy přidání zařízení a přiřazení účtu, který byl vytvořen na záložce Kids, čímž se na zařízení přenesou vytvořená omezení. Na Obr. 19 je uveden příklad takového nastavení pomocí programu WinBox, kde červený rámeček s čísly 1 a 2 ukazuje, jak se dostat do nastavení Kid Control. Pod číslem 3 se skrývá okno, které zobrazuje záložku Kids a Devices, která se otevře pomocí prvních 2 kroků. Pod 4 je vyobrazen příklad nastavení účtu, který byl pojmenován kid1, kterému byly přiřazeny jak časy omezené, tak i neomezené v jednotlivé dny v týdnu, přičemž nebyl nastaven limit omezení. V rámečku číslo 5 je poté zobrazeno vytvoření zařízení, které nese jméno Huawei_P20 a přidáním jeho MAC adresy, která se zjistí například v záložce Wireless. V posledním kroku poté stačí zařízení přiřadit pouze účet, v tomto případě se jedná o účet kid1. V tuto chvíli by se zařízení s názvem Huawei_P20 mělo chovat podle nastavení, to znamená, že například v pátek mu je povolen přístup k Internetu pouze v čase od 8:30 do 10:00. Samozřejmě jde nastavení účtu pozastavit, čímž bude zařízení poskytnut neomezený přístup k Internetu.



Obr. 19. Nastavení Kid Control ve WinBoxu.

Další možností je blokování webových stránek určených pro dospělé. Mikrotik nabízí více možností blokování stránek, a to za pomoci Web Proxy, Firewallu nebo také DNS. Nejjednodušší je nastavení pomocí DNS, jako tomu bylo v předchozích případech, kde už jsou automaticky zahrnuty prakticky všechny webové stránky určené pro dospělé, které jsou blokovány. První 2 možnosti jsou dobré pro blokování určitých stránek jako je Facebook nebo k blokování stahování určitých souborů jako jsou .mp3, .avi nebo .exe. Navíc se dá nastavit, pro které IP adresy daná blokace má platit, čímž se můžou omezit určitá zařízení podle vlastního uvážení. Na Obr. 20 je ukázka nastavení DNS s názvem FamilyShield, který je nastaven tentokrát přes prohlížeč Webfix, kde červený rámeček s čísly 1 a 2 značí postup, jak se dostat k nastavení DNS na Wi-Fi routeru. V rámečku číslo 3 je poté zobrazeno, kde se má zadat upřednostňovaný (208.67.222.123) a Alternativní (208.67.220.123) server DNS, poté stačí potvrdit tlačítkem Apply.

RouterOS v6.44.3 (stable)

Apply Static Cache

Servers

- 108.67.222.123
- 208.67.220.123

Dynamic Servers

- 8.8.8.8
- 8.8.4.4

Allow Remote Requests ☒

Max UDP Packet Size 4096

Query Server Timeout 2.000 s

Query Total Timeout 10.000 s

Max. Concurrent Queries 100

Max. Concurrent TCP Sessions 20

Cache Size 2048 KiB

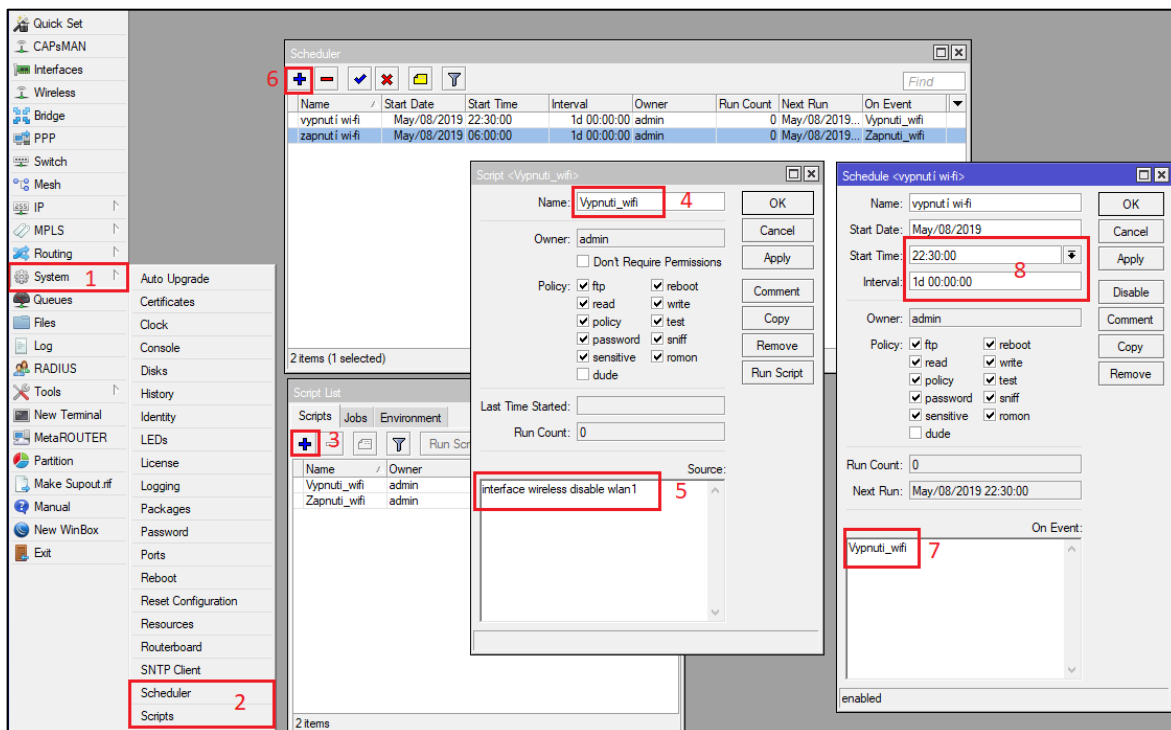
Cache Max TTL 7d 00:00:00

Cache Used 90 KiB

Obr. 20. Nastavení DNS serveru přes WebFix.

Velice oblíbené na internálních zařízeních je nastavení automatického zapnutí a vypnutí Wi-Fi, kterým se všem uživatelům odepře přístup k Wi-Fi síti. Samozřejmě i tuto funkci toto zařízení dokáže, a to například pomocí nastavení scriptů, kde se vytvoří script pro zapnutí (interface wireless disable wlan1) a také pro vypnutí (interface wireless enable wlan1) Wi-Fi sítě. Poté se v plánovači vytvoří plán, kde se vybere vytvořená akce k vypnutí nebo zapnutí. Dále se nastaví datum, čas i opakování dané akce (zapnutí nebo vypnutí Wi-Fi). Vytvoření automatického vypnutí lze shlédnout na Obr. 21, ve kterém je zobrazen červený rámeček s čísly 1 a 2 cestu k oknům Scripts a Scheduler. V dalším kroku je potřeba přes modré znaménko plusu (číslo 3) přidat script a vyplnit údaje, které jsou skryté pod čísly 4 a 5, poté přes tlačítko OK vše potvrdit. V poslední fázi je potřeba opět přes modré znaménko plusu tentokrát u okna Scheduler (číslo 6) přidat plánovač, kdy se má daný script spustit. Vyplnění plánu je zobrazeno v rámečku s čísly 7 (název scriptu) a 8, přičemž je na-

staveno spuštění scriptu ve 22:30:00 a opakování na 1d 00:00:00, tedy každodenní opakování. Vše stačí následně potvrdit tlačítkem OK. Úplně na stejném principu se vytvoří i automatické vypnutí.



Obr. 21. Vytvoření automatického vypnutí pomocí scriptu.

Jako na drtivé většině Wi-Fi routerů i zde jde nastavit, kterým zařízením má být blokován/povolen přístup k Internetu, dále jde nastavit jejich časové trvání, jaké stránky mají být blokovány/povoleny, zda mají být blokovány stránky všem zařízením, které jsou připojené pouze přes Wi-Fi nebo přes LAN apod. Jelikož bylo ukázáno nastavení přes program WinBox, rozhraní prohlížeče Webfix, tak bude uveden příklad nastavení pomocí příkazového řádku, v tomto případě se jedná o Terminál. Na Obr. 22 je ukázáno zablokování zařízení přes MAC adresu pomocí zmíněného příkazového řádku Terminál, kde se nachází tento řádek je vidět na Obrázku pod číslem 1. Následně se do otevřeného příkazového řádku zapíše příkaz, který zablokuje zařízení s MAC adresou F8:C3:9E:B3:3B:56, což ostatně ukazuje číslo 2. Jelikož se jedná o zařízení, které je připojené k routeru pomocí Wi-Fi sítě, tak se tato adresa bude hledat v sekci Wireless Tables a to buď v záložce Registration nebo Connect List jak je vyobrazeno pod číslem 3. Po zadání příkazu a potvrzení se vytvoří ve Firewallu pravidlo, které právě výše zmíněné zařízení zablokuje. V této chvíli po rozkliknutí tohoto pravidla jdou dále nastavovat další možnosti, jako je kdy toto pravidlo má platit apod., které se zapíší do příslušných polí [24].

The screenshot shows the MikroTik WinBox interface. On the left is a sidebar with various configuration categories. The main window is divided into two panes. The top pane, titled 'Wireless Tables', shows a table of wireless interfaces. The bottom pane is a terminal window showing the command-line interface of a MikroTik Router.

Wireless Tables:

#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0	wlan2	F8:C3:9E:B3:3B:56	yes		-120..120	default

Terminal:

```
MikroTik Router0
[?]          Gi
command [?]  Gi

[Tab]        Co
              a

/            Mo
..           Mo
[admin@MikroTik] >
[admin@MikroTik] > /ip firewall filter add chain=forward src-mac-address=F8:C3:9E:
B3:3B:56 action=drop
[admin@MikroTik] >
```

Red boxes and numbers highlight key elements: 'New Terminal' in the sidebar (1), the MAC address 'F8:C3:9E:B3:3B:56' in the table (3), and the firewall filter command in the terminal (2).

Obr. 22. Příklad zablokování zařízení pomocí MAC adresy přes Terminál.

5 TESTOVÁNÍ A VYHODOCENÍ RODIČOVSKÉ KONTROLY

Všechny výše uvedené software i hardware v této části projde testováním určitých bodů, podle kterých se následně udělá vyhodnocení. Cílem je vytvoření přehledné tabulky, která by měla vykazovat odpovědi na dané body, podle kterých by mělo být patrné co daný software, popřípadě hardware zvládne a co už ne. Odpovědi na jednotlivé otázky budou značeny symboly ✓, které představují úspěšné zvládnutí testu nebo ✗, které naopak znamenají neúspěch.

5.1 Test aplikací na PC

Jako první se testování zaměří na aplikace/programy, které byly podrobněji rozebrány a popsány v kapitole 3.1, která se věnovala PC/notebookům. Pro testování těchto aplikací bylo vytvořeno celkem 25 testových otázek/úkolů, které buď zaznamenaly úspěšné zvládnutí, nebo naopak neúspěšné. Otázky se zaměřily jak na blokování či omezení nevhodných webových stránek, aktivit, aplikací, tak i na sledování aktivit nebo zobrazování statistik. Výsledky jednotlivých bodů jsou tak k vidění v Tab. 1, ve které je na konci celkový počet úspěšných odpovědí.

Seznam testovaných aplikací:

- A Rodičovská kontrola Windows
- B Open DNS – FamilyShield
- C Weblocker
- D PC Screen Watcher
- E ManicTime

Tab. 1. Testované aplikace na PC s výsledky.

Test	A	B	C	D	E
1. Filtr webových stránek (pornografie)	✓	✓	✓	✗	✗
2. Filtr webových stránek (hazard, sociální sítě, malware...)	✗	✓	✓	✗	✗
3. Možnost přidání/odebrání blokováných web. stránek	✓	✗	✓	✓*	✗
4. Nastavení časové omezení pro určité webové stránky	✗	✗	✓	✓*	✗
5. Blokace výrazů pro dospělé ve vyhledávači	✓	✗	✓	✓*	✗

6. Blokace na všech web. prohlížečích	x	✓	✓	✓*	x
7. Zobrazení navštívených/vyhledávaných web. stránek	✓	x	x	x	✓
8. Zablokování zařízení	✓	x	x	x	x
9. Časový harmonogram zařízení	✓	x	x	✓	x
10. Časový limit zařízení	✓	x	x	✓	x
11. Přidání výjimky pro časový limit	x	x	x	✓	x
12. Blokování aplikací/programů	✓	x	x	✓	x
13. Omezení času aplikací/programů	x	x	x	✓	x
14. Omezení aplikací podle věkového hodnocení	✓	x	x	x	x
15. Zaslání zprávy dítětem o povolení/prodloužení aktivit	✓	x	x	x	x
16. Sledování aktivity	✓	x	x	x	✓
17. Zobrazení stráveného času na jednotlivých aplikacích	✓	x	x	x	✓
18. Zobrazení aktivit ve vybraný čas	x	x	x	x	✓
19. Pořizování Screenshotů (snímků obrazovky)	x	x	x	✓	✓
20. Pořizování záznamu stisknutých kláves	x	x	x	✓	x
21. Sledování emailového účtu dítěte	x	x	x	✓	x
22. Přesné použití aplikace (MS Word – název souboru)	x	x	x	x	✓
23. Procentuální zobrazení používání aplikací	x	x	x	x	✓
24. Zobrazení statistik	x	x	x	x	✓
25. Zjištění polohy zařízení	✓	x	x	x	x
Celkový počet ✓	13	3	6	12	8

* pokud se nastaví v pravidlech výraz či stránka, která má být blokována, tak při vyhledávání takového výrazu/web. stránky dojde po cca 3 vteřinách k vypnutí webového prohlížeče.

Vyhodnocení

Z celkového počtu úspěšných bodů, které jsou patrné z Tab. 1 vyšly nejlépe 2 aplikace, a to Rodičovská kontrola Windows a PC Screen Watcher, které získali 13, respektive 12 bodů

z celkových 25. Důležité je také zmínit, že u 4 bodů co získala aplikace PC Screen Watcher visí otazník, který je označen hvězdičkou a je vysvětlen pod tabulkou. Proto se nejlépe jeví aplikace rodičovské kontroly od Windows, která se zabývá širšímu obzoru zabezpečení a jedná se tak o celkem solidní základ rodičovské kontroly, který by spolu s minimálně jedním z dále umístěných aplikací mohl vytvořit dobrou spolupráci v rámci kontroly dětí. Jednou takovou aplikací může být ManicTime, který se zabývá monitorováním toho, co dítě na zařízení dělá, jak tráví čas, kolik hodin denně se věnuje, které aplikaci apod. a z výsledků je patrné, že z testovaných 5 aplikací je v této kategorii nejlepší. To samé se dá říci o WebLockeru, který zase vyšel v testu nejlépe v blokování webových stránek a mohl by tak spolu s Rodičovskou kontrolou Windows a aplikací ManicTime vytvořit opravdu silnou trojku v oblasti kontroly dětí na PC.

5.2 Test aplikací na mobilních zařízeních

Testování bylo také provedeno na aplikacích rodičovské kontroly na mobilních telefonech/tabletech, které používají OS Android. Tyto aplikace byly rozebrány v kapitole 3.2. Stejně jako u předchozího testu, byly i zde vytvořeny otázky, podle kterých proběhlo hodnocení. V tomto případě se jedná o 29 testových otázek/bodů, které jsou k vidění v Tab. 2, opět na konci s celkovým počtem úspěšných zvládnutí. Z testování byla vynechána pouze aplikace Spyzie, která bezplatně nabízí pouze demo verzi nastavení na svých stránkách. Z toho důvodu, nelze ověřit funkčnost jednotlivých bodů.

Seznam testovaných aplikací:

- A Obchod Google Play
- B Google Family Link
- C SecureKids
- D Kids Zone

Tab. 2. Testované aplikace na mobilních zařízeních s výsledky.

Test	A	B	C	D
1. Filtr webových stránek (pornografie)	✗	✓	✓	✗
2. Filtr webových stránek (hazard, sociální sítě, malware...)	✗	✗	✓	✗
3. Možnost přidání/odebrání blokováných webových stránek	✗	✓	✓	✗

4. Blokace výrazů pro dospělé ve vyhledávači	x	✓	✓	x
5. Blokace na všech web. prohlížečích	x	x	x	x
6. Zobrazení navštívených/vyhledávaných webových stránek	x	x	x	x
7. Zablkování zařízení	x	✓	✓	✓
8. Časový harmonogram zařízení	x	x	✓	x
9. Časový limit zařízení	x	✓	x	✓*
10. Nastavení večerky	x	✓	✓	x
11. Blokování aplikací	x	✓	✓	✓
12. Omezení času aplikací	x	x	✓*	x
13. Spravování oprávnění aplikací	x	✓	x	x
14. Zaslání zprávy dítětem o povolení/prodloužení aktivit	x	✓	✓	x
15. Sledování aktivity	x	✓	✓	x
16. Zobrazení stráveného času na jednotlivých aplikacích	x	✓	✓	x
17. Procentuální zobrazení používání aplikací	x	x	✓	x
18. Zobrazení statistik	x	x	✓	x
19. Zjištění polohy zařízení	x	✓	✓	x
20. Omezení/zakázání stahování z Google Play obchodu	✓	✓	x	x
21. Požadování ověření při nákupech na Google Play	✓	✓	x	x
22. Zakázání stahování z neznámých zdrojů	x	✓	x	x
23. Zobrazení stavu baterie na zařízení dítěte	x	x	✓	x
24. Nastavení budíků	x	x	✓	x
25. Zobrazení/zaslání seznamu upozornění	x	✓	✓	x
26. Správa hovorů	x	x	✓*	x
27. Zaslání nouzového zprávy	x	x	✓	x
28. Online nastavení	x	✓	✓	x

29. Vytvoření omezeného účtu dítěte na zařízení rodiče	x	x	x	✓
Celkový počet ✓	2	17	21	4

* Nabízí pouze placená služba

Vyhodnocení

Při pohledu na Tab. 2, jde zjistit, že nejlépe obstála aplikace SecureKids, která získala z 29 testovaných otázek hned 21 bodů, i když 2 body získala přesto, že se jedná o placenou službu. Z tabulky je patrné, že se aplikace věnovala nejširšímu spektru možností kontroly od blokování webových stránek až po časový harmonogram nebo správu hovorů. Vůbec špatně nedopadla ani aplikace Family Link od Googlu, která se ziskem 17 bodů jeví také jako dobrá varianta. Oproti vítězi se sice nezabývá správou hovorů, zobrazením statistik nebo nastavením budíků, ale naopak nabízí omezení stahování, časový limit zařízení nebo správu aplikací.

5.3 Test na Wi-Fi routeru

V poslední části se práce zaměřila také na testování dvou výše zmíněných Wi-Fi routerů z kapitoly 3.3, pro které bylo vytvořeno celkem 17 testových otázek, na které se bude stejně jako u předchozích variant odpovídat kladně nebo záporně. Tyto otázky se zaměřili hlavně na blokování stránek nebo omezení přístupu k Internetu. Výsledky jednotlivých otázek jsou zobrazeny v Tab. 3.

Seznam testovaných aplikací:

- A Tenda F303 Wireless-N
- B Mikrotik RB952Ui-5ac2nD-TC

Tab. 3. Testované Wi-Fi routery s výsledky.

Test	A	B
1. Blokace web. stránek (pomocí DNS)	✓	✓
2. Vlastní blokace stránek	x	✓
3. Blokace webových stránek na určitých zařízeních	✓	✓
4. Blokace různých webových stránek na různých zařízeních	x	✓
5. Nastavení časového omezení blokace webových stránek	✓	✓

6. Zakázání/povolení přístupu k Internetu	✓	✓
7. Omezení přístupu k Internetu na každý den zvlášť	✗	✓
8. Omezení limitu stahování	✓	✓
9. Omezení limitu stahování na každý den zvlášť	✗	✓
10. Omezení limitu nahrávání	✓	✓
11. Omezení limitu nahrávání na každý den zvlášť	✗	✓
12. Zadání více času omezení denně	✗	✓
13. Možnost omezení každého zařízení zvlášť	✗	✓
14. Možnost nastavení automatického vypnutí/zapnutí Wi-Fi	✗	✓
15. Zakázání stahování určitých souborů (.avi, .mp3, .exe atd.)	✗	✓
16. Nastavení pomocí příkazového řádku	✗	✓
17. Blokace určitých LAN/WLAN	✗	✓
Celkový počet ✓	6	17

Vyhodnocení

Z výsledku testu dvou Wi-Fi routerů, který lze zjistit z Tab. 3 vyšel jednoznačně lépe Mikrotik, který ve všech 17 sledovaných bodech úspěšně prošel, zatímco zařízení od společnosti Tenda získalo pouze 6 bodů, přičemž by rozdíl mohl být daleko větší, pokud by se test zabýval daleko hlubším zkoumáním. Router Tenda disponuje pouze základními funkcemi jako je blokování webových stránek pomocí DNS serverů, nebo blokování přístupu zařízení k Internetu a jeho časové omezení. Zatímco zařízení od Mikrotiku nabízí navíc široké spektrum možností od nastavení automatického vypínání/zapínání routeru, Blokování WLAN/LAN, zakázání stahování určitých souborů jako je .mp3 nebo .exe, či omezením více zařízeníů řadou omezení najednou. Jediným negativem vítězného Wi-Fi routeru je jeho složitější nastavování, které tak není pro tzv. laiky, ale spíše pro zralejší uživatele.

ZÁVĚR

Bakalářská práce se zabývala problematikou zaměřenou na rodičovskou kontrolu u zařízení, které používají děti. Hlavním cílem tak bylo navrhnout vhodné aplikace pro tato zařízení dětí, pro bezpečné používání v tzv. světě online.

V teoretické části se práce zaměřila na literární rešerši hrozeb IT, která si rozdělila do 5 hlavních skupin. V komunikačních hrozbách byly popsány pojmy jako jsou kyberšikana, kyberstalking, kybergrooming nebo sexting. Další skupina, která se v práci objevuje je Obsahová, která se zabývá nevhodným obsahem na Internetu jako je násilí nebo pornografie a pro děti je tak jednou z nejnebezpečnějších. Mezi další skupinu hrozeb byla zařazena i závislost, která se může projevit hraním her, na sociálních sítích nebo na Internetu obecně. Posledními 2 skupinami je škodlivý obsah, který se zabývá viry, spamem, spywarem apod. a také svoji vlastní skupinu hrozeb získali i sociální sítě, které představují také určité riziko pro děti, hlavně v podání oblíbeného Facebooku.

Praktická část se poté v první části věnovala možnostem rodičovské kontroly z pohledu obecných rad a tipů, následně se věnovala těmto možnostem za předpokladu použití specializovaných softwarů. Druhá část se už zabývala jednotlivým zařízením IT a aplikacím pro rodičovskou kontrolu. Ve 4. kapitole se tak práce na úvod věnovala programům rodičovské kontroly na PC, kde byly popsány programy/možnosti: Rodičovská kontrola Windows, OpenDNS, WebLocker, PC Screen Watcher a ManicTime. Poté následovaly mobilní aplikace rodičovské kontroly, které byly prozkoumány a popsány. Jedná se o následující aplikace Obchod Google Play, Google Family Link, SecureKids, Kids Zone a v neposlední řadě se také práce zmíní o placené službě Spyzie, která ovšem nabízí prakticky vše, na co si jen rodič vzpomene. Věnováno několik stránek bylo také 2 Wi-Fi routerům, které byly prozkoumány z pohledu nabízených možností rodičovské kontroly.

Na závěr se práce zaměřila na testování jednotlivých aplikací pomocí vytvořených otázek s následným vyhodnocením, která aplikace či kombinace aplikací vychází z testu nejlépe. U PC se nejlépe jeví kombinace Rodičovské kontroly Windows, spolu s aplikací WebLocker určenou k blokování nevhodných stránek a programem ManicTime, který je naopak skvělý v monitorování aktivit. Za mobilní aplikace nejlépe obstál SecureKids, který se věnuje širokému spektru možností od blokování stránek až po sledování aktivit nebo správu hovorů. Velice dobře dopadl také Google Family link, který ve výsledku zaostál pouze o 4 body. V testování Wi-Fi routerů se stal jednoznačným vítězem router od Mikrotiku.

SEZNAM POUŽITÉ LITERATURY

- [1] ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013, 224 s. ISBN 978-80-251-3804-5.
- [2] ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Vyd. 1. Praha: Grada, 2014. 183 s. Psyché.
- [3] HOLLÁ, Katarína. Sexting a kyberšikana. Vydanie: prvé. Bratislava: Iris, 2016. 165 stran.
- [4] *Internetem bezpečně* [online]. Karlovy Vary: you connected, c2018 [cit. 2018-11-24]. Dostupné z: <https://www.internetembezpecne.cz>
- [5] *Bezpečně online* [online]. Praha: Národní centrum bezpečnějšího internetu, c2017 [cit. 2018-11-24]. Dostupné z: <https://bezpecne-online.saferinternet.cz>
- [6] MÁCA, Roman. Děti a rizika sociálních sítí. In: *Šance dětem* [online]. Praha 1: Obecně prospěšná společnost Sirius, 2014 [cit. 2019-02-28]. Dostupné z: <https://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-social-nich-siti-112.html>
- [7] HOLZMAN, Ondřej. Bud' safe online. In: *Tyinternety.cz* [online]. 2018 [cit. 2019-02-28]. Dostupné z: <https://tyinternety.cz/digital/bud-safe-online-avast-youtuberem-jirkou-kralem-uci-deti-bezpecnosti-internetu/>
- [8] *Children and Parents: Media Use and Attitudes Report* [online]. Londýn: ofcom, 2017 [cit. 2019-02-02]. Dostupné z: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf
- [9] Netholismus - závislost na internetu. In: *PSYCHOTERAPIE ANDĚL* [online]. Praha: Psychologické centrum PSYCHOTERAPIE ANDĚL, c2019 [cit. 2019-02-28]. Dostupné z: <https://www.psychoterapie-andel.cz/netholismus-zavislost-na-internetu/>
- [10] *Avast* [online]. Praha: Avast Software, c1988 [cit. 2019-02-28]. Dostupné z: www.avast.com
- [11] *HOAX* [online]. Třebíč: DIGITAL ACTION, c2000 [cit. 2019-02-28]. Dostupné z: <http://www.hoax.cz/cze/>
- [12] *Projekt E-Bezpečí* [online]. Olomouc: Pedagogická fakulta Univerzity Palackého, c2008 [cit. 2019-02-28]. Dostupné z: <http://www.e-bezpeci.cz/index.php>

- [13] *Sexting* [online]. Olomouc: Centrum prevence rizikové virtuální komunikace, c2010-2013 [cit. 2019-02-12]. Dostupné z: <https://www.sexting.cz/>
- [14] V jakém věku dát dětem elektroniku?. In: *Blog Mall.cz* [online]. Praha: Internet Mall, 2018 [cit. 2019-05-12]. Dostupné z: <https://blog.mall.cz/technologie/v-jakem-veku-dat-detem-elektroniku-naucte-je-na-ni-postupne-748.html>
- [15] Téměř čtvrtina dětí dostane... In: *O2* [online]. Praha: O2 Czech Republic, 2017 [cit. 2019-02-12]. Dostupné z: https://www.o2.cz/spolecnost/tiskove-centrum/552886-Temer_ctvrtina_deti_dostane_svu_j_mobil_uz_v_predskolnim_veku_O_jejich_bezpeci_na_internetu_se_vsak_rodice_prilis_nestaraji.html
- [16] Přelom roku splnil Microsoftu přání... In: *Živě.cz* [online]. Praha: CZECH NEWS CENTER, 2019 [cit. 2019-02-22]. Dostupné z: <https://www.zive.cz/clanky/prelom-roku-splnil-microsoftu-prani-windows-10-uz-se-konecne-pouzivaji-vice-nez-windows-7/sc-3-a-196551/default.aspx>
- [17] Správa účtu. *Microsoft* [online]. c2019 [cit. 2019-05-12]. Dostupné z: <https://account.microsoft.com/account/manage-my-account>
- [18] SET UP OPENDNS ON YOUR DEVICE. *OpenDNS* [online]. San Jose: Cisco Systems, c2019 [cit. 2019-05-12]. Dostupné z: <https://www.opendns.com/setup-guide/#familyshield>
- [19] *Goppie.inc* [online]. 2013 [cit. 2019-05-12]. Dostupné z: <https://sites.google.com/site/goppieinc/>
- [20] *Time Tracker Management Tracking Software* [online]. ManicTime, c2019 [cit. 2019-05-12]. Dostupné z: <https://www.manictime.com/>
- [21] Jak ochránit děti před nevhodným obsahem?. In: *Mobinfo.cz* [online]. Brno: DK Media Net s.r.o, 2016 [cit. 2019-05-12]. Dostupné z: <http://www.mobinfo.cz/jak-ochranit-deti-pred-nevhodnym-obsahem-navod/>
- [22] Kompatibilita zařízení. *Google Family Link* [online]. Mountain View: Google, c2019 [cit. 2019-05-12]. Dostupné z: <https://families.google.com/intl/cs/family-link/device-compatibility/>
- [23] *Spyzie* [online]. c2019 [cit. 2019-05-12]. Dostupné z: <https://www.spyzie.com/>
- [24] *Mikrotik Wiki* [online]. Mikrotik, 2017 [cit. 2019-04-29]. Dostupné z: https://wiki.mikrotik.com/wiki/Main_Page

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Information Technology
FB	Facebook
PC	Personal Computer
DNS	Domain Name System
OS	Operating System
PEGI	Pan European Game Information
PIN	Personal Identification Number
USD	United States Dollar
LAN	Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
IP	Internet Protocol
IPv4	Internet Protocol version 4
TCP	Transmission Control Protocol
SMS	Short message service
RPG	Report Program Generator
KB/s	Kilobyte Per Second
MAC	Media Access Control

SEZNAM OBRÁZKŮ

<i>Obr. 1. Procentuální znázornění dětí vlastníci telefony podle věku [8].</i>	10
<i>Obr. 2. Výstupní data z keyloggerru [4].</i>	23
<i>Obr. 3. Příklad phishingu neboli podvodného e-mailu od České spořitelny.</i>	26
<i>Obr. 4. Využívání sociálních sítí podle věkových skupin [7].</i>	28
<i>Obr. 5. Sekce Aktivita.</i>	36
<i>Obr. 6. Nastavení časového plánu.</i>	37
<i>Obr. 7. Nastavení DNS serveru.</i>	39
<i>Obr. 8. Vzhled WebLockeru a jeho nastavení.</i>	40
<i>Obr. 9. PC Screen Watcher – nastavení pravidel.</i>	43
<i>Obr. 10. Program ManicTime, záložka Den.</i>	45
<i>Obr. 11. Nastavení Obchodu Play.</i>	47
<i>Obr. 12. Možnosti Google Family Linku.</i>	48
<i>Obr. 13. Možnosti nastavení a příklad přestávky.</i>	50
<i>Obr. 14. SecureKids na zařízení dítěte.</i>	51
<i>Obr. 15. Povolení aplikací a náhled účtu dítěte.</i>	52
<i>Obr. 16. Ukázka demo verze Spyzie.</i>	53
<i>Obr. 17. Parental Controls a jeho nastavení.</i>	55
<i>Obr. 18. Příklad nastavení v sekci Bandwidth Control.</i>	56
<i>Obr. 19. Nastavení Kid Control ve WinBoxu.</i>	58
<i>Obr. 20. Nastavení DNS serveru přes WebFix.</i>	59
<i>Obr. 21. Vytvoření automatického vypnutí pomocí scriptu.</i>	60
<i>Obr. 22. Příklad zablokování zařízení pomocí MAC adresy přes Terminál.</i>	61

SEZNAM TABULEK

<i>Tab. 1. Testované aplikace na PC s výsledky.</i>	<i>62</i>
<i>Tab. 2. Testované aplikace na mobilních zařízeních s výsledky.</i>	<i>64</i>
<i>Tab. 3. Testované Wi-Fi routery s výsledky.</i>	<i>66</i>

SEZNAM PŘÍLOH

P I Programy PC

P II Aplikace Mobil

PŘÍLOHA P I: PROGRAMY PC

Rodičovská kontrola Windows

Správa účtu dítěte probíhá po přihlášení se na stránkách Microsoftu a propojení účtu dítěte s účtem rodiče.

Odkaz: <https://account.microsoft.com/account>

Family Shield - OpenDNS

Pro použití OpenDNS Family Shieldu tato bakalářská práce využila webové stránky poskytovatele.

Odkaz: <https://www.opendns.com/setupguide/#familyshield>.

WebLocker

Pro stažení programu WebLocker byl využit softwarový portál Stahuj.cz, ze kterého byla stažena nejnovější verze 2.1.1.

Odkaz: https://www.stahuj.cz/internet_a_site/prohlizece_a_rozsireni/filtry/weblocker-2/

PC Screen Watcher

Pro stažení programu PC Screen Watcher byla využita webová stránka goppie.inc, ze které byla stažena nejnovější verze 1.3.

Odkaz: <https://sites.google.com/site/goppieinc/pc-screen-watcher>

ManicTime

Pro stažení nejnovější verze 4.2.8 programu ManicTime, byla využita domovská stránka programu.

Odkaz: <https://www.manictime.com/>

PŘÍLOHA P II: APLIKACE MOBIL

Obchod Google Play

Pro nastavení rodičovské kontroly u této aplikace není potřeba žádné stahování.

Google Family Link

Při použití rodičovské kontroly Family Link od Googlu, je zapotřebí aby si rodič stáhnul z Google obchodu mobilní aplikaci určenou pro rodiče, naopak dítě si musí stáhnout aplikaci určenou pro děti a teenagery.

Odkaz pro rodiče: https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylink&hl=cs&referrer=utm_source%3Dfamilylink%26utm_medium%3Dwebsite%26utm_campaign%3Dgetapp

Odkaz pro děti: <https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylinkhelper>

SecureKids

Pro stažení nejnovější verze 0.24 byl využit opět Google obchod, ze kterého byla stažena společná aplikace určená jak pro rodiče, tak i děti.

Odkaz: https://play.google.com/store/apps/details?id=com.securekids.launcher_reloaded&referrer=utm_source%3Dhttps%253A%252F%252Fsecurekids.es%252F%26utm_medium%3Dslider%26utm_term%3DDescargas%2520desde%2520el%2520Slider%26utm_content%3DDescargate%2520al%2520app%26utm_campaign%3DSlider%2520SecureKids

Kids Zone

V tomto případě stačí stáhnout pouze jednu aplikaci, a to na zařízení, na kterém se bude vytvářet profil dítěte.

Odkaz: <https://play.google.com/store/apps/details?id=com.ootpapps.kids.zone.app.lock>

Spyzie

Vyzkoušení demoverze či stažení a předplacení nabízených služeb aplikace lze na stránkách poskytovatele.

Odkaz: *<https://www.spyzie.com/>*