Univerzita Pardubice
Fakulta ekonomicko-správní

Hrozby a rizika na sociálních sítích

Petr Vitouš

Bakalářská práce

2018

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr Vitouš**
Osobní číslo:	**E14262**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Hrozby a rizika na sociálních sítích**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce bude popsat a zmapovat problematiku rizik sociálních sítí, vysvětlit pojem kybernetická trestná činnost a předložit možnosti výskytu těchto činů na sociálních sítích. V závěru práce budou doporučení pro minimalizaci rizik na sociálních sítích pro vybranou věkovou skupinu uživatelů.
Osnova:
- Teoretický úvod do problematiky kybernetické trestné činnosti
- Sociální sítě, specifikace hrozeb a rizik na sociálních sítích
- Výběr cílové skupiny uživatelů
- Doporučení pro minimalizaci rizik na sociálních sítích

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

GRAGIDO, Will., John. PIRC a Russ. ROGERS. Cybercrime and espionage: an analysis of subversive multivector threats. Oxford: Elsevier Science, c2011. ISBN 1597496138.
JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

[redacted]

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

Datum zadání bakalářské práce: **1. září 2017**

Termín odevzdání bakalářské práce: **30. dubna 2018**

[redacted]

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

[redacted]

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2017

Prohlašuji:

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

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 27. 6. 2018

Petr Vitouš

PODĚKOVÁNÍ

Chtěl bych poděkovat Ing. Renátě Máchové, Ph.D. za vedení mé bakalářské práce, trpělivost, cenné rady a odborný dohled. Dále děkuji všem, kteří mě až do konce psaní bakalářské práce podporovali.

ANOTACE

Bakalářská práce „Hrozby a rizika na sociálních sítích“ pojednává o fenoménu poslední doby – sociálních sítích ve spojení s možnými hrozbami a riziky, se kterými se uživatel při jejich používání může setkat. Cílem práce je zmapování tohoto prostředí, specifikace hrozeb a rizik a doporučení pro jejich minimalizaci. Pro potřeby práce byla vybrána nejohroženější skupina uživatelů sociálních sítí, a to adolescenti ve věku 11-ti až 15-ti let odpovídající žákům 2. stupně základní školy.

KLÍČOVÁ SLOVA

Sociální sítě, kyberkriminalita, rizika, děti, prevence, programy rodičovské kontroly.

TITLE

Threats and risks on social networks

ANNOTATION

This Bachelor thesis „Treats and risks on social networks“ deals with the phenomen of the last years – social networks with the possible threats and risks that the user may encounter. The aim of the thesis is to map this environment, specification of threats and risks and recommendations for their minimization. For the thesis needs, adolescents in the age 11-15 years (students of the second grade of elementary school) was selected.

KEYWORDS

Social networks, kybercrime, risks, children, prevention, parental control programs.

OBSAH

SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

AHP	Analyticko-hierarchický proces
BBS	Bulletin board system
CDP	Criterium DecisionPlus
CEO	Command executive order
CSR	Corporate social responsibility
HTTPS	Hypertext Transfer Protocol Secure
ICT	Informační a komunikační technologie
IRC	Internet relay chat
MS-DOS	Microsoft Disk Operating System
PC	Personal computer – osobní počítač
SMS	Short message service

ÚVOD

Vzhledem k tomu, že člověk je tvor společenský a nejspíše i díky možnosti být nepřetržitě online jsou jedním z největších trendů dnešní doby sociální sítě. Člověk tak může být téměř nepřetržitě v kontaktu se svými blízkými a sdílet s nimi vše, co uzná za vhodné. Toto sebou ovšem přináší i spoustu hrozeb a rizik.

S rozmachem sociálních sítí vzrůstá i kybernetická trestná činnost. Tato činnost je oprávněně považována za vážnou hrozbu nejen pro jedince, ale i pro společnost. Každý, kdo používá počítač a sociální sítě může být ohrožen. Proto je potřeba při užívání počítače, respektive používání sociálních sítí naučit se využívat všech nabízených funkcí. Také je žádoucí naučit se identifikovat možné hrozby, a přizpůsobit své chování/počínání tak, aby se eliminovaly případné nežádoucí dopady.

Práce bude zaměřena na problematiku rizik sociálních sítí, podrobně vysvětlí pojem kybernetická trestná činnost a předloží možnosti výskytu těchto činů na sociálních sítích. V závěru práce budou doporučení pro minimalizaci rizik na sociálních sítích pro vybranou věkovou skupinu uživatelů.

1 ÚVOD DO PROBLEMATIKY KYBERNETICKÉ TRESTNÉ ČINNOSTI

Během posledních dvou desetiletí se svět stal propojenějším než kdykoliv předtím. Geografické rozdíly byly smazány s nástupem moderních datových a telekomunikačních sítí a internetem jako takovým. Naše životy, práce, ambice, trávení volného času, identita jsou propletené sítí nul a jedniček ve virtuálním světě. Neočekávaným, leč nezbytným vedlejším produktem této evoluce je výskyt nového druhu kriminální aktivity tzv. kybernetické trestné činnosti [12]. V následujících kapitolách vysvětlím především pojmy související s touto problematikou a nastíním jednotlivé druhy kyberkriminality.

1.1 Vznik kyberprostoru

Když v roce 1968 došlo ke spuštění počítačové sítě prostřednictvím propojení počítačů čtyř amerických univerzit, s jistotou se dá říct, že šlo o první zárodek internetu. Bohužel v té době šlo o obrovský rozmach internetu a na bezpečnostní sítě a protokoly nebyl kladen takový důraz jako dnes. Tyto slabiny se staly cílem nelegálních aktivit probíhajících právě v počítačových sítích. Rychlost, kterou v té době prodělával vývoj počítačových a komunikačních technologií, byla nevídaná a společnost na ni reagovala z technického hlediska se zpožděním [17].

Vznik kyberprostoru tzv. pátou dimenzí života společnosti postupně nabýval všech společenských atributů – politických, obchodních, emocionálních, kultovních nebo náboženských. Do tohoto prostoru se postupně přenášely všechny rysy dobové společnosti, a tento prostor si postupně vytváří vlastní pravidla, která se však vymykají přirozenému řádu pro lidskou společnost. Tento způsob existence však přináší i jistá nebezpečí, se kterými se společnost musí vypořádat, naučit se je akceptovat, popř. najít způsoby, jak jim čelit [17].

S poněkud „vědečtější“ definicí přišel později teoretik a spoluzakladatel Elextronic Frontier Foundation John Barlow. Ten tento pojem představil jako existující počítačové sítě a veškeré telekomunikační sítě. Zcela zřejmým příkladem kyberprostoru mohou být systémy virtuální reality a další druhy virtuálních a počítačem simulovaných prostředí. V neposlední řadě do kyberprostoru zasahují i počítačové hry a internet [17].

Je nutné si zpočátku uvědomit, že s příchodem kyberprostoru dochází ke vzniku tzv. projekcí pachatelů, které mohou být vzdálené od skutečných rysů pachatele. S tímto faktem se stávající metody vyšetřování a samotné chápání trestných činů velice obtížně vyrovnávají [17]. Od prostředí kyberprostoru je odvozen pojem kybernetické kriminality/kybernetické trestné činnosti.

1.2 Vymezení Kybernetické trestné činnosti

Kybernetickou trestnou činnost lze datovat a přisoudit okamžiku tzv. zlidovění počítačů, kdy se osobní počítače staly dostupnou možností pro běžné uživatele. Toto se odvíjí od vzniku počítačových sítí a internetu zmíněném výše.

Globální povaha internetu a snadnost vzniku a následné distribuce nelegálních materiálů mezi různými servery a uživateli internetu vedla a vede ke vzniku velkého problému, kterým bezpochyby kyberkriminalita je. Mezi nejrizikovější skupinu patří právě děti, kde získávání osobních informací, fotografií, popř. videí obětí, vystavování nebezpečným a nevhodným materiálům jako je např. pornografie a sexuálně agresivní chování, kybergrooming, násilí různého druhu, pobízení k nebezpečnému a nevhodnému chování a také kyberšikana je usnadněna prostřednictvím komerčních internetových stránek, osobních webových stránek, popř. níže zmiňovaných sociálních sítí [14].

V první řadě je třeba si vymezit pojem kybernetická trestná činnost. Při popisu tohoto pojmu si je nutno uvědomit, že spolu s rozmachem informačních a komunikačních prostředků roste i možnost jejich užívání/zneužívání k páchání trestné činnosti [20]. Různí autoři i různé právní normy používají pro označení těchto aktivit různé pojmy, mezi které patří: informační, informatická, elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer-related-crime, počítačová kriminalita, kybernetická trestná činnosti, kyberkriminalita, aj. [20].

„Tzv. kybernalitou neboli kybernetickou kriminalitou rozumíme činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.“ [17].

Skutečným problémem kybernality je globální prostředí, ve kterém se pachatel může neomezeně pohybovat a měnit svoji identitu, popř. využívat variability předpisů v různých jurisdikcích. Tato kriminalita představuje pro společnost hrozby, které nejsou reálně viditelné a konečné důsledky nejsou s průběhem páchaného trestného činu viditelně spjaty.

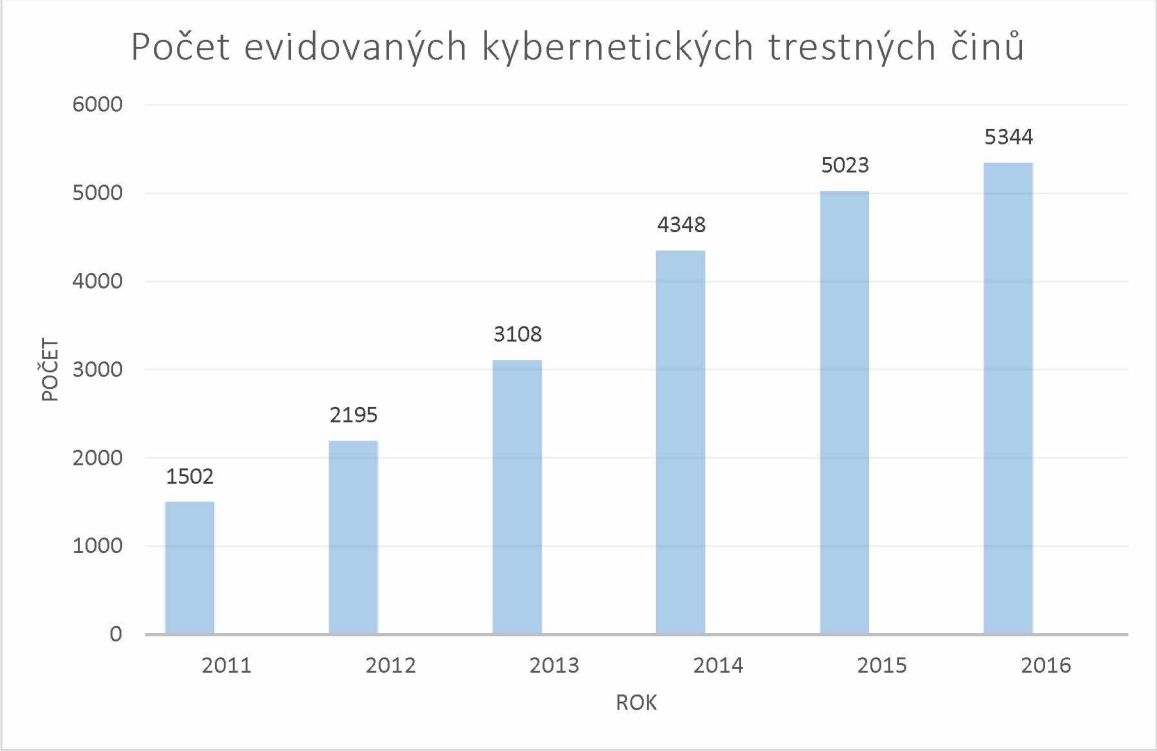
Prof. Ing. Vladimír Smejkal, CSc. pro internetové stránky www.pravniprostor.cz pojem kybernetické kriminality popisuje prakticky jako *„všechny druhy trestné činnosti, které jsou alespoň trochu sofistikovanější a jsou spáchány prostřednictvím výpočetní techniky coby věci hmotné“*. [41]

„Kybernetická kriminalita je trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti. Jako další vymezení počítačové kriminality či kybernetické kriminality lze uvést, že se jedná o zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.“ [16].

Česká technická norma říká, že *„počítačový zločin je zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený“* [42].

Nejobecněji je možné kybernetickou kriminalitu definovat jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu [20].

Policie ČR od roku 2011 sleduje počty trestných činů spáchaných v kyberprostoru. Trendem pro počet evidovaných trestných činů je jejich setrvalý nárůst, jak je patrné z přiloženého grafu č. 1.



Graf 1 – Počet evidovaných kybernetických trestných činů

zdroj: [15], vlastní zpracování

1.3 Klasifikace kyberkriminality

Obecně lze internetovou kriminalitu definovat jako takovou trestnou činnost, kde je síťové připojení nástrojem, cílem nebo místem pro spáchání trestného činu. Tato činnost zahrnuje široké spektrum potenciálně ilegálních aktivit, kdy dochází ke krádežím, podvodům, vydírání, sexuálním deliktům apod. [14].

Níže budou uvedené různé klasifikace kybernetické kriminality.

Klasifikace dle Úmluvy o kybernetické kriminalitě a dle dodatkového protokolu [20]:

a) trestné činy proti utajování, integritě a dostupnosti počítačových dat a systému,

b) trestné činy související s počítači,

c) trestné činy související s obsahem,

d) trestné činy související s porušováním autorských práv.

Další klasifikace je dle Commitee of Expert on Crime in Cyberspace [20]:

a) podle pozice počítače při páchání trestné činnosti (cíl a prostředek útoku),

b) dle typu činu (protiprávní jednání tradiční jako např. je padělání bankovek, a nová např. phishing).

Jako další lze uvést klasifikaci počítačových zločinů dle eEurope+ [20]:

a) zločiny, které porušují soukromí (např. nelegální sběr, zveřejňování a šíření osobních dat, atd.),

b) provinění, které se vztahují k obsahu v počítači (např. dětská pornografie, vyzývání k násilí, atd.),

c) ekonomické (např. hackerství, šíření virů, počítačové padělání a podvody, aj.),

d) zločiny vztahující se k duševnímu vlastnictví.

Jako poslední zde bude uvedena klasifikace dle kriminalistiky [20]:

a) neoprávněné zásahy do vstupních dat,

b) neoprávněné změny v uložených datech,

c) neoprávněné pokyny k počítačovým operacím,

d) neoprávněné pronikání do počítačů, počítačového systému a jeho databází,

e) napadení cizího počítače, programového vybavení a souborů a dat v databázích.

1.4 Jednotlivé druhy kyberkriminality

- Podvodná jednání

Jedná se o nejčastěji dokladované jednání, ke kterému se může připojit neoprávněný přístup do počítače, popř. nosiče. Patří sem např. podvodné inzeráty, e-maily, krádeže peněz z bankovních účtů pomocní phishingu nebo podvodné e-shopy, prostřednictvím kterých dochází k vylákání finančních prostředků, které jsou zpravidla vyvedeny mimo území České republiky za účelem anonymizace.

- Hacking

Je klasifikován jako neoprávněný přístup k počítačovému systému a nosiči informací, tzv. narušování dat, systému a zneužívání zařízení. Pachatel překoná zabezpečení a získá přístup k materiálům oběti. Nejčastější formou je napadání e-mailových účtů, účtů na sociálních sítích nebo účtů internetového bankovnictví. Součástí tohoto druhu trestné činnosti jsou kybernetické útoky nebo vydírání prostřednictvím ransomware[1]. Pachatelé se k citlivým údajům dostávají nejčastěji díky nezabezpečeným wi-fi připojením, zmanipulovaným e-mailovým účtům nebo napadením domácích routerů a citlivý materiál používají k vlastnímu obohacení, popř. nátlaku na oběť.

- Blagging

V tomto případě se jedná o podvody využívající sociálního inženýrství CEO - Command Executive Order. Riziku jsou vystaveny obchodní společnosti, kdy fiktivním příkazem oprávněného dochází k manipulaci k provádění požadovaných aktivit.

- Podvodné e-shopy
- Mravnostní trestné činy

Do této kategorie lze začlenit Ohrožování výchovy dítěte dle ust. § 201 trestního zákoníku, Šíření pornografie dle ust. § 191 trestního zákoníku, Výroba a jiné nakládání s dětskou pornografií dle ust. § 192 trestního zákoníku, Zneužití dítěte k výrobě pornografie dle ust. § 193 trestního zákoníku, Účast na pornografickém představení dle ust. § 193a trestního zákoníku

[1] Ransomware z angl.. ransom = výkupné. Jde o hackerskou činnost, kdy dochází k zašifrování uživatelských dat a následné vydírání uživatele k opětovnému zpřístupnění počítače.

a v neposlední řadě Navazování nedovolených kontaktů s dítětem dle ust. § 193b trestního zákoníku. V těchto případech dochází k ohrožování dětí mladších 18 let. Nejčastěji k tomuto dochází na sociálních sítích, chatech popř. v on-line hrách.

- Trestné činy proti autorskému právu
- Násilné projevy a hate crime

Do této kategorie spadají trestné činy jako např. Vydírání dle ust. § 175 trestního zákoníku, Nebezpečné vyhrožování dle ust. § 353 trestního zákoníku, Nebezpečné pronásledování (známé také pod pojmem stalking) dle ust. § 354 trestního zákoníku nebo také Šíření poplašné zprávy dle ust. § 357 trestního zákoníku. Při využití informačních technologií dochází k větší míře anonymity, která napomáhá např. k extremistickým projevům, podněcování nenávisti apod. [15].

1.5 Pojmy související s kybernetickou trestnou činností

S kybernetickou trestnou činností souvisí celá řada pojmů, některé budou vysvětleny v následujících bodech.

Kyberprostor

„Kyberprostor je prostor, který se nám otevírá ve chvíli, kdy pomocí internetových sítí vstupujeme do online prostředí.“ [26].

Zjednodušeně lze říci, že kyberprostor je virtuální realita. Jde o prostor kybernetických aktivit či prostor vytvořený informačními a komunikačními technologiemi, který tvoří virtuální svět jako paralelu k prostoru reálnému [20].

Lze říci, že kyberprostor je virtuální realitou, která nemá začátek ani konec a je zcela závislá na materiální podstatě, tedy technologiích ze světa reálného. Jeho hlavními znaky jsou decentralizovanost, globálnost, otevřenost, bohatost na informace (včetně lží a polopravd), interaktivnost a možnost ovlivňování mínění skrze uživatele [21].

Dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů je tento prostor definován: *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvoření informačními systémy, a službami a sítěmi elektronických komunikací.“* [6].

Kybernetický útok

Jako kybernetický útok lze považovat nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Kybernetický útok může být zaměřený na krádež osobních dat, spam, zpronevěru, šíření či držení dětské pornografie atd. [20].

Kybernetický útok má na postiženém dopad nejen v psychické rovině, ale významně se dotýká i fyziologického stavu oběti, kdy může ovlivňovat celkové fyzické zdraví člověka [5].

„Jedná se o jakékoliv protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Toto jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.“ definuje kybernetický útok Jan Kolouch ve své publikaci [20].

V následujících letech je pravděpodobné, že terčem kybernetických útoků se stanou nejenom počítače a smartphony, ale i další spotřební zboží např. chytrá televize či kuchyňská technika s připojením k internetu. V případě propojení techniky s osobními daty spotřebitelů může dojít k jejich zneužití [13].

Počítač (počítačový systém)

Tento pojem, ať se zdá zřejmý je vysvětlován záměrně z důvodu jeho výkladu v trestním zákoníku ve spojitosti s kybernetickou kriminalitou. Ve stručnosti, počítač je zařízení, které obsahuje centrální procesorovou jednotku, která je schopná řídit se programovým kódem a je schopná ovládat další části počítače. Dále obsahuje médium pro ukládání dat (např. disk). Mezi nepovinné části počítače se řadí zařízení pro vstup dat (klávesnice, myš, aj.), dále pak zobrazovací zařízení (monitor, projektor, aj.) [20].

Hardware

Hardware vyjadřuje souhrn hmotných technických prostředků umožňujících nebo rozšiřujících provozování počítačového systému. Jde říci, že jde o veškeré fyzické zařízení, které je třeba pro funkci systémů zpracování informací a dat [20].

Software

Software je souhrnný název pro všechny počítačové programy, které jsou používané v počítači a provádějí nějakou činnost. Zjednodušeně lze říci, že co není v počítači označováno za hardware, je software. [44].

Data a informace

Data jsou zaznamenané poznatky, fakta, čísla, události, grafy, mapy atd. Jsou základem pro informace. Data jsou uchovávána/uložena na paměťovém médiu. Informace jsou údaje/data zpracovaná do podoby užitečné pro příjemce. Ne všechna uložená data se musejí stát informacemi [20].

2 SOCIÁLNÍ SÍTĚ

Sociální sítě jsou dlouhodobě velice oblíbeným prostředkem nejenom ke komunikaci. Často sdružují jednotlivce, kteří vytvářejí různorodé, specifické skupiny, které ač by se mohly sdružovat na nejrůznějších „reálných" místech (např. školách, univerzitách apod.), tak se jim nejoblíbenějším místem stal internet. Jednou z motivací k sdružování na tomto místě je skutečnost, že tento prostor nabízí možnosti celosvětového propojení a potřebu uživatelů sdílet informace, sdružovat se, navazovat přátelství, intimní vztahy, profesionální spojenectví apod. [14].

2.1 Sociální síť

„Sociální síť je společenský prostor na internetu, který umožňuje uživatelům založit vlastní profil a komunikovat s ostatními uživateli." [38].

Především jde o internetovou službu, která lidem umožňuje vytvářet veřejné, uzavřené nebo firemní profily, prezentace, diskuzní fóra a nabízí prostor ke sdílení fotografií, videí, obsahu a dalších aktivit. Je to zařízení vyrobené z uzlů. Social Nerworking popř. Social Network Service jsou služby určené pro komunity lidí, kteří navzájem sdílejí svá data ve virtuální síti a naplňují zejména komunikační, poznávací, emoční, sociální a bezpečnostní potřeby svých uživatelů [38]. Většina obsahu na těchto sítích je tvořena jejich uživateli, ti prostřednictvím příspěvků nebo veřejnou komunikací, chatů a dalších kanálů tvoří tento obsah [25].

Dají se klasifikovat také jako místo k setkávání lidí, sdílení zážitků, obsahu atd. Očekává se zde vzájemná interakce uživatelů. Existuje mnoho typů sociálních sítí. Řada z nich vzniká na základě rodinných vazeb, kamarádů, spolužáků, pracovních kolegů, témat, jiné se zaměřují na seznámení [3]. Velice oblíbené jsou tematické skupiny, diskuzní fóra, kde si lidé vyměňují zkušenosti a názory na určitá témata [25].

Během posledních let se užívání sociálních sítí stalo nejpopulárnější aktivitou uživatelů internetu. Pokud srovnáme televizní a rozhlasové vysílání s možnostmi internetu, hlavní rozdíl je v tom, že televize a rozhlas dokáží přilákat miliony diváků a posluchačů k sledování jedné show, ale už to neumí naopak. Již neumí přinést miliony show k jednotlivcům, což internet s přehledem zvládne. Tato skutečnost nahrává individualismu, na druhou stranu může být také veliké množství nabídek pro uživatele stresující [14].

Podle Maslowovy teorie potřeb člověk potřebuje pro uspokojení těch základních, jako je potřeba přežití a bezpečí, uspokojit i potřebu úcty, uznání a seberealizace – to mu poskytuje sociální prostředí a možnost být ve spojení. S tím souvisí nadále pokračující vnitřní souboj uživatele mezi ochranou vlastního soukromí a potřebou být akceptován ostatními [14].

2.2 Historie sociálních sítí

Pojem sociální síť byl poprvé použit v roce 1954 J. A. Barnesem, kdy první sociální sítě tvořili lidé, kteří používali klasické e-maily pro podporu svých sociálních vztahů.

Počátek webových sociálních sítí se váže k roku 1978, kdy byl spuštěn provoz první skutečné sociální sítě BBS (Bulletin Board Systém). Šlo o soubor elektronických nástěnek, v grafice MS-DOS, kde si uživatelé vyměňovali informace různého charakteru. Dle A. Pavlíčka byl BBS systémem, který umožňoval přístup k systému centrálnímu, odkud bylo možné stahovat programy a hry a zároveň zanechávat zprávy ostatním uživatelům. Jednalo se o pomalý proces, vzhledem k tomu, že v jednu chvíli mohl být přihlášen jen jeden uživatel [36].

Další posun byl zaznamenán v roce 1988, kdy Jarkko Oikarinen pracující na univerzitě v Oulu vytvořil první IRC (Internet Relay Chat) aplikaci, která se jmenovala OuluBox. Tato aplikace položila základy chatovacím sítím. Oproti BBS IRC nabízela možnosti komunikovat po internetu v reálném čase [43].

Původní myšlenka se časem transformovala do potřeby sdílení multimédií, zastávala pozici nástroje k seznámení a udržování vzájemných vazeb a zároveň se tyto sítě staly prostředkem k používání jiných služeb [3].

V roce 1995 Randy Conrad vybudoval sociální síť Classmates.com, která již v té době měla hodně společného se současnou podobou těchto sítí [38]. Letecký inženýr firmy Boeing měl potřebu se spojit se svými spolužáky a na tento popud vznikla tato komunitní sociální síť, která byla vzorem pro český server „spolužáci.cz“. Rozmach sociálních sítí nastal v období takzvaného „neomezeného internetu“, který byl do té doby pro mnohé uživatele drahý a nedostupný [25].

První tzv. moderní sociální síť přišla na trh v roce 1997. Šlo o SixDegrees.com[2], kde si registrovaní uživatelé vytvářeli profily, navazovali s ostatními vazby a procházeli seznamy vazeb

[2] Název je odvozen od anglického termínu „six degrees of separation“, který v českém jazyce znamená „šest stupňů odloučení“, což je název teorie, která předpokládá, že každý člověk na planetě je v průměru spojený s každým člověkem prostřednictvím řetězce šesti navzájem známých lidí [36].

ostatních uživatelů. Tato sociální síť nově uživateli nabízela vytvářet si kvalitu a vlastní obsah. Služba disponovala v roce 2000 milionem plně registrovaných uživatelů a přes 100 zaměstnanců. Umožňovala především vytvářet si vlastní okruhy přátel, se kterými pak mohli komunikovat a prohlížet si jejich profily. Je všeobecně známo, že tato síť tzv. „předběhla svou dobu" a na přelomu století zkrachovala [43].

V roce 2002 zakládá Jonathan Abrams sociální síť Friendster.com, která měla usnadňovat navazování kontaktů mezi „přáteli přátel". Během prvního čtvrtletí provozu překonala hranici tří milionů aktivních uživatelů [43].

V následujícím období se sociální sítě stávají mainstreamovou záležitostí a vzniká mnoho dodnes populárních sítí, které míří na určitou skupinu lidí [36]. Mezi ty nejvýznamnější služby patří MySpace.com, Facebook, Twitter atd.

2.3 Sociální sítě v České republice

Před nástupem Facebooku bylo v České republice populárních několik sociálních sítí a mezi ty nejvýznamnější patřily Lidé.cz, Xchat.cz, Libimseti.cz nebo Spolužáci.cz [25]:

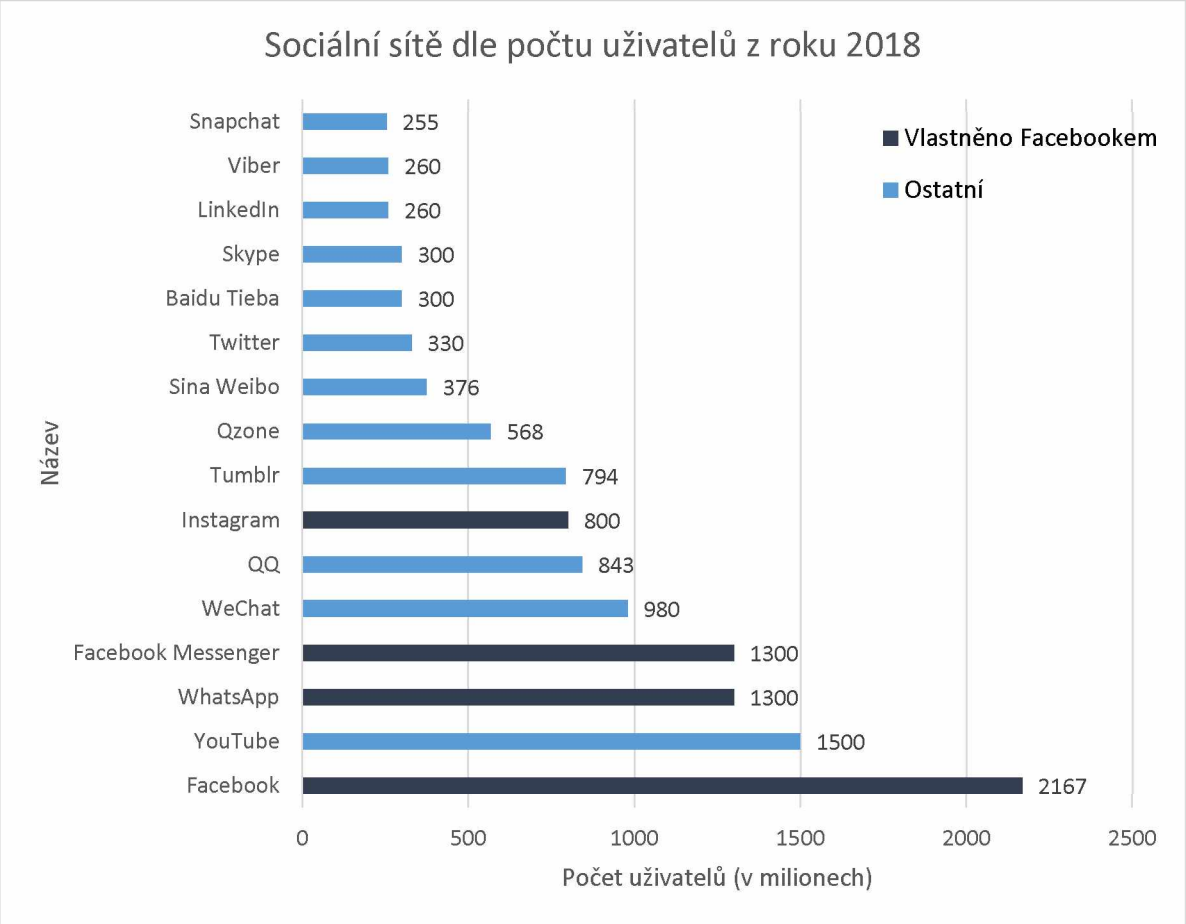
- Lidé.cz – největší česká seznamovací síť, která se po změně konceptu v roce 2014 zaměřila na uživatelské profily, diskuzní fóra a soukromé chaty,
- Spolužáci.cz – portál prioritně sloužící k setkávání současných i bývalých spolužáků v uzavřených skupinách,
- Libimseti.cz – síť nabízející profily, seznamku, chat i diskuzní fóra,
- Xchat.cz – kdysi významná sociální síť, v současné době nabízí hlavně chatovací služby,
- ČSFD.cz – největší sociální síť, která se zaměřuje na filmové fanoušky,
- Štěstí.cz – avizována jako osudová seznamka se starší uživatelskou základnou,
- Seznamka.cz – jedna z nejstarších českých služeb nabízející seznámení prostřednictvím inzerátů.

V současné době již jejich uživatelská základna nezaznamenává příliv nových uživatelů, jak tomu bylo u jejich vzniku, kdy evidovaly i několikamilionové registrace [25].

2.4 Mezinárodní sociální sítě

Na níže přiloženém grafu č. 2 lze vidět současné celosvětově neoblíbenější sociální sítě z hlediska celkového počtu uživatelů. Z grafu je jasně patrný náskok sítě Facebook, která má ohromný náskok v počtu uživatelů. Mimo to se na předních příčkách umístily i sítě patřící pod tento gigant (WhatsApp, Messenger, Instagram). Za zmínku stojí i vysoké počty uživatelů čínských sociálních sítí We Chat, Qzone a Sina Weibo. Pro potřeby práce byly vybrány nejznámější sociální sítě v České republice.

S lokalizací služeb se změnilo vnímání české společnosti mezinárodních sociálních sítí. Ty se pro české uživatele stávají atraktivními např. z důvodu možností využití intuitivních mobilních verzí s použitými novými technologiemi a trendy [25].



Graf 2 – Sociální sítě dle počtu uživatelů z roku 2018

Zdroj: [28], vlastní zpracování

2.4.1 Facebook

Jde o největší celosvětově rozšířenou sociální síť a zároveň největší webovou službu na světě. Tuto službu nyní využívá téměř 2,07 miliardy měsíčně aktivních uživatelů. V Evropě je na Facebooku registrováno přes 307 milionů lidí. Zároveň jde o sociální síť, na kterou se denně přihlašuje prostřednictvím mobilního telefonu 1,15 miliardy uživatelů. Každou vteřinu je vytvořeno 5 nových profilů. Bohužel 83 milionů profilů ze všech je fiktivních [50]. Facebook je lokalizován do více než osmdesáti jazyků včetně češtiny. Služba byla založena Markem Zuckerbergerem v roce 2004 jako studentský komunitní projekt na Harvardově univerzitě, už v dalším roce se rychle rozšířila i na ostatní univerzity v USA a zároveň i v Evropě, a postupně se otevřela i pro další po celém světě. V září roku 2006 byl tento portál spuštěný i pro veřejnost. Výhodou této sociální sítě je interakce mezi uživateli, sdílení obsahu nebo komunikační nástroje [25].

Na Facebooku si své profily zakládají převážně reální lidé. Při registraci na této stránce je nutností zadat reálný e-mail. Po registraci se uživatel dostává k základnímu kamenu sociálních sítích všeobecně, a to přidání přátel. V případě autorizace dochází k možnosti nahlížení do profilů uživatelům, kteří jsou v seznamu přátel. Hlavním prvkem sítě je tzv. Zeď, která slouží k veřejné komunikaci, sdílení stavů, poznámek, fotek, videí a odkazů s ostatními uživateli. Uživatel o sobě taktéž sdílí informace, které o sobě nepovinně vyplňuje na svém profilu. Mimo samotné uživatelské profily na Facebooku mohou být zakládány tzv. Stránky, které fungují stejným způsobem jako tyto profily s tím rozdílem, že se jedná o veřejné, popř. oficiální verze profilu. Uživatelé mají dále možnost přidat se do „Skupiny“, které jsou využívány převážně k diskuzi na určitá témata. Zajímavým prvkem je možnost vytvoření „Události“ a pozvat ostatní uživatele Facebooku na tuto akci spolu s uvedením důležitých informací o události. Součástí této funkce je zveřejnění odpovědi o účasti. Nedílnou součástí nejenom této sociální sítě je reklama. Tato reklama má unikátní možnost přesného zacílení na zákazníka a zároveň může efektivně získávat informace z různých statistik [36].

2.4.2 Instagram

Služba, která svým uživatelům umožňuje zveřejňování fotografií a videosekvencí, které mohou být upraveny grafickým filtrem. Zároveň tato síť nabízí možnost sdílení tzv. Instrastories, což jsou krátká videa a příspěvky, které po 24 hodinách ze sítě automaticky mizí. Uživatelé mají možnost zveřejnit obsah, popř. sledovat/vyhledávat příspěvky na podobné téma pomocí

„hashtagů“ [25]. Tvůrcem Instagramu je Kevin Systrom, který po studiu vysoké školy vyprojektoval službu Burbn, na kterou získal dotaci, kterou využil na vývoj sítě Instagram. Poprvé tato aplikace byla uvedena do provozu v říjnu roku 2010. První den první verzi Instagramu použilo 25 tisíc uživatelů. Po jejím spuštění počet uživatelů strmě narůstal a tento trend panuje až do současnosti. Nyní má Instagram 800 milionů aktivních uživatelů a denně ho využívá přes 500 milionů uživatelů [35].

2.4.3 Twitter

Twitter.com je webová stránka, jejíž provozovatelem je soukromá kalifornská společnost Twitter, Inc. Tyto stránky byly spuštěny v roce 2006 současným předsedou společnosti Twitter, Inc. Jackem Dorsey [36]. Jejich základ stojí na sdílení krátkých tzv. tweetů o maximální délce 140 znaků. Tweety se zobrazují na stránce uživatele, který je jejich autorem a mohou být sledovány odběrateli tzv. followers. První prototyp byl používán jako interní služba pro zaměstnance, ale ve stejný rok byl představen i veřejnosti. Tento web je populární obzvláště mezi publicisty a firmami [25].

2.4.4 LinkedIn

LinkedIn je největší internetová sociální síť zaměřená na korporátní klientelu sdružující profesionály v nejrůznějších oborech celého světa. Jedná se o profesní sociální síť, kde má uživatel možnost vložení profesního životopisu, odborných článků a dalšího obsahu. Systém je velice podobný Facebooku – lze si jednoduše přidávat kontakty do svého profilu z řad spolužáků, zaměstnanců, spolupracovníků, obchodních partnerů a vytvořit si tzv. „síť kontaktů“. Pokud poté dojde ke ztrátě zaměstnání, tato síť zůstane nedotčena [36]. Síť LinkedIn je oblíbená hlavně u personalistů, kteří přes ni vyhledávají vhodné kandidáty na pracovní pozice [25].

3 SPECIFIKACE HROZEB A RIZIK NA SOCIÁLNÍCH SÍTÍCH

Na sociálních sítích existuje obrovské množství rizik, se kterými se může uživatel setkat. Prostředí anonymity navíc nabízí prostor, ve kterém se lidé chovají dost odlišně od chování ve světě reálném. Často nemají zábrany rozebírat témata, o nichž by se běžně zdráhali nebo se styděli mluvit. Dochází k dezinhibici a často jejich jednání končí až virtuálním exhibicionizmem. Internet jim nabízí možnosti, díky kterým mohou např. oslovit více uživatelů současně popř. jim technické nedostatky umožňují získat osobní a citlivá data, která mohou být zneužita.

Zcela jednoznačně důležitým rizikem pro užívání sociálních sítí je ohromné množství přístupných dat uživatelů v celosvětovém měřítku. Jde o jednoduchý přístup k informacím a osobním údajům, které by si v běžném životě uživatel rád ponechal v soukromí. V souvislosti s bezpečností na sociálních sítích zcela jasně souvisí bezpečnost informací, a to především těch osobních. Takové informace jsou uložené v databázích, které jsou velice cenou surovinou např. pro tvorbu a šíření reklamy. Dle webu mam.ihned.cz *„Podíl reklamy na sociálních sítích na celkové internetové inzerci by se mohl tento rok zvýšit na 20 procent oproti roku loňskému, který byl na procentech 13. V roce 2016 zadavatelé utratili na sociálních sítích v Česku kolem 2,5 miliardy korun. Všeobecně reklama na sociálních sítích na vyspělých trzích každoročně vzroste o více než 20 procent. V USA v roce 2016 představovala sociální média zhruba pětinu objemu on-line reklamy.“* [37].

Další příklady nebezpečí jsou vysvětleny níže a jde o pojmy kyberšikana, kybergrooming, sexting a kyberstalking.

3.1 Kyberšikana

Jedním z vážných nebezpečí, které zneužívá internet a mobilní telefony k psychickému týrání bližních a naprosto ignoruje mravní pravidla komunikace je kyberšikana [39]. Jde o chování, které odpovídá klasické šikaně, nicméně je prováděno prostřednictvím elektronických prostředků. To může zvyšovat její nebezpečnost, protože stejně jako internet pozbývá hranic. Nejčastěji je tato forma šikany zpodobněna v úmyslném publikování nadávek, zesměšňujících informací, zveřejňování choulostivých nebo upravených fotografií či videí. Těchto útoků se může zúčastnit širší okruh agresorů, a na rozdíl od drobných urážek nebo fyzických útoků jsou viditelnější pro větší publikum [26].

Kyberšikana smazává nepoměr sil mezi agresorem a obětí prostřednictvím nabízené virtuální anonymity, kdy lidé komunikují bez ohledu na své nedostatky, a tak si lehce získávají svoji

převahu. V porovnání s šikanou klasickou je tato forma četnější, velmi často stupňující se a oběť nemá šanci ji předvídat [25]. V České republice není kyberšikana trestným činem. Takové chování ale může naplňovat skutkovou podstatu některých trestných činů např. vydírání, vyhrožování, ohrožování mravní výchovy dítěte, nebezpečné pronásledování tzv. stalking nebo útisk [39].

Samotná definice kyberšikanu specifikuje jako *„jakékoliv chování, jehož záměrem je vyvést z rovnováhy, ublížit, zastrašit nebo jinak ohrozit oběť za pomoci moderních informačních technologií (zejména pak internetu nebo mobilního telefonu). Oběť je napadána cíleně a opakovaně, a to jedincem nebo skupinou. V některých případech je kyberšikana spojena s šikanou klasickou, která zahrnuje např. fyzické útoky, slovní nadávky, pomluvy nebo ponižování. Kyberšikana zahrnuje několik forem útoku, kterými mohou být verbální útoky, ztrapňování šířením fotografie, videa nebo zvukové nahrávky, vyhrožování, zastrašováni, krádež identity, průnik na účet s cílem dehonestovat oběť, vydírání nebo i obtěžování vyzváněním.“* [25].

Jak již bylo řečeno výše, oběť na rozdíl od klasické šikany nemá možnost takové útoky, čas a jejich četnost předvídat. Útočníci až na výjimky používají k agresi fiktivní identity, čímž je posílena jejich odvaha. Pro většinu útočníků anonymní prostředí funguje jako spouštěcí faktor kyberšikany [25]. Útočníci navíc nevidí způsobené újmy a postrádají tak pocit viny.

Sociální sítě umožňují snadné a jednoduché spojení s ostatními s možností sdílení fotografií a zábavy, ovšem pokud se na nich neuplatňují bezpečnostní pravidla, mohou být zneužity ke kyberšikaně. Zároveň zde není složité vytvořit si fiktivní profil, prostřednictvím kterého může dojít k útokům [39].

Velikost internetového světa dává kyberšikaně nečekané rozměry, lidé se zde chovají méně ostražitě a sdílejí o sobě daleko více informací než ve světě reálném, a to zpravidla z toho důvodu, že nevidí reálné důsledky jejich chování. Možnosti, které zjednodušují odhalení útočníka jsou v dnešní době větší z důvodu zanechávání „virtuální stopy“. Podmínkou pro dopadení útočníka je včasné řešení a dostatek důkazů, které mohou být zálohovány. Pro vyřešení situace je třeba začít ji řešit okamžitě, kontaktovat technickou podporu příslušných služeb, nereagovat na zprávy neznámých osob, svěřit se a poprosit o pomoc popř. vytvořit zálohu důkazního materiálu a obrátit se na policii [25].

3.2 Kybergrooming

Dalším rizikem, se kterým se uživatel může na sociálních sítích setkat je tzv. kybergrooming nebo také child grooming. Jde o druh psychické manipulace probíhající v prostředí internetu,

jehož cílem je pomocí internetových komunikačních prostředků a jiných technologií vyvolat v dospělém nebo dítěti pocit důvěry a prostřednictvím falešné identity ho zneužít nebo vylákat na schůzku [25]. Důsledkem takové schůzky může být sexuální zneužití oběti, zneužití oběti pro dětskou prostituci, fyzické mučení, zneužití oběti k terorismu apod.

„Původ pojmenování kybergrooming pochází z anglického grooming nebo také allogrooming, což ve zvířecím světě označuje proces starání se či pečování jednoho člena skupiny o tělo a vzhled druhého člena. Toto chování slouží k udržování nebo posílení dobrých vzájemných vztahů nebo také k usmiřování. V lidském světě je slovo grooming synonymem milostného poměru, důvěry, rodičovské lásky a péče.“ [26].

Psychická manipulace dítěte probíhá obvykle delší dobu, od několika měsíců, po několik let. Délka manipulace je často závislá na dosažení zletilosti dítěte (existují případy, kde útočník z obavy před tvrdými tresty čekal, dokud oběť nedosáhne věkové hranice zletilosti, teprve poté došlo k osobní schůzce a sexuálnímu zneužití) [24].

Nejčastějšími obětmi kybergoomingu jsou děti ve věku 11-17 let a častěji jde o dívky. Mezi ohrožené skupiny dětí patří děti s nízkou sebeúctou nebo s nedostatkem sebedůvěry, děti s emocionálními problémy a oběti v nouzi, děti naivní a přehnaně důvěřivé, děti z bohatých rodin, po materiální stránce zabezpečené, ale citově strádající, popř. děti, hledající informace o sexu. Útočníci tvoří heterogenní skupinu, jsou to lidé s nízkým i vysokým sociálním statusem. Ve většině případů oběť útočníka zná (jde o příbuzného, známého rodiny apod.). U většiny útočníků byl diagnostikován patologický zájem o děti [24].

Tento proces manipulace s dítětem/dospělým má několik fází [25]:

- **Navázání přátelství/vzbuzení důvěry:** útočník se staví do role osoby, která dítěti rozumí a má stejné problémy nebo zájmy. Nejčastěji útočník osloví oběť na základě údajů, které má oběť uvedené na internetu. Útočníci si systematicky prohlížejí fotky či videa. Vytipují si objekt zájmu a různým způsobem jej osloví. Útočníci mají většinou několik identit, které využívají v celém procesu důvěryhodnosti profilů. Některé z nich využívají k potvrzování pravdivosti jiných, některé působí jako fiktivní přátelé. Společně mají v oběti vzbudit zájem.
- **Vytváření vztahu:** útočníci využívají různých forem motivace budoucích obětí k navázání vztahu. Nebrání se možnostem odměn k manipulaci k zaslání intimních materiálů. Většinou se jedná o nabídky velice velkorysé. Útočník vzbuzuje dojem, že mu peníze nedělají problém a často zůstává pouze u příslibu odměn.

- **Posuzování rizik:** tzv. groomer mapuje území působnosti a zjišťuje např. umístění počítače a snaží se odhadnout pravděpodobnost, že bude jeho činnost odhalena. V některých případech útočníci nepotřebují tuto otázku řešit z důvodu pocitu tzv. nedostižnosti.
- **Navázání tzv. „exkluzivního vztahu“:** nezřídka dochází k navázání virtuálního vztahu a u oběti vzniká závislost na útočníkovi. Intenzita takového vztahu mezi groomerem a dítětem se stupňuje a groomer tento vztah posiluje dojmem, že dítě samo může jejich vztah ovlivňovat a tak ho mít pod kontrolou. Tento vztah se útočník snaží posilovat vzájemnou důvěrou a připravit ho na intimnější témata.
- **Sexuální vztah:** tato fáze je přirozeným pokračováním celého hlubokého a důvěrného vztahu. Útočník oběť prostřednictvím konverzace zapojuje do kybersexu, který jen prohlubuje intenzitu vztahu.
- **Osobní setkání:** jednou z posledních fází kybergroomingu je osobní setkání, kdy dochází k napadení, obtěžování nebo zneužití dítěte.

3.3 Sexting

Jde o rizikový komunikační jev, který se v posledních letech stále častěji stává součástí zmíněné kyberšikany, kybergroomingu, kyberstalkingu či stalkingu a dalších souvisejících jevů. Zároveň se jedná o poměrně nový a rychle se rozšiřující fenomén, kterým označujeme elektronické rozesílání/šíření textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem, ke kterému dochází prostřednictvím elektronických médií [46].

Popularita tohoto chování je spojena s masovým využíváním moderních informačních technologií. Tato aktivita má dvě úrovně. Výměna podobných typů zpráv s partnerem, což je nejčastější forma sextingu popř. výměna s neznámými osobami. Obojí je svým způsobem rizikové [25].

Slovo samotné je složeninou ze slov sex a textování. První případy byly zaznamenány v roce 2005. Sexting je celosvětově zakázanou činností, vzhledem k tomu, že v jeho průběhu může docházet k šíření dětské pornografie. Sexting se taktéž často stává prostředkem pro kybergrooming [40].

Jde o jedno z nejrizikovějších chování z několika důvodů. Jedním z nich je, že po zaslání citlivých materiálů ztrácí oběť nad citlivými materiály kontrolu a tyto mohou být využívány neomezeně. Takový materiál může v prostředí internetu kolovat i několik let od svého pořízení a lze jej jen velmi obtížně z internetového prostředí odstranit [46]. Tento citlivý materiál může

být zneužit proti této osobě. Zároveň může docházet k vydírání, kyberšikaně, cílené manipulaci vydírání, popř. nátlaku [25].

3.4 Stalking/Kyberstalking – nebezpečné pronásledování nebo slídění

Stalking ve volném překladu z angličtiny znamená lov nebo pronásledování. Jde o chování, zahrnující opakované a vytrvalé pokusy o navázání nevyžádaného kontaktu či komunikace, jež u oběti vzbuzuje obavy nebo diskomfort. Toto obtěžování může mít řadu různých forem a různou intenzitu. Ve spojení s informačními technologiemi potom hovoříme o termínu kyberstalking [5]. Jedná se o opakované a stupňované obtěžování a pronásledování oběti, kterou pachatel „bombarduje" SMS zprávami, e-maily či telefonáty. Pro kyberstalkera je charakteristická vytrvalost a systematičnost. K získávání kontaktů agresoři používají promyšlené postupy a pečlivě si vybírají svoji oběť. Často také mění svou identitu v závislosti na typu oběti. Samotná definice kyberstalkingu zní: *„Kyberstalking je chování jednotlivce, skupiny nebo organizace, které využívá informační a komunikační technologie k pronásledování a obtěžování jiné osoby, skupiny či organizace. Takové chování může zahrnovat hrozby a falešná obvinění, poškození dat nebo zařízení oběti, krádež identity, odcizení dat, monitorování počítače oběti, navádění mladistvých k sexuálním praktikám a jakoukoli formu agrese. Obtěžování je myšleno ve smyslu způsobování oběti emoční stres."* [26].

Pachatel se opakovaně a dlouhodobě snaží o kontakt s obětí prostřednictvím webového rozhraní. Obsah takových zpráv může být v počátcích příjemný až veselý, stalker se snaží od oběti získat odpověď či kontakt, později může obsah zpráv přejít do urážení a zastrašování. V rámci snahy kontaktovat oběť je využívána široká paleta citů (vyhrožování, vydírání, vyvolávání pocitu viny apod.). Stalker ve svých projevech dává důraz na přímé či nepřímé výhružky, které v oběti budí oprávněný strach a obavy. Do této kategorie patří reálné pronásledování oběti. Výjimkou nejsou ani výhružky přímého násilí, výhružky zabitím apod., kterými se stalker snaží demonstrovat svoji moc a sílu. V případě elektronických médií se kyberstalker omezuje na různé druhy výhružek, které opírá o znalosti oběti. Další etapy stalkingu jsou charakteristické poškozování a ničení různých věcí oběti. Ve virtuálním světě pak jde např. o zasílání virů e-mailem a tím ztrátu dat v počítači oběti, stejně jako různé druhy invazivních technik spojených se snahou dostat se k osobním údajům oběti prostřednictvím elektronických médií. V některých případech dochází k tomu, že stalker jako útočník označuje sám sebe za oběť. V rámci stalkingu/kyberstalkingu často dochází ke snahám stalkera očernit oběť a poškodit jeho reputaci šířením nepravdivých informací v okolí oběti. Kyberstalker např. vytvoří falešnou internetovou

stránku/blog, na který píše nepravdivé informace o oběti ve snaze snížit její důvěryhodnost, reputaci apod. Tyto informace šíří synchronními a asynchronními komunikačními kanály [5].

Sklony k nebezpečnému pronásledování mají ve velké míře expartneři, osoby, jejichž city nejsou opětovány nebo lidé se zájmem o osoby známé či blízké. V jejich chování jsou známky manipulace, citového vydírání často spojené s velkým objemem zpráv a telefonátů [25].

Dle zákona se za stalkera považuje osoba, která: *„svoji oběť dlouhodobě pronásledují tím, že: a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým, b) vyhledává jeho osobní blízkost nebo jej sleduje, c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, d) omezuje jej v jeho obvyklém způsobu života, nebo e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých...“* [25].

3.5 Pornografické stránky, dětská pornografie

S vysokou mírou dostupnosti internetu a sociálních sítí se zvyšuje dostupnost pornografických stránek či portálů se sexuálním obsahem, které jsou pro vybranou věkovou skupinu krajně nevhodné. Tyto stránky návštěvníka žádným způsobem nekontrolují a co se týče zletilosti je uživatelům v tomto směru zaručována anonymita. Bohužel jsou takové stránky daleko více přístupnější nejen dospělým, ale i adolescentům.

Dostupnost pornografických stránek či portálů se sexuální tématikou je celkově nezletilým dnes mnohem více dostupná než dříve. S rozmachem komunikačních médií a aplikací se možnost produkce a distribuce pornografického materiálu po internetu rozšířila. Dítě do styku s těmito stránkami může přijít nechtěně, vzhledem k tomu, že se šíří i mezi dalšími kanály. Tento agresivní podtext na něj může mít špatný vliv a psychické důsledky. Jedinci, kteří mají zkušenost s vyšší frekvencí sexuální expozice na internetu, mají sníženou schopnost ovládat své vlastní choutky a jejich dospívání je doprovázeno emočními potížemi [47].

Pro zdravý psychický vývoj dětí je naprosto nevhodné setkat se s pornografickým materiálem. V souvislosti s touto problematikou byla mládež doposud vnímána jako jednoznačná oběť. V poslední době (zejména v USA) jsou však známy případy, kdy děti v adolescentním věku za úplatu zveřejňovaly na internetu své erotické fotografie. Pedofilní materiály se tak dostávají do nové úrovně a jejich tvůrce je obtížnější postihovat a komplikované případy právně klasifikovat. Pachatel v tomto případě splývá s obětí a v některých případech odmítá s orgány spolupracovat [26].

„Dětskou pornografii lze definovat jako jakékoli vizuální zobrazení sexuálně explicitního chování dětí a mladistvých do 18 let. Jde o jakékoliv zpodobnění dítěte účastnícího se skutečné nebo předstírané explicitní sexuální aktivity, ať už je toto zpodobnění provedeno jakýmkoli způsobem, a rovněž tak jakékoli zpodobnění sexuálních orgánů dítěte určené primárně k sexuálním účelům.“ Samotná dětská pornografie existovala již před vznikem a vývojem počítačů a internetu a v dnešní době právě internet funguje jako dokonalý pomocník pro konzumenty, šiřitele a výrobce dětské pornografie. Zároveň slouží jako prostředek pro komunikaci mezi těmito uživateli a působí jako prostředník v kontaktu s potencionální obětí [26].

Aktivně se k této problematice postavila např. firma Vodafone, která automaticky blokuje přístup svých uživatelů k nelegálnímu obsahu souvisejícím s dětskou pornografií a rasismem a zákazník nemá možnost toto nastavení zrušit [5].

3.6 Weby s jiným nevhodným obsahem

Jde především o tématiku nabádající k agresivnímu chování, chování podporující trestnou činnost, materiály s návody k sebepoškozování či sebevražednému chování. Do této skupiny dále patří stránky podporující rasismus a nenávist [26].

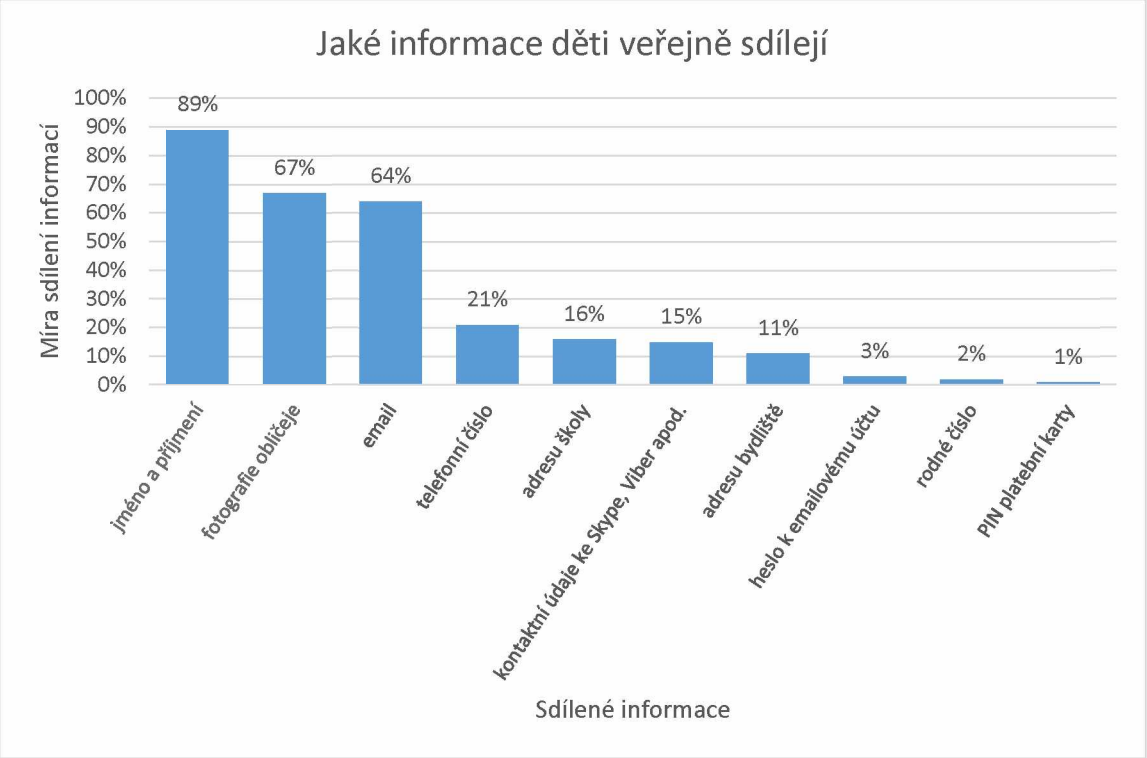
Agresivní obsah se na internetu vyskytuje především ve formě videí, popř. fotografií na různých portálech např. YouTube. Atraktivní je zejména pro chlapce, kteří taková videa mezi sebou sdílí.

Internet nabízí prostor také pro šíření, v České republice ilegálních, extremistických myšlenek. Takové stránky jsou často na první pohled nevinně vyhlížející a aktivně informují např. o historických událostech, ale fakta jsou často zkreslená a zmanipulovaná. Extremismus souvisí s komplexem méněcennosti, která je podpořena snahou dospívajícího získat sociální pozici a s ní i určitou moc. Ve skupině stejně smýšlejících uživatelů se tito vzájemně podporují, sdílejí společné názory, přejímají charakterizující znaky (vzhled, způsob oblékání, symboliku apod.). Jejich sebevědomí roste, a to často vede k šíření násilí proti určitým skupinám osob [27].

4 VÝBĚR CÍLOVÉ SKUPINY

Děti byly vždy snadnou kořistí pro pachatele jakékoliv trestné činnosti, a to hlavně pro svou důvěřivou povahu, naivitu a nezkušenost. Děti oplývají přirozenou zvídavostí a jsou dychtivé zkoušet stále nové věci. V procesu dospívání procházejí různými fázemi a často hledají náklonost mimo domov [14]. Chceme-li porozumět problematice využívání internetu dospívajícími, měli bychom porozumět motivaci adolescentů ke komunikaci ve virtuálním světě. Specifické prostředí internetu svým uživatelům nabízí prostředí bez zábran, prostředí odreagování se a zábavy, prostředí bez závazků, prostředí lží a přetvářky a pro některé prostředí štěstí [48]. Pachatelé internetové kriminality to vědí a dokáží toho využít pro vlastní prospěch.

Mezi nejzranitelnější uživatele internetu, kteří mohou být kybernetickou trestnou činností postiženi, patří adolescenti v období pubescence. Z tohoto důvodu byla pro potřeby práce zvolena věková kategorie 11-ti až 15-ti let odpovídající žákům 2. stupně základní školy. Jedním z důvodů, proč se s kyberkriminalitou setkávají nejčastěji je jejich nižší smysl pro zodpovědnost a nízká míra uvědomění si nebezpečných důsledků. V případě sociálních sítí pak velice sporadicky řeší možnosti nastavení soukromí ve svém profilu a ochranu dat všeobecně. Graf č. 3 ilustruje povahu sdílených informací na internetových stránkách. Děti se nebojí sdílet informace od telefonního čísla až po adresu bydliště.



Graf 3 – Jaké informace děti veřejně sdílejí

Zdroj: [49], vlastní zpracování

5 DOPORUČENÍ PRO MINIMALIZACI RIZIK NA SOCIÁLNÍCH SÍTÍCH

Aby bylo možné výše zmíněným rizikům předejít a maximálně zabránit kriminalitě, je nutné děti vést k bezpečnému užívání internetu a sociálních sítí. Je důležité je od prvního okamžiku vést ke zdravým návykům od časného užívání internetu, maximálně jim vysvětlit rizika a dát jim najevo, že si nemají nechat líbit věci, které jsou jim nepříjemné. Je stěžejní, aby adolescent měl kolem sebe alespoň jednu dospělou osobu, které může věřit a kdykoliv má možnost se na ní obrátit.

Současné děti a dospívající se setkávají s počítačovými médii již od nejútlejšího dětství. Již ve škole používají počítač od první, druhé třídy. Od druhého stupně základní školy získávají zkušenosti s prací s internetem, vyhledavači a e-mailem. Jejich počítačová gramotnost může být poněkud lepších kvalit než u rodičů. V rámci pochopení a zachycení rizika je potřeba angažovanost rodičů a jejich zájem o aktivity dětí na internetu. O rizicích, která internet přináší, je nutné vědět, mluvit o nich a dopředu na ně být připraven a umět je řešit. Základními negativními rysy internetového prostředí je možnost nepřirozeného úniku do světa fantazie, virtuálních lákadel a „online efekt ztráty zábran" neboli princip disinhibice na internetu. Útěk do fantazie pro uživatele přináší hodiny strávené na internetu (počítači, telefonu), ochlazování a uvadání skutečných vztahů na úkor virtuálních, zjednodušeně řečeno žití více na síti než v reálu [26].

Většina veřejných sociálních sítí obsahuje kontrolní mechanismy, které např. znemožňují přístup na sociální síť od určitého věku, případně obsahují jiné mechanismy kontroly uživatelů (např. kontrola pomocí institucionálního e-mailu). Většinu z těchto zabezpečujících mechanismů lze však snadno „obejít" např. zadat jiné datum narození. V praxi je pak běžné, že sociální sítě masově využívají i uživatelé, kteří kritéria pro přístup do dané sociální sítě nesplňují – tedy i děti [23].

5.1 Prevence

Prevence je jedním z nejdůležitějších postupů, jak předcházet různým druhům nebezpečí na internetu, popř. sociálních sítích. Jde o zásadní otázku v užívání sociálních sítí. Následná náprava škod je totiž často složitá ne-li nemožná. Stoprocentní ochrana před kybernetickou trestnou činností bohužel neexistuje, možné riziko lze pouze snížit. Osvětu v tomto směru je důležité sířit již od raného věku dítěte. Preventivně slouží např. debaty o rizicích, vytváření pravidel pro užívání médií popř. instalace vhodného softwaru. V souladu s tímto vyjadřuje Krčmářová

B. svůj názor: *„Je stokrát příjemnější a v dlouhodobém důsledku i výrazně efektivnější věnovat se prevenci, než řešení vzniklé krizové situace – uklidňování rozrušeného dítěte (po zhlédnutí agresivních či pornografických videí na internetu), návštěva psychologa, odvirování zařízení či dokonce kontaktování policie (v případě kyberšikany či kyberstalkingu).“ [26].*

Důležitou roli proti nebezpečí nejenom na sociálních sítích hraje především prevence a zvýšení informovanosti o této problematice a používání informačních a komunikačních technologií. Jde především o prostředky, které jsou dětem dnes už lehce dostupné např. mobilní telefon, tablet apod. *„Pokud budou děti seznámeny s riziky virtuální komunikace, budou mít mnohem větší šanci vyvarovat se případným chybám a zbytečně riskantnímu chování.“* [5].

Existuje shoda, že děti mladší dvou let by se konzumaci jakéhokoliv vizuálního média, tedy i internetu, měly vyvarovat úplně. Maximální doba, po kterou by se internetu měly věnovat starší děti dvou let, by denně neměla přesáhnout dvě hodiny. Takové doporučení je individuální a odvíjí se zároveň od úrovně schopností a dovedností dítěte v daném věku [26].

5.1.1 Rodič a jeho role

Jak již bylo uvedeno výše, i dospělí, a to zejména rodiče se svým způsobem nevědomě podílejí na šíření kybernetické trestné činnosti mezi mládeží, a to především nedostatečnou informovaností o rizicích, která s sebou tyto technologie přinášejí a pasivním přístupem k supervizi svých dětí. Jedním z důvodů, proč k tomu dochází, je skutečnost, že jsou mnohdy o možnostech zneužití informačně komunikačních technologií nedostatečně informováni a zároveň také o možnostech podpůrných technologií pro minimalizaci takových rizik. Svoji roli v tomto procesu hraje odlišná počítačová gramotnost mezi jednotlivými generacemi [51].

Stěžejní při vedení dialogu s dítětem je, aby bylo dítě obeznámeno s pravidly chování, které se nikterak neliší od pravidel při běžném kontaktu s ostatními lidmi v reálném životě. Rodič musí u pubescenta podporovat a posilovat pozitivní zásady a pravidla pro komunikaci s respektem a důstojností. Adolescent si musí osvojit vhodné chování na internetu a postupovat v souladu se stanovenými pravidly při používání internetu či mobilního telefonu, k tomu může rodičům sloužit např. smlouva o používání internetu v rodině. Důležité je vysvětlení, k jakým problémům může dojít, pokud je moderní technologie zneužita. Rodič je pro dítě vzorem vhodného užívání těchto technologií.

V současné době více než polovina českých dětí[3] nemá svými rodiči žádným způsobem limitovaný čas strávený na počítači a internetu. Téměř totožné množství dětí má počítač k dispozici ve svém vlastním pokoji, který nesdílí se sourozencem. *„Prevence i edukace dětí a ve zdravé míře také dohled rodičů jsou přitom nejdůležitějšími kroky, jak zabránit jejich rizikovému chování na internetu. Na 80% dětí však nemá nijak omezen přístup na nevhodné internetové stránky, i když k tomu v dnešní době existují jednoduché nástroje.“* říká Tomáš Minka, odborník ne internetovou bezpečnost O2 [5].

Jedním z možných kontrolních rodičovských preventivních přístupů je tzv. „vyrovnaná mediální dieta“ popisovaná publikací Sesame Workshop. Všeobecně lze programy a aktivity rozdělit na ty, které jsou pro dítě vhodné kdykoliv a ty, jež lze využívat/sledovat jednou za čas. Zástupcem prvních jmenovaných jsou vzdělávací programy a aplikace, k druhému patří zábavné pořady, a právě sociální sítě. [26].

O vhodnosti používaného programu či aplikace, který může rodičům pomoci v rozhodovaní je tzv. tři C přístup, kdy se k jednotlivým kritériím pro hodnocení programu váží různé klasifikační otázky. Podoba kritérií je následující [26]:

- *„Content (Obsah) – Jaká je hlavní myšlenka aplikace? Jak je aplikace designovaná? Uvádí zdroje, ze kterých vychází? Je založena na nějakém výzkumu? Je věkově vhodná? Pochází z ověřeného zdroje?*
- *Context (Souvislost) – Jak a kdo je s dítětem při konzumaci aplikace ve spojení? Mluví s ním rodiče či další osoby o tom, co se na obrazovce odehrává? Učí se dítě prostřednictvím aplikace něco, co pak může použít i v jiné aktivitě či situaci? Vypráví dítě o tom, co online sleduje a potkává?*
- *Child (dítě) – Kolik mediální stimulace může dítě dostat? Jaký typ média mu dodává nejvíce zábavy a vzbuzuje nejzvídavější otázky? Které médium mu přináší nejvíce radosti a nejvíc ho přitahuje? Co dítě ztrácí, pokud věnuje aplikaci či médiu čas?“.*

[3] 60 % (dle výzkumu „Sexting a rizikové seznamování českých dětí v kyberprostoru“ realizovaným Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci a společností O2 Czech Republic z roku 2017).

5.1.2 Programy rodičovské kontroly

Před nevhodným internetovým obsahem a nástrahami internetu lze děti účinně chránit pomocí tzv. programů rodičovské kontroly. Jednou z funkcí takových programů je možnost omezit aktivitu na používaném zařízení, popř. zaznamenávat, co se na něm děje a jaké stránky/aplikace pubescent navštěvuje [8]:

Rodičovská kontrola – freeware

Ve Windows 7 se poprvé objevila funkce „Rodičovská kontrola". S příchodem nového typu Windows 10 se proměnila na „Rodina". Oba systémy slouží k nastavení a kontrole využívání Windows dětmi. Umožňují sledovat, co děti na počítači dělají a následně lze nastavit limity k používání počítače. Program je schopný zasílat reporty, co přesně děti na internetu dělají.

Norton Online Family – freeware

Tento freeware blokuje nevhodné webové stránky a zároveň pomáhá získat přehled o zájmech dětí na internetu. Aplikace Norton Family obsahuje nástroje, které rodiče informují o aktivitách dětí a upozorní je na nebezpečné chování.

PC Screen Watcher 1.3 – freeware

Tento program umožňuje nastavit denní a týdenní limity pro uživatelem zvolené aplikace, které odpovídají určitým klíčovým slovům v názvu. V rámci tohoto programu je možné nastavit např. pravidlo pro omezení na Facebooku na 30 minut denně. Pravidla je možná vytvořit stejně tak na konkrétní klíčová slova. Aplikace dovoluje pořizovat screenshoty obrazovek a zaznamenávat stisky kláves a uložit je do protokolu nebo je odeslat e-mailem.

Verity 1.1 – shareware

Program slouží k monitorování a hlídání dětí a rodiče jejich aktivitu mohou sledovat on-line pomocí webového rozhraní. Shareware běží skrytě na pozadí systému a udržuje informace o všech navštívených internetových stránkách a spuštěných programech. V rámci programu lze mimo jiné nastavit denní limit pro použití PC, pořizovat záznamy obrazovky, ukládat informace o aktivitách, omezení vybraných funkcí a zasílání informací o aktivitě.

CYBERsitter – 10 denní trial

Funkcí tohoto programu je blokace internetu dle nastavených restrikcí a zamezit tak například dětem přístup na pochybné stránky. Poradí si i se sociálními sítěmi, omezením používání her atd. V rámci sociálních sítí zaznamenává např. rozhovory na Facebooku apod.

Eset Parental Control

Jde o aplikaci pro mobilní telefony a tablety, která rodičům nabízí seznam nejčastěji navštěvovaných domén. Její součástí je tzv. „webový strážce", který blokuje stránky/aplikace s nevhodným obsahem. Zároveň umožňuje režim sledování. Stejně jako většina výše zmíněných umožňuje nastavit maximální čas používání zařízení [9].

Google Family Link

Služba Family Link umožňuje uživateli nastavit pravidla pro užívání vybraného zařízení. Tato aplikace je kompatibilní se zařízeními podporujícími operační systém Android na kontrolovaném přístroji. Pro kompatibilní zařízení rodiče program dokáže spolupracovat se systémy Android nebo IOS. Nutností je mít vytvořený Google učet pro dítě. Rodič díky této aplikaci může spravovat aplikace, které dítě používá. Má přehled o tom, kolik času dítě na zařízení stráví a může nastavit denní limit. Má možnost vzdáleně uzamykat zařízení pubescenta tzv. funkci „večerka". Bohužel služba nenabízí blokaci nevhodného obsahu [11].

5.1.3 Projekty pro ochranu dětí

Stále více dětí se v souvislosti s riziky na internetu obrací se žádostí o pomoc na odborníky nebo neziskové organizace. Marie Mališková, CSR manažerka společnosti O2 říká: „*Na jedné straně stojí edukace, která dětem pomáhá rozlišit, co již není standardní chování. Stejně důležité ale je, aby se měly na koho obrátit, pokud se jim cokoliv závažného děje, ať v reálném světe nebo na internetu.*" [49].

Statistiky nasvědčují výše zmíněnému. Např. v roce 2008 se na Linku bezpečí obrátilo s prosbou o pomoc v souvislosti s internetem 40 dětí, v roce 2016 to bylo již o téměř 560 případů více. Nejčastěji děti řeší potíže s kyberstalkingem (24%), kyberšikanou (20%) nebo zneužitím osobních dat (6%) [49].

E-Bezpečí

Jedním z takových zajímavých projektů je server E-Bezpečí. Jedná se o „*celorepublikový projekt zaměřený na prevenci, vzdělání, výzkum, intervenci a osvětu spojenou s rizikovým chováním na internetu a souvisejícími fenomény. Projekt je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého*[4] *ve spolupráci s dalšími organizacemi.*“ Konkrétněji se projekt zaměřuje na nebezpečné internetové fenomény, které ohrožují všechny uživatele internetu, a to především na kyberšikanu a sexting, kybergrooming, kyberstalking a stalking, rizika sociálních sítí, hoax a spam a zneužití osobních údajů v prostředí elektronických médií [14].

„*Základním východiskem činnosti projektu je terénní práce s nejrůznějšími cílovými skupinami, přednášková činnost, preventivní vzdělávací akce apod. Přednášky/besedy mapují, jak konkrétní nebezpečné jevy, tak možnosti prevence a obrany proti útočníkům. Představa o problematice je vytvářena na základě modelových situací i skutečných kauz. Besedy jsou multimediální, jsou doprovázeny prezentací a videoukázkami. Kromě vzdělávacích akcí realizuje projekt E-Bezpečí také pravidelná celorepubliková výzkumná šetření, zaměřená na rizikovou komunikaci v online prostředích, provozuje také online poradnu, vydává řadu zajímavých tiskovin pro žáky/učitele a realizuje řadu dalších aktivit.*“ [14].

Saferinternet

Tento český projekt centra bezpečnějšího internetu je zaměřený na poskytování specifických služeb zejména dětem a mladým lidem s cílem propagovat vhodný obsah přístupný online. Hlavní zadání projektu je provoz platformy, který pomáhá z internetu vytvořit důvěryhodné prostředí pro děti. Saferinternet sdílí již ověřené postupy s ostatními evropskými národními centry bezpečnějšího internetu sdruženými v síti Insafe a INHOPE. Projekt nabízí horké linky – ohlašovny ilegálního obsahu (www.stoponline.cz), linky pomoci (www.pomoconline.cz) a osvětového centra (www.bezpecneonline.cz) [34].

Bezpečně-online

Tento projekt, provozovaný Národním centrem bezpečnějšího internetu díky finanční podpoře Poštovní spořitelny, je zaměřený především na děti a dospívající s cílem podporovat bezpečné

[4] Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci se zaměřuje na oblast rizikových komunikačních jevů spojených s využíváním informačních a komunikačních technologií. Své poznatky centrum implementuje do vzdělávacích, výzkumných, preventivních a intervenčních aktivit.

a sebevědomé používání internetu a nových komunikačních technologií. Hlavními kameny projektu je bezpečné používání finančních online služeb, aktivní ochrana soukromých informací před zneužitím a efektivní využívání možností informačních technologií a internetu. Vedlejším cílem je poskytnutí základní metodické podpory učitelům a žákům [33].

Linka bezpečí

Posláním Linky bezpečí je poskytovat pomoc dětem, studentům a všem, kteří jednají v jejich zájmu. Zároveň Linka bezpečí pomáhá s řešením různých náročných životních situací i každodenních starostí a problémů. Pro své klienty poskytuje krizovou intervenci a poradenství prostřednictvím telefonu, chatu a e-mailu [26].

V posledních letech registruje tento projekt nárůst počtu dětí, které se na tuto instituci obrací kvůli nebezpečí na internetu v podobě sextingu, kyberšikany, obtěžování, lákání na schůzku nebo nebezpečných výzev na internetu.

5.2 Specifikace zařízení

Rozmach internetu, komunikačních technologií (mobilní telefony, tablety apod.) a sociálních sítí, jejich masové rozšíření v posledních letech zásadně ovlivnily způsoby, jak mezi sebou současní pubescenti a mladí lidé komunikují, socializují se, a jak tráví svůj volný čas. Tato generace proto bývá často označována jako iGeneration neboli ve volném překladu jako digitální či síťová generace [4].

Tyto technologie mnohým lidem život zjednodušily, usnadnily, obohatily a poskytly tak přístup k neomezenému množství informací. Zároveň jim nabídly možnost s pomocí chytrých telefonů/smartphonů, tabletů, notebooků čerpat těchto výhod kdekoliv v dosahu internetového připojení.

Mobilní telefony (a telefony všeobecně), které v minulosti sloužily především ke komunikaci, se postupem času staly ideálním prostředkem k páchání kybernetické kriminality. Zvětšující se kvantita a diverzifikace sociálních interakcí realizovaných v kyberprostoru, zahrnující každodenní komunikaci s sebou přináší množství negativních souvislostí a důsledků. V současné době mobilní telefon slouží jako nejčastější prostředek šikanování. Většina pubescentů ve vybrané věkové kategorii disponuje vlastním telefonem a ten tak prostřednictvím sociálních sítí bývá zneužíván k nejrůznějším výše zmíněným druhům kyberkriminality. Mimo to v důsledku zdokonalování technologií může být smartphone negativně využíván k pořizování různých dehonestujícím videím a později jednoduše použit při jejich šíření.

Podle studie realizované společností Nielsen Admosphere v říjnu roku 2016 ovládají děti moderní technologie velmi dobře. Ve zkoumané věkové kategorii 6-14 let má 58% dětí smartphone a 40% z celkového počtu vlastní tablet. Z průzkumu dále plyne, že platí čím starší dítě, tím větší pravděpodobnost, že má chytrý telefon. Důležitou informací je, že internet ve svém telefonu nevyužívají pouze 4% dotazovaných dětí. Téměř tři čtvrtiny se na svém chytrém telefonu připojují k internetu pouze prostřednictvím wi-fi, 3% využívají mobilní data a o něco více než pětina využívá jak wi-fi, tak mobilní data. Nejsilnější konzumenti moderních technologií jsou právě nejstarší děti ve věku 12-14 let. Jen 2% adolescentů v tomto věku nevlastní žádné elektronické zařízení. Nejčastější činností těchto dětí na mobilních telefonech je poslech hudby (77%), hraní her (70%), pořizování fotek a videí, elektronická komunikace s kamarády a návštěva sociálních sítí (68%), a sledování videí (60%). *„Využívání mobilních zařízení k různým činnostem roste s věkem dětí. U těch, kteří mobilní telefon používají, roste nejvýrazněji jeho využití v oblasti elektronické komunikace, návštěvy sociálních sítí, vyhledávání informací ve vyhledávačích, ale také využívání k přípravě do školy, které alespoň jednou týdně deklaruje 31% dětí ve věku 12-14 let.“* [7].

Vzhledem k výše uvedenému bude práce zaměřena na chytrá mobilní zařízení.

5.3 Dohled nad činností dětí na internetu

Pro ochranu dětí před nástrahami internetu a sociálních sítí je vhodné použití aplikace pro rodičovskou kontrolu. Tyto aplikace umožňují sledovat aktivitu na internetu, blokovat nevhodný obsah, omezovat spouštění a instalaci určitých aplikací nebo například sledovat polohu zařízení.

Před samotným výběrem aplikace pro rodičovskou kontrolu je třeba si uvědomit jaké funkce bude uživatel od dohledového software očekávat. Nejprve následuje výčet možných funkcí dohledového systému s detailnějším popisem jednotlivých funkcí.

Dohled nad používáním webu

První a možná nejvíce zřejmá funkce, která je nabízená většinou aplikací rodičovské kontroly, je možnost monitorovat pohyb dětí na internetu a sledování jejich návyků při procházení internetu. Základním prvkem této funkce je monitorování či zaznamenávání procházení webových stránek, díky čemuž má rodič přehled o tom, jaké stránky jejich dítě nejčastěji navštěvuje, případně o co se na internetu zajímá. Toto může být dále rozšířeno o možnost blokování nevhodných webových stránek, případně kategorií stránek. V případě kategorií má většinou výrobce

několik kategorií, do kterých jsou webové stánky rozřazovány, např. sex, násilí, zbraně, gambling, atd. Do těchto kategorií dodavatel software zařazuje jednotlivé webové stránky a je tak pro rodiče velice snadné zablokovat přístup k určitému obsahu [19] [32] [30].

Řízení doby přístupu

Řízení doby přístupu je funkce umožňující vytvoření časového plánu, ve kterém je možné zařízení používat. Jednotlivé aplikace se pak liší tím, co vše umožnují řídit. Některé aplikace umožnují pouze blokování procházení internetu, ať už na mobilním zařízení nebo na počítači. Jiné umožňují řízení doby strávené v určité aplikaci, či hře. Další umožňují dokonce úplné odpojení internetu v závislosti na typu zařízení [19] [32] [30].

Blokování aplikací

Funkce blokování aplikací umožnuje zablokovat používání určitého typu aplikací na zařízení, podobně jako tomu je u blokování nevhodného obsahu na internetu. Funkce tak může pomoci například při pokusu o obcházení omezení přístupu např. k obsahu pro dospělé, vyhledáním aplikace, přes kterou je možné se k takovému obsahu dostat [19] [32] [30].

Monitorování sociálních sítí

Se vzestupem sociálních sítí je důležité mít přehled o pohybu dětí na tomto médiu. Tato funkce umožnuje sledovat aktivitu dítěte na sociálních sítích, nejčastěji pak aplikace podporují monitoring sociální sítě Facebook, k tomuto ovšem jsou třeba přihlašovací údaje dítěte. Aplikace jsou schopny zaznamenávat čas strávený na sociální síti, případně jaké příspěvky a fotografie potomek sdílí. Existují aplikace umožňující monitoring dalších sítí jako je např. Twitter, Snapchat a podobně [19] [32] [45] [30].

Monitorování polohy

Díky monitorování polohy má rodič přehled o tom, kde se jeho dítě či jeho mobilní telefon nachází. Většina aplikací ukládá historii pohybu. Některé aplikace umožnují vytvoření povolených oblastí, ve kterých se dítě smí vyskytovat, a dokonce i v jaký čas se zde dítě smí vyskytovat. Pokud je dítě mimo tuto určenou zónu, aplikace zašle upozornění rodiči [19] [32] [30].

Monitorování volání a SMS

Monitorování volání a SMS umožnuje rodiči kontrolovat s kým si dítě píše a volá, a u některých aplikací i obsah zpráv. Většina aplikací umožňuje kontrolu SMS zpráv pouze na zařízeních se systémem Android. Systém iOS vzhledem ke své uzavřené povaze toto neumožňuje [19] [32] [45] [30].

Vzdálená správa

Většina aplikací dnes obsahuje přístup k webovému portálu, kde má rodič možnost přehledně zobrazit aktivitu dítěte, ať už v souhrnném zobrazení, tak například detailnější statistiky navštěvovaných webových stránek, aktivitách na sociálních sítích, čas používání zařízení a jednotlivých aplikací. V neposlední řadě je zde možnost upravit jednotlivá nastavení dohledového software bez fyzického přístupu k zařízení, které si nové nastavení automaticky stáhne hned, jak bude připojeno k internetu [19] [32] [30].

Pomocí rozhodovacího procesu bude z několika variant vybrán vhodný dohledový software pro chytrá mobilní zařízení. Výběr vhodné varianty bude prováděn za pomocí softwaru Criterium Decision Plus s využitím Analyticko-hierarchického procesu.

5.3.1 Kritéria

V této kapitole budou popsána kritéria, dle kterých bude vybírán nejvhodnější dohledový software. Jako jedno z kritérií by se nabízela cena, ovšem vzhledem k tomu, že chci vybrat co nejvhodnější software z co nejširšími možnostmi ochrany, nebude cena jako kritérium použita.

Dohled nad používáním webu

Jedná se o jednu ze základních funkcí dohledového systému. Pomocí této funkce aplikace umožňuje bezpečně procházet web pomocí nástrojů, které blokují nevhodné webové stránky dle nastavených pravidel. Software většinou umožňuje filtrování dle kategorií. Kategorizaci stránek provádí výrobce software. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cíl u tohoto kritéria je maximalizace.

Řízení doby přístupu

Umožňuje sledovat dobu používání zařízení, případně dobu strávenou v jednotlivých aplikacích. Díky tomu je možné např. znemožnit používání zařízení v noci, kdy má dítě spát, a ne používat chytrá zařízení. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cíl u tohoto kritéria je maximalizace.

Blokování aplikací

Umožňuje blokovat nevhodné aplikace na zařízení. Je tak možné blokovat spouštění, případně instalaci konkrétních aplikací, případně určitých kategorií aplikací. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cíl u tohoto kritéria je maximalizace.

Monitorování sociálních sítí

Umožňuje sledování přístupu na sociální sítě, případně aktivit na sociálních sítích, jako například jaké příspěvky a obrázky uživatel sdílí. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cíl u tohoto kritéria je maximalizace.

Vzdálená správa

Aplikace umožňuje vzdálenou správu a k úpravě nastavení není třeba mít fyzický přístup k zařízení. Vzdálená správa se u různých aplikací liší komplexností nabízených funkcí a také přehledností. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cílem u tohoto kritéria je maximalizace.

Monitorování volání a SMS

Umožnění monitorování a kontrolu SMS zpráv a hovorů. Toto je vhodné v situacích, kdy má rodič podezření např. na kyberšikanu či kybergrooming. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cílem u tohoto kritéria je maximalizace.

Monitorování polohy

Aplikace má přístup k poloze zařízení a umožňuje dohled nad tím, kde se zařízení vyskytuje, případně pokud to aplikace umožňuje, také ukládání historie polohy, tedy kde se zařízení vyskytovalo. Kritérium bude hodnoceno body 1-10 dle možností nabízených funkcí. Cílem u tohoto kritéria je maximalizace.

Tabulka 1 – Kritéria pro výběr dohledového software

Označení	Kritérium	Cíl
K1	Dohled nad používáním webu	Maximalizace
K2	Řízení doby přístupu	Maximalizace
K3	Blokování aplikací	Maximalizace
K4	Monitorování sociálních sítí	Maximalizace
K5	Vzdálená správa	Maximalizace
K6	Monitorování volání a SMS	Maximalizace
K7	Monitorování polohy	Maximalizace

Zdroj: vlastní zpracování

5.3.2 Varianty

Vzhledem k tomu, že se jedná o rychle vyvíjející se oblast, nejsou knižní publikace zcela aktuální. Proto jsem důkladně prostudoval internetové zdroje.

Problematikou bezpečnosti se zabývá např. Neil J. Rubenking, vedoucí analytik pro bezpečnost pro internetový magazín PC Mag a člen poradní skupiny pro organizaci Anti-Malware Testing Standards Organization, mezinárodní neziskovou skupinu zaměřenou na koordinaci a zlepšování testování řešení proti malwaru [29]. V článku, který publikoval společně s Ben Moore, doporučuje pro rok 2018 následující dohledové systémy [30]:

- Qustodio,
- Net Nanny,
- Kaspersky Safe Kids,
- Symantec Norton Family Premier,
- Circle with Disney,
- Clean Router,
- Mobicip,
- OpenDNS home VIP,
- uKnowKids Premier,
- SafeDNS.

Web TopTenReviews testuje systémy rodičovské kontroly již 7 let. Testování věnovali přes 120 hodin a testovali 19 různých programů. Testování probíhalo na domácích zařízeních, tak aby autoři poznali chování aplikací v reálném světě. Testování probíhalo i v laboratorních podmínkách. Takto bylo možné zjistit, jak se jednotlivé aplikace používají, jak rychle aplikace upozorní na nežádoucí aktivitu atd. Výsledkem testování je doporučení následujících aplikací [18]:

- Qustodio,

- Norton Family,
- Surfie,
- Net Nanny,
- Witigo,
- SpyAgent,
- ContentBarrier,
- WebWatcher,
- Verity.

Web tom's guide, doporučuje následující aplikace [1]:

- Northon Family Premier,
- Eset Parental Control,
- Qustodio,
- Net Nany,
- My Mobile Watchdog.

Z doporučovaných variant zmiňovaných výše, jsou vyloučena řešení vyžadující dodatečný hardware jako je například Circle with Disney a Clean Router. Dále jsou vyloučena řešení umožňující pouhé filtrování webového obsahu skrze DNS jako je OpenDNS home VIP a Safe-DNS, protože chci vybrat aplikaci schopnou nejen filtrování webového obsahu, ale aplikaci s rozšířenými možnostmi rodičovské kontroly.

Dále se omezím na software od nejvýznamnějších společností v tomto segmentu, dle výzkumu provedené společností Intense Research [10].

Po prostudování zdrojů jsem se rozhodl provádět výběr nad těmito variantami:

- Qustodio,
- Net Nanny,
- Kaspersky Safe Kids,
- Symantec Norton Family Premier.

Varianta A: Qustodio

Jedná se o dohledový systém, jak s placenými variantami, tak variantou zdarma. V rámci rozhodování bude uvažována základní placená varianta umožňující instalaci (dohled) na 5 zařízeních. Aplikace umožnuje filtrovat webový obsah, monitorovat a omezovat aktivní dobu používání zařízení, včetně monitorování a omezení času stráveného v jednotlivých aplikacích, sledování polohy a v případně systému Android i monitorování volání a SMS. Co se dohledu

nad sociálními sítěmi týče, aplikace umožňuje pouze monitorování času stráveného v jednotlivých aplikacích. Jedinou výjimkou je Facebook, kde aplikace umožňuje monitorování příspěvků a vkládaných fotografií (není možné číst konverzace z Facebook Chatu). Aplikace podporuje vzdálenou správu [2].

Varianta B: Net Nanny

Placený dohledový systém umožňující v základní variantě instalaci na 5 zařízení, aplikace nabízí filtrování webového obsahu, řízení času stráveného na internetu, možnost povolovat nebo zakazovat spouštění aplikací a vzdálenou správu. Aplikace neumožnuje sledování polohy zařízení a nenabízí rozšířené možnosti sledování sociálních sítí [31].

Varianta C: Kaspersky Safe Kids

Placený dohledový systém, který nemá omezen počet zařízení, na které je možné jej nainstalovat. Aplikace umožnuje filtrování webového obsahu, řízení času stráveného na zařízení, řízení spustitelných aplikací, monitorování aktivity na soc. síti Facebook a dohled nad polohou zařízení. Zde aplikace dokonce umožňuje nadefinovat povolenou zónu pohybu zařízením (případně i čas kdy má být zařízení v této zóně), a v případě, že zařízení tuto zónu opustí, aplikace odešle notifikaci rodiči. Aplikace taktéž disponuje vzdálenou správou [19].

Varianta D: Symantec Norton Family Premier

Placený dohledový systém, který nemá omezen počet zařízení, na které je možné jej nainstalovat. Aplikace obsahuje zdařilou vzdálenou správnou. Aplikace umožnuje filtrování webového obsahu, ačkoliv filtrování HTTPS funguje pouze v podporovaných prohlížečích pomocí doplňku. Aplikace dále nabízí řízení času stráveného na zařízení, řízení spustitelných aplikací. Monitorování aktivity na soc. síti Facebook umožňuje pouze na zařízení s operačním systémem Windows. Dále aplikace umožňuje dohled nad polohou zařízení [32].

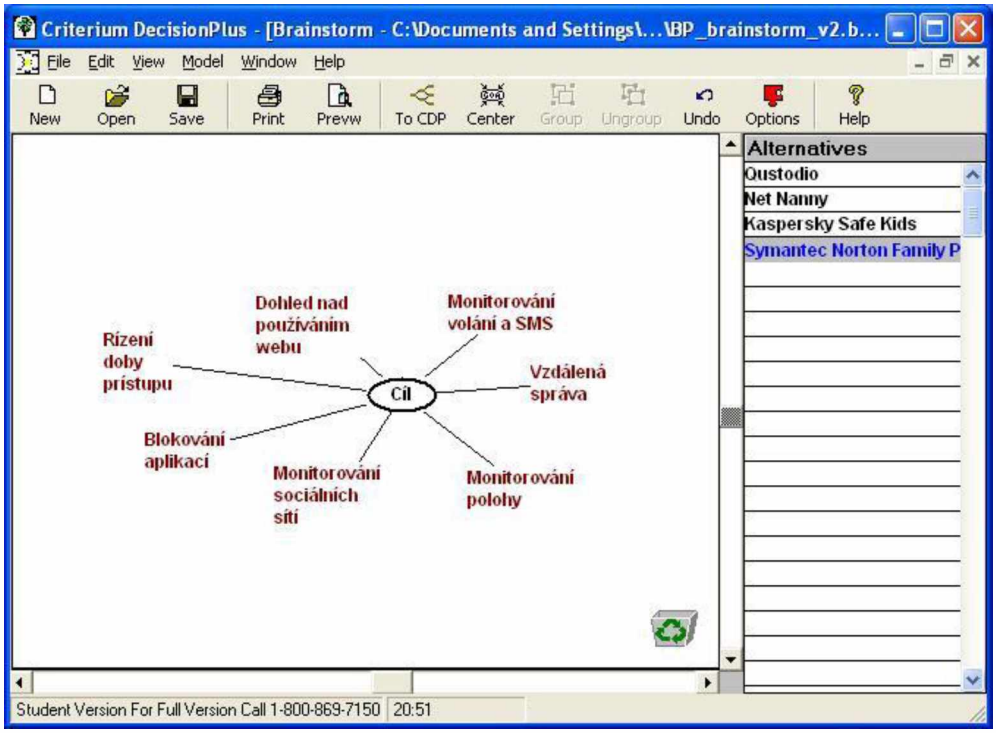
Tabulka 2 – Přehled alternativ a hodnocení kritérií

	K1	K2	K3	K4	K5	K6	K7
Varianta A	6	10	10	8	9	6	8
Varianta B	8	8	8	1	8	1	1
Varianta C	8	6	6	6	10	7	10
Varianta D	7	6	6	6	10	6	8

Zdroj: vlastní zpracování

5.3.3 Hodnocení variant pomocí CDP

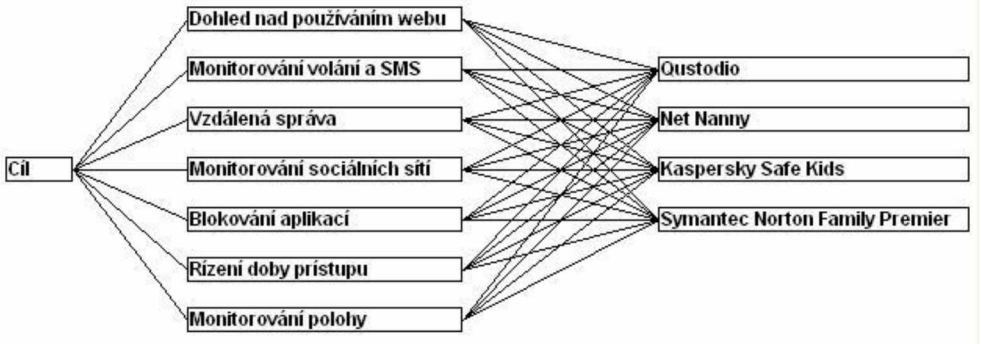
K hodnocení jednotlivých variant byl použit Analyticko-hierarchický proces v softwaru Criterum DecisionPlus. Nejprve je třeba sestavit Brainstorm, ve kterém si nastavíme jednotlivé alternativy a kritéria.



Obrázek 1 – Brainstorm v aplikaci CDP

Zdroj: vlastní zpracování

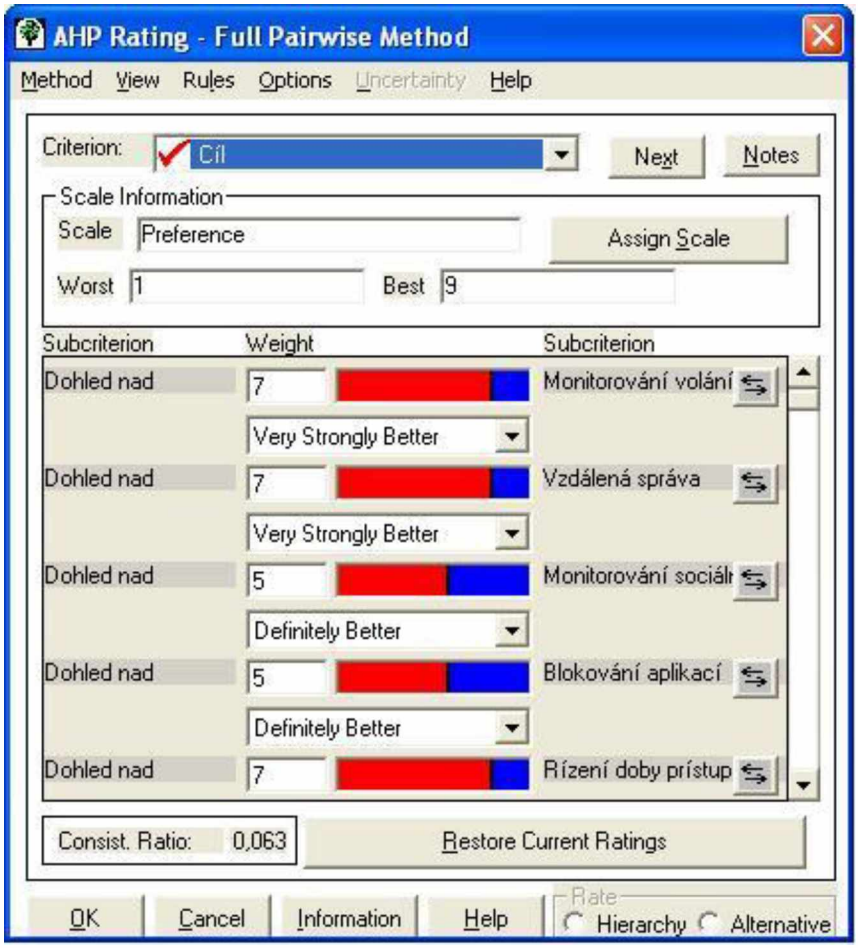
Dalším krokem je přepnutí aplikace do hierarchického modelu. Zde je třeba nastavit metodu AHP a porovnávání „Full Pairwise" tedy párové porovnání.



Obrázek 2 – Hierarchický model v aplikaci CDP

Zdroj: vlastní zpracování

Poté se nastaví vzájemné váhy jednotlivých kritérií pro každé kritérium. Nastavení jednotlivých vah je zobrazeno v tabulce č. 3. V tomto dialogovém okně se v pravém spodním rohu zobrazuje index konzistence „Consistency Ratio“. Tento index představuje „kvalitu“ sestavení párového porovnání. Na tento index je všeobecně kladen požadavek CR < 0,1, což je v tomto případě s hodnotou 0,063 splněno.



Obrázek 3 – Nastavení vah kritérií a Consist. Ratio

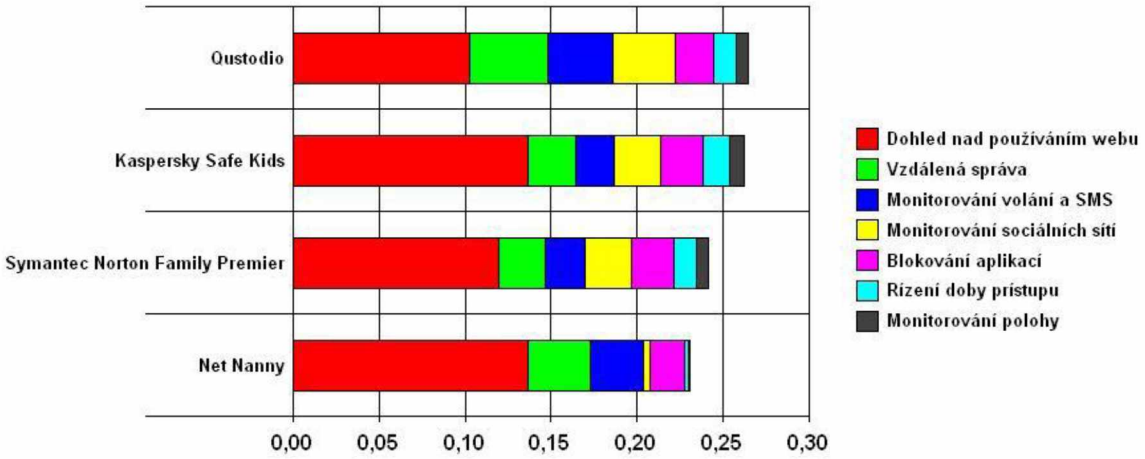
Zdroj: vlastní zpracování

Tabulka 3 – Saatyho matice kritérií

	K1	K2	K3	K4	K5	K6	K7
K1	1	7	5	5	7	7	9
K2	1/7	1	1/3	1/4	1/4	1/3	4
K3	1/5	3	1	1	1/2	1	4
K4	1/5	4	1	1	1/2	1/2	5
K5	1/7	4	2	2	1	1	7
K6	1/7	3	1	2	1	1	5
K7	1/9	1/4	1/4	1/5	1/7	1/5	1

Zdroj: vlastní zpracování

V poslední řadě se nastaví hodnoty kritérií u jednotlivých alternativ. V tuto chvíli se kliknutím na příkaz „Scores“ zobrazí výsledek procesu rozhodování, s možností přepnout náhled na graf podílu jednotlivých kritérií na variantách.



Obrázek 4 – Výsledek procesu rozhodování a podíl jednotlivých kritérií na celkovém skóre

Zdroj: vlastní zpracování

Cílem rozhodovacího procesu bylo vybrat nejvhodnější dohledový software. Do procesu rozhodovaní byly vybrány čtyři varianty se sedmi kritérii a data byla zpracována pomoci CDP. Nejvyššího skóre 0,265 dosáhl software Qustodio.

ZÁVĚR

S nástupem moderních datových a telekomunikačních sítí a internetem jako takovým se náš život stal propojenějším než kdykoliv předtím. Nezbytným vedlejším produktem této evoluce je výskyt kybernetické trestné činnosti. Má bakalářská práce přibližuje vznik kyberprostoru a vysvětluje s tím související pojmy kyberkriminality a její jednotlivé druhy. Zároveň v další podkapitole zmiňuje pojmy související s kybernetickou trestnou činností.

V další kapitole se práce věnuje sociálním sítím. Během posledních let se toto místo stalo mezi uživateli nejpopulárnější aktivitou na internetu. Bohužel v tomto prostředí existuje obrovské množství rizik, se kterými se může uživatel setkat. Těmto se práce věnuje ve třetí kapitole, kde je uveden jejich podrobný výčet.

Mezi nejohroženější skupinu, která se může dostat do kontaktu s kyberkriminalitou, patří adolescenti ve věku od 11-ti do 15-ti let. V souladu s tím byla pro potřeby práce vybrána právě tato kategorie uživatelů sociálních sítí.

V páté kapitole se práce věnuje doporučením pro minimalizaci rizik na sociálních sítích a rozebírá důležitou roli rodiče v tomto procesu. S tím souvisí možnost účinné ochrany v podobě tzv. programů pro rodičovskou kontrolu. Práce obsahuje jejich srovnání pomocí rozhodovacího procesu. Výběr vhodné varianty byl prováděn za pomocí softwaru Criterium Decision Plus s využitím Analyticko-hierarchického procesu ze čtyř variant pomocí sedmi kritérií. Nejvhodnější variantou byl vyhodnocen software Qustodio, který dosáhl nejvyššího skóre.

Celkově je z práce patrné že rizika, která se v prostředí internetu nacházejí, jsou obrovská a je potřeba s nimi být obeznámen a být na ně dostatečně připraven. Stěžejní je v tomto procesu prevence a dostatečná informovanost, které mohou taková rizika minimalizovat.

POUŽITÁ LITERATURA

[1] About Us. *Tom's Guide* [online]. [cit. 2018-06-14]. Dostupné z: https://www.tomsguide.com/us/toms-guide-who-we-are,review-4166.html

[2] Best Parental Control Software - Qustodio. *Qustodio* [online]. [cit. 2018-06-14]. Dostupné z: https://www.qustodio.com/en/

[3] Bezpečný internet | Co jsou sociální sítě. *Bezpečný internet.cz* [online]. [cit. 2018-06-24]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/co-jsou-socialni-site.aspx?kurz=true

[4] BRDIČKA, Bořivoj. Rizika spojená s technologiemi podle Rosena. *Metodický portál: inspirace a zkušenosti učitelů* [online]. 2013, 2013 [cit. 2018-04-05]. Dostupné z: https://spomocnik.rvp.cz/clanek/17161/

[5] Co je to stalking a cyberstalking. *E-Bezpečí* [online]. Olomouc, 17 Květen 2008 [cit. 2018-06-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23

[6] ČESKO. Zákon č. 181/2014 Sb.Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[7] Děti a nová média: Chytrý mobil má téměř 60 % dětí | MediaGuru. MediaGuru [online]. [cit. 2018-04-04]. Dostupné z: https://www.mediaguru.cz/clanky/2017/05/deti-a-nova-media-chytry-mobil-ma-temer-60-deti/

[8] DVOŘÁK, Jakub. Jak ochránit činnost dětí na počítači, tabletu i chytrém telefonu. *Technet.cz* [online]. 2016, 3. února 2016 [cit. 2018-05-17]. Dostupné z: https://technet.idnes.cz/ochrana-deti-na-internetu-0ye-/software.aspx?c=A160114_102132_software_dvr

[9] ESET Parental Control. *Google Play* [online]. [cit. 2018-03-20]. Dostupné z: https://play.google.com/store/apps/details?id=com.eset.parental&hl=cs

[10] Global Parental Control Software Market 2018 - Production, Sales, Supply, Demand, Cost Structure, Manufacturers, Shares, Forecast to 2023. *Intense Research* [online]. 2017, Jun-2017 [cit. 2018-06-14]. Dostupné z: http://www.intenseresearch.com/report/115777

[11] *Google Family Link – Domovská stránka* [online]. [cit. 2018-03-20]. Dostupné z: https://families.google.com/intl/cs/familylink/

[12] GRAGIDO, Will., John. PIRC a Russ. ROGERS. *Cybercrime and espionage: an analysis of subversive multivector threats*. Oxford: Elsevier Science [distributor], c2011. ISBN 1597496138.

[13] HONUS, Aleš. Kybernetické útoky brzy ohrozí nejen techniku, ale i lidské životy. *Novinky.cz* [online]. 2014, 19. září 2014 [cit. 2018-06-24]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/348190-kyberneticke-utoky-brzy-ohrozi-nejen-techniku-ale-i-lidske-zivoty.html

[14] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

[15] Jednotlivé druhy kyberkriminality. *Policie České republiky* [online]. [cit. 2018-01-15]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[16] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978–80–7251–397–0.

[17] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[18] JOHNSTON, Nicole. The Best Parental Software of 2018 - Filters, Time Management. TopTenReviews [online]. Purch, 2018, May 10, 2018 [cit. 2018-06-14]. Dostupné z: http://www.toptenreviews.com/software/privacy/best-parental-software/

[19] Kaspersky Safe Kids. *Kaspersky Lab* [online]. [cit. 2018-06-14]. Dostupné z: https://www.kaspersky.com/safe-kids

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

[21] KOLOUCH, Jan. *Kyberprostor* [online]. [cit. 2018-01-29]. Dostupné z: http://www.teorieib.cz/pbi/files/281-Kyberprostor-Kolouch.pdf

[22] KOPECKÝ, Kamil. *České děti a Facebook 2015: Výzkumná zpráva*. 1. Olomouc, [2015]. Dostupné také z: https://drive.google.com/file/d/0B5sdIAT8WtLBZWVQM1FBMTU0WWs/view

[23] KOPECKÝ, Kamil. Informace o projektu. *E-Bezpečí* [online]. [cit. 2018-03-19]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

[24] KOPECKÝ, Kamil. Nebezpečí zvané kybergrooming I. *Metodický portál: inspirace a zkušenosti učitelů* [online]. 2010 [cit. 2018-02-17]. Dostupné z: https://clanky.rvp.cz/clanek/a/9741/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/

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

[26] KRČMÁŘOVÁ, Barbora. *Děti a online rizika: sborník studií*. Praha: Sdružení Linka bezpečí, 2012. ISBN 978-80-904920-2-8.

[27] MAŠKOVÁ, Anna, Lukášová KATEŘINA, Rastislav PACÁK a Jana BRANDEJSOVÁ. *NEZÁKONNÝ A NEVHODNÝ OBSAH NA INTERNETU: Metodický materiál pro pedagogické pracovníky*. 2012. Dostupné také z: http://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=39:metodika-nezakonny-a-nevhodny-obsah-na-internetu

[28] Most famous social network sites worldwide as of April 2018, ranked by number of active users (in millions). *The Statistics Portal: Statistics and Studies from more than 22,500 Sources* [online]. [cit. 2018-04-17]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[29] Neil J. Rubenking (Author Bio). *PCMag.com* [online]. [cit. 2018-06-14]. Dostupné z: https://www.pcmag.com/author-bio/neil-j.-rubenking

[30] NEIL J., Rubenking a Ben MOORE. The Best Parental Control Software of 2018. *PCMag.com* [online]. 2019, June 6, 2018 [cit. 2018-06-14]. Dostupné z: https://www.pcmag.com/article2/0,2817,2346997,00.asp

[31] Net Nanny Family Internet Protection Pass. *Net Nanny* [online]. [cit. 2018-06-10]. Dostupné z: https://www.netnanny.com/products/family-protection-pass/

[32] *Norton Family | Oceněný software rodičovského zámku pro zařízení iPhone a zařízení se systémem Android, Windows* [online]. [cit. 2018-03-16]. Dostupné z: https://family.norton.com/web/

[33] O projektu. *Bezpečně online.cz* [online]. [cit. 2018-03-19]. Dostupné z: https://bezpecne-online.saferinternet.cz/uvod/o-projektu

[34] O projektu: Centrum bezpečnějšího internetu (SIC CZ). *Saferinternet.cz* [online]. [cit. 2018-03-19]. Dostupné z: https://www.saferinternet.cz/info-o-n%C3%A1s/o-n%C3%A1s.html

[35] Our Story. *Instagram* [online]. [cit. 2018-01-25]. Dostupné z: https://instagram-press.com/our-story/

[36] PAVLÍČEK, Antonín. *Nová média a sociální sítě*. Praha: Oeconomica, 2010. ISBN 978-80-245-1742-1.

[37] Podíl sociálních sítí na on-line reklamě vzroste na pětinu. Marketing & Media [online]. Forum Media, 2017, 24. 8. 2017 [cit. 2018-06-25]. Dostupné z: https://mam.cz/reklama/c1-65856510-podil-socialnich-siti-na-on-line-reklame-vzroste-na-petinu

[38] POSPÍŠIL, Jan a LUCIE SÁRA ZÁVODNÁ. *Mediální výchova*. Kralice na Hané: Computer Media, 2009. ISBN 9788074020223.

[39] ROGERS, Vanessa. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.

[40] *Sexting.cz - vse, co chcete vedet o sextingu* [online]. [cit. 2018-04-05]. Dostupné z: http://www.sexting.cz/

[41] SMEJKAL, Vladimír. Kybernetická kriminalita - fenomén dneška. *Právní prostor* [online]. 2015, 20.07.2015 [cit. 2018-06-25]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

[42] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

[43] Sociální sítě a jejich vývoj – pohled do historie. *Objevit.cz* [online]. 2013, 5 Březen, 2013 [cit. 2018-06-24]. Dostupné z: http://objevit.cz/socialni-site-vyvoj-pohled-do-historie-t22280

[44] Software I. *Informatika na Gymnáziu a Jazykové škole s právem státní jazykové zkoušky Zlín* [online]. [cit. 2017-10-22]. Dostupné z: http://www.gjszlin.cz/ivt/esf/ostatni-sin/software-1.php

[45] STOBING, Chris. The Best Parental Control Software and Apps of 2018. *Comparitech* [online]. [2018] [cit. 2018-06-14]. Dostupné z: https://www.comparitech.com/parental-control/

[46] SZOTKOWSKI, René a Kamil KOPECKÝ. Sexting a rizikové seznamování českých dětí v kyberprostoru 2017. Centrum PRVOK PdF UP v Olomouci, 2017. Dostupné z https://drive.google.com/file/d/0B5sdIAT8WtLBUmV5VDdZNlJyRXc/view

[47] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-.

[48] ŠMAHEL, David. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton, 2003. Psychologická setkávání. ISBN 80-7254-360-1.

[49] Téměř každé šesté dítě sdílí své intimní fotografie a videa. Nezdráhají se ani videochatů nebo osobních schůzek s cizími lidmi. *E-Bezpečí* [online]. Olomouc, 2017, 13. 6. 2017 [cit. 2018-03-19]. Dostupné z: https://www.e-bezpeci.cz/index.php/tiskove-zpravy/1246-vyzkum-sexting-2017

[50] The Top 20 Valuable Facebook Statistics – Updated January 2018. *Zephoria Inc.* [online]. 2018 [cit. 2018-01-23]. Dostupné z: https://zephoria.com/top-15-valuable-facebook-statistics/

[51] VAŠUTOVÁ, Maria. *Proměny šikany ve světě nových médií*. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5.