VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INTERNET – PROBLEMATIKA SOCIÁLNÍCH SÍTÍ

Autor práce: Martin Turek, DiS.
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2018

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

TUREK, M. *Internet – problematika sociálních sítí: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2018. 60 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: internet, sociální sítě, kyber, prevence

Bakalářská práce se zaměřuje na problematiku sociálních sítí v rámci internetu. V práci je popsán internet obecně, stručná historie jeho vzniku a vývoje a způsob použití. Dále je definován pojem sociální sítě a jsou představeny nejdůležitější představitelé konkrétních sociálních sítí postupně podle doby jejich vzniku. V další části práce jsou popsány nejzávažnější negativní a škodlivé jevy a rizika v používání sociálních sítí a prevence používaná proti nim. Na základě výsledků teoretické části a experimentu jsou navrženy další preventivní opatření model pro ideální sociální sítě.

ABSTRACT

TUREK, M. *Internet – Issues of Social Networks: Bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2018. 60 p. Supervisor: RNDr. Růžena Ferebauerová

Key words: internet, social networks, cyber, prevention

The bachelor thesis focuses on the issue of social networks within the Internet. The thesis describes the Internet in general, a brief history of its origin and development and its use. Next, the concept of social networks is defined and the most important representatives of specific social networks are gradually introduced according to the time of their creation. The next part describes the most serious negative and harmful phenomena and risks in the use of social networks and the prevention used against them. Based on the results of the theoretical part and the experiment, further preventive measures are proposed for ideal social network.

Obsah

Úvod

Jako téma bakalářské práce bylo zvoleno „Internet – problematika sociálních sítí“. Internet v posledních letech v České republice zažil takové rozšíření, že v současnosti patří do běžného života obyvatel napříč všemi sociálními vrstvami i věkovými kategoriemi. V důsledku toho se masově rozšířily i služby, které internet nabízí. Mezi takové služby se dají počítat i sociální sítě. Vedle výhod a přínosů používání internetu a sociálních sítí ovšem přináší i rizika a negativní jevy. V závislosti na aktuálnost a celospolečenskou obsažnost tohoto tématu je třeba se jím zabývat a hledat řešení pro omezení takových rizik a negativních jevů.

První část bakalářské práce se bude zabývat obecně internetem a sociálními sítěmi. Bude popsána historie internetu, jeho možnosti a budou vysvětleny základní pojmy z oblasti informačních technologií. Dále bude definován pojem „sociální sítě“, budou vyjmenovány a popsány jednotliví představitelé sociálních sítí se zaměření na ty, které jsou v současné době aktuálně nejpoužívanější v rámci České republiky i celosvětově.

Další část bakalářské práce bude zaměřena na zmapování negativních jevů, které mohou používání internetu a sociálních sítí provázet. Budou vyjmenovány a popsány jednotlivé druhy negativních jevů a rizik, ke kterým v současné době dochází, včetně konkrétních příkladů z praxe. Tyto příklady budou záměrně zvoleny takové, které již byly medializované Bude hodnocena společenská nebezpečnost těchto jevů jak z pohledu kvantity, tak i z pohledu dopadů na společnost. Současně budou představeny preventivní programy a systému, které jsou v této oblasti v České republice zřizovány a provozovány.

V závěrečné části bakalářské práce bude proveden experiment za účelem zjištění faktické úrovně zabezpečení sociálních sítí z pohledu zamezení negativním jevům, které se v jejich rámci vyskytují. Na základě zjištěních z teoretické části práce a z výsledků experimentu budou navrhnuty další způsoby prevence v oblasti negativních jevů sociálních sítí a bude vytvořen návrh ideální sociální sítě z pohledu bezpečnosti.

1 Cíl a metodika bakalářské práce

Cílem této bakalářské práce je v obecné rovině představit vznik a vývoj internetu v souvislosti se zavedením jeho využívání širokými vrstvami obyvatelstva se zaměřením na problematiku využívání sociálních sítí. V úvodní části dojde k představení samotného internetu a definování jednotlivých odborných pojmů, které jsou nezbytné pro pochopení následné problematiky. Následně budou představeny jednotlivé druhy sociálních sítí. Pomocí metody popisu a explanace budou popsány rizika a negativní dopady v používání takových sociálních sítí a budou zmapovány preventivní programy proti takovým rizikům, která jsou aktivní v současné době v České republice.

V praktické části bakalářské práci bude použita metoda experimentu v prostředí celosvětově nejrozšířenější sociální sítě Facebook pro zjištění, jaká je míra účinnosti nástrojů společnosti Facebook pro zamezování nežádoucích a rizikových jevů, a pro zjištění míry obtížnosti takové nežádoucí a rizikové situace vyvolat.

Na základě výsledků teoretické i praktické části bakalářské práce budou navrhnuty další využitelné modely prevence v oblasti negativních jevů provázející sociální sítě a internet a bude navrhnuta vzorová sociální síť, která by mohl být považována za ideální sociální síť z pohledu bezpečnosti a omezení nežádoucích jevů.

2 Internet

Pojmem internet se rozumí systém celosvětově propojených počítačů, který umožňuje jejich vzájemnou komunikaci. Samotný pojem internet je užíván obecně jako označení pro veřejně přístupnou počítačovou síť, avšak z hlediska historie a jejího vývoje se jedná o název pouze jedné z více takových sítí, které byly vyvíjeny, ale v rámci historie neuspěly.

Přestože vizionářské představy o možnosti propojení počítačů a zároveň lidí byly popisovány již mnohem dříve, pravým počátkem výzkumu síťových komunikací byl až projekt s názvem Advanced Research Projects Agency (zkráceně ARPA), jehož základ byl položen v roce 1962 ve Spojených státech amerických. Jednalo se o uzavřenou síť počítačů, která byla vytvořena pro vojenské účely. Na základech této sítě byla dne 29. října 1969 ve Spojených státech amerických spuštěna nová experimentální síť pojmenovaná ARPANET. Tuto síť tvořily počítače umístěné ve čtyř vybraných univerzitách ve Spojených státech amerických. Jednalo se o University of California Los Angeles, Stanford Research Institute, University of California Santa Barbara a University of Utah. K těmto původním čtyřem univerzitám byly postupně připojovány další významné instituce, později dokonce došlo k propojení Spojených států amerických s řadou evropských zemí. Síť ARPANET byla založena pro vojenské a vládní účely a zpočátku nebylo ani uvažováno o jejím obchodním a komerčním využití. Nákladný vývoj a provoz této sítě byl financován vládou Spojených států amerických. V roce 1971 vytvořil americký vývojář Ray Tomlinson pro síť ARPANET první e-mailový program a e-mailová komunikace také zpočátku tvořila velkou většinu celkového provozu na ARPANETu. V roce 1983 se od ARPANETu odloučila armádní síť MILNET (Military NET), čímž samotný ARPANET začal ztrácet na významu a v roce 1990 zcela zanikl. Úkoly ARPANETu převzala síť NSFNET vyvinutá Národní vědeckou nadací USA, která dodnes tvoří páteř Internetu.

V současné době internet tvoří stovky miliónů počítačů, ať už se jedná o počítače v domácnostech, firmách nebo vědeckých institucích, které jsou propojeny pomocí protokolu TCP/IP. Nejdůležitějšími službami, které internet poskytuje jsou World Wide Web (WWW) a e-mail. WWW jsou klasické pro běžné uživatele známé internetové stránky tvořené texty a grafikou, které jsou propojeny hypertextovými odkazy. E-mail slouží pro elektronickou poštu.

Abychom si dokázali představit, jak enormní je provoz na internetu. Každou minutu na internetu:

- globálně se přenesou IP data v objemu 639 800 GB,
- je staženo 47 tisíc aplikací,
- proběhne více než dva miliony vyhledávání na Googlu,
- odešle se 204 milionů e-mailů,
- 277 tisíc lidí se přihlásí na svůj účet na Facebooku,
- zobrazí se 6 milionů webových stránek,
- lidé na YouTube nahrají 30 hodin obrazového materiálu a současně je zde zhlédnuto na 1,3 milionu videí,
- na Twitteru se objeví 100 tisíc nových tweetů a současně zde přibude 320 nových uživatelů,
- na Wikipedii je publikováno šest nových článků nebo hesel,
- dojde k zaregistrování 1 300 nových mobilních telefonů.[1]

2.1 Odborná terminologie

Při práci s internetem se nemůžeme vyhnout styku a používání odborných výrazů z oboru informačních technologií, popř. ustáleným výrazům z prostředí internetové komunity. Pro proniknutí do problematiky internetu a sociálních sítí je třeba těmto výrazům rozumět a chápat je, proto si některé nejdůležitější pojmy vysvětlíme.

Jak již bylo definováno, internet je celosvětově propojená síť počítačů. Pro přístup k internetu je tedy potřeba mít nějaké zařízení. Může to být stolní počítač, notebook, tablety či mobilní telefony. V současné době se prosazuje tzv. internet věcí, protože připojení k internetu využívají i domácí spotřebiče jako chladničky, pračky či vysavače, nebo i osobní automobily.

Abychom se ze svého počítače nebo jiného zařízení k internetu dostali, potřebujeme mít připojení k internetu. Takové připojení nám umožní poskytovatel internetového připojení. To je společnost nebo organizace (používá se ustálená zkratka

[1] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. s. 52-59. ISBN 978-80-7380-501-2.

ISP z anglického Internet Service Provider), který zprostředkuje a umožní přístup k internetu. Jako ISP v České republice působí velcí telefonní operátoři jako T-Mobile, O2 nebo Vodafone, ale i další společnosti jako UPC, která poskytuje i televizní příjem, či další menší společnosti zaměřené pouze na poskytování internetového připojení, jako je např. Starnet nebo Tukanet.

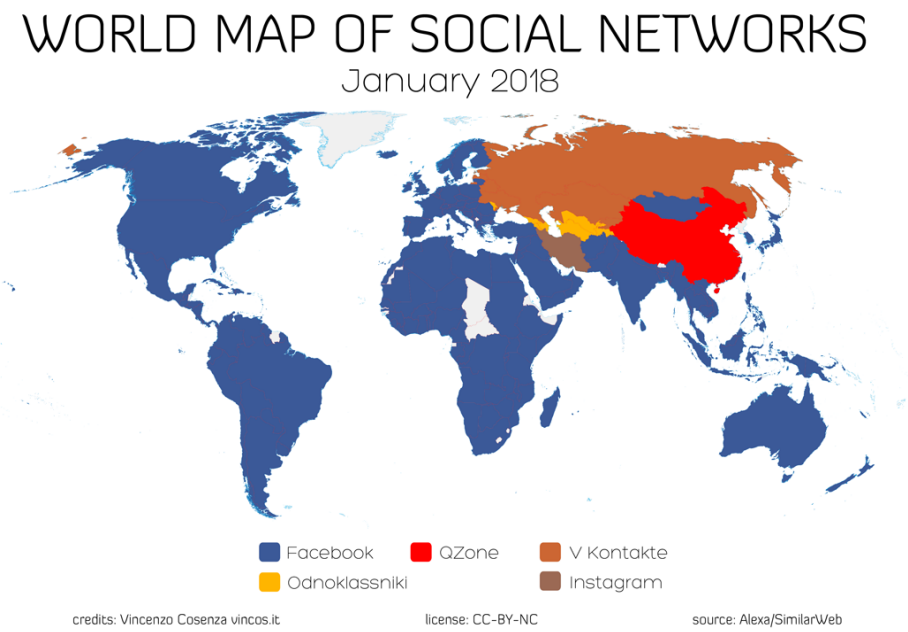
Poskytovatelé internetového připojení mohou koncovým uživatelům přístup k internetu umožnit pomocí několika druhů technologií. Buď to mohou být drátová připojení, bezdrátová připojení nebo mobilní připojení. Drátové připojení může být realizováno prostřednictvím technologie ADSL/VDSL (telefonní kabely), CATV (internet přes kabelovou televizi) nebo optické a ethernetové přípojky. Bezdrátovým připojením k internetu se rozumí v České republice nejpoužívanější technologie WiFi (z anglického Wireless Fidelity – bezdrátová věrnost). Mobilní připojení k internetu poskytují operátoři telefonních služeb a je provozováno prostřednictvím telefonních vysílačů formou GPRS, 3G nebo LTE připojení. Každé z těchto technologií, ať už drátová, bezdrátová nebo mobilní, má své výhody i nevýhody a každá z nich si najde své uplatnění.[2]

V rámci studia problematiky internetu se velmi často setkáme s předponou kyber (či anglicky cyber), např. kybersvět, kyberšikana, kyberkriminalita, apod. V tomto významu předpona kyber samotné slovo zasadí do prostředí internetu a informačních technologií.

[2] DSL.cz [online]. [cit. 1. 2. 2018]. Dostupné z: <http://www.dsl.cz/jak-na-to/jak-se-pripojit-k-internetu>

3 Sociální sítě

Sociální síť je služba v rámci internetu, která svým, zpravidla registrovaným, uživatelům umožňuje komunikovat mezi sebou buď hromadně, ve skupinách nebo soukromě a poskytují jim k tomu vhodné nástroje a podmínky. Za sociální sítě by v širším pojetí mohla být považována i internetová diskuzní fóra.



Obr. 1 – Nejoblíbenější sociální sítě podle států[3]

3.1 Historie sociálních sítí a jejich představitelé

Jaká byla úplně první sociální síť na světě se dnes již pravděpodobně nikdy nedozvíme. Nejpravděpodobněji se mohlo jednat o nějakou malou síť mezi nevýznamným množství uživatelů, která brzy po svém vzniku zanikla. A takových mohly být desítky. My si ale v následujících kapitolách představíme sociální sítě, které nezapadly a naopak se dostaly do širokého povědomí lidí, především v rámci České republiky.

[3] Nejoblíbenější sociální sítě podle států. [online]. [cit. 12. 3. 2018]. Dostupné z: <http://vincos.it/wp-content/uploads/2018/02/WMSN0118_1029.png

3.1.1 Classmates

Za jednu z prvních všeobecně známých sociálních sítí se považuje CLASSMATES. Tato sociální síť je dostupná na adrese www.classmates.com byla založena v roce 1995 v americké městě Seattle za účelem získání kontaktu na ztracené spolužáky a pro organizování školních srazů a setkání. Nejvíce registrovaných uživatelů, kolik tato služba zaznamenala, bylo 50 miliónů.

3.1.2 Friendster

Další sociální sítí, která už splňovala všechny představy, které má o sociálních sítích běžný uživatel i dnes, byla Friendster. Tato síť byla založena roku 2002 v Malajsii a jednalo se o sociální síť zaměřenou na nadšené hráče počítačových her, která svým uživatelům umožňovala vzájemně se kontaktovat, komunikovat spolu a sdílet spolu on-line obsah. Tato sociální síť byla populární převážně v jihovýchodní Asii a její počet uživatelů dosahoval 115 miliónů.

3.1.3 Myspace

V roce 2003 byla založena sociální síť Myspace, která se stala známou i pro běžné uživatele z České republiky. Tato sociální síť nabízela svým uživatelům možnost vytvořit si svoji profilovou stránku, kde mohli sdílet své fotografie, blogy, hudbu a videoklipy. Zaměření sítě bylo spíše na hudební fanoušky. V dobách své největší slávy se jednalo o nejvíce navštěvovanou internetovou stránku na světě a na Myspace bylo registrováno více než 1 miliarda založených uživatelských účtů.

3.1.4 LinkedIn

Sociální síť LinkedIn je zaměřená na propojení kontaktů mezi potencionálními zaměstnavateli a zaměstnanci. Jedná se o profesní sociální síť. LinkedIn bývá často využíván jako nástroj personalistů při náboru a vyhledávání nových zaměstnanců. To, že se jedná o celosvětově významnou sociální síť, dokládá to, že spojuje více než 546 miliónů členů z dvou set zemí a oblastí po celém světě.[4] Služba LinkedIn byla oficiálně

[4] LinkedIn.com [online]. [cit. 28. 2. 2018]. Dostupné z: <https://about.linkedin.com/cs-cz>

spuštěna 5. května 2003. V roce 2016 byla převzata společností Microsoft za částku 26,2 miliardy amerických dolarů (téměř 630 miliard korun českých).[5]

Do této sociální sítě se může registrovat každý uživatel starší 16 let a na svůj uživatelský profil vyplnit své vzdělání, schopnosti, dovednosti a dosavadní profesní zkušenosti, dále údaje o své osobě, místě svého bydliště a i své fotografie. Síť umožňuje navazovat kontakty a s dalšími uživateli a společnostmi, které hledají zaměstnance.

3.1.5 Facebook

Zlomovým se pro svět sociálních sítí stal den 4. únor roku 2004, kdy nadaný student matematické informatiky a psychologie Mark Zuckerberg ve věku 19 let založil Facebook. Facebook byla sociální síť založena na základech programu Facemash, který Zuckerberg vytvořil na Harvardské univerzitě ve Spojených státech amerických za účelem sdílení profilů studentů. Facebook funguje na principu jednotlivých uživatelských profilů a sledování svých přátel, jehož výstupy se zobrazují uživateli na tzv. zdi. Facebook bývá používán pro sdílení krátkých textů, fotogalerií, videí, pro vytváření pozvánek na události. Už v roce 2007 měl Facebook 57 miliónu aktivních uživatelů. Ke konci roku 2016 byl počet aktivních uživatelů 1,6 miliardy. Finanční hodnota společnosti Facebook byla v roce 2016 odhadována na 45 miliard amerických dolarů, což je v přepočtu zhruba 1,1 biliónu korun českých. Raketový vzestup Facebooku znamenal úplný konec nebo velký útlum většiny sociálních sítí, které do té doby existovaly, protože byly Facebookem převálcovány.

3.1.6 VKontakte

Obdobou amerického Facebooku je ruská sociální síť VKontakte. Tato síť je dostupná na adrese vk.com a je také dostupná v mnoha jazykových mutací včetně té české. Tato síť byla založena v roce 2006 v ruském Petrohradu autorem Pavlem Durovem. VKontakte následně zažil prudký vzestup způsobený dobrou marketingovou politikou vedení společnosti a také spoluprací s počítačovým gigantem Apple. O vlastnictví společnosti VKontakte nejsou v podstatě známy žádné spolehlivé informace. Informace o akcionářích jsou neveřejné, stopy o vlastnictví vedou do společností registrovaných na Britských Panenských ostrovech. Předpokládá se, že službu VKontakte pro svoje aktivity využívá i ruská tajná služba FSB (Federální služba

[5] Microsoft.com [online]. [cit. 28. 2. 2018]. Dostupné z: <https://news.microsoft.com/2016/06/13/microsoft-to-acquire-linkedin/#sm.00000b7idtbygdtjwcl1kxxr4mvby>

bezpečnosti Ruské federace), nástupce nechvalně známé KGB. VKontakte je používaná hlavně v ruskojazyčných státech. V zemích jako je Ruská federace, Ukrajina, Bělorusko, Moldavsko nebo Kazachstán je dokonce používanější než samotný Facebook. VKontakte je samozřejmě používán i ruskojazyčnými občany sídlícími v jiných zemích včetně České republiky.

3.1.7 Twitter

Jednou z mála sociální sítí, která ustála vzestup Facebooku, je Twitter. Twitter byl založen v roce 2006. Jejím základním principem je sdílení krátkých textových příspěvků v maximální délce 140 znaků, které se označují jako tweety. Tyto příspěvky mohou prohlížet uživatelé, kteří přispěvatele sledují. Twitter je používán hlavně pro sledování profilů populárních celebrit. Největší počet sledujících má zpěvačka Katy Perry, která jich k datu 24. 1. 2017 měla přesně 95.476.845. Twitter se dále často používá pro sledování zpravodajských serverů s aktuálními událostmi. Twitter byl také hlavním komunikačním kanálem pro účastníky tzv. Arabského jara v Egyptě, Tunisku a dalších arabských zemích v roce 2011. Jeho zpravodajská funkce je v současnosti velmi významná. To, že Twitter nebyl potlačen Facebookem, je právě pro své odlišné zaměření.

3.1.8 Instagram

Instagram je sociální síť založená na principu sdílení fotografií. Velký rozmach zažívá v poslední době spolu s fenoménem „selfie“, což je fotografie sebe sama, nejčastěji mobilním telefonem nebo webkamerou a následně sdílená prostřednictvím sociálních sítí.[6]

Instagram umožňuje komukoliv založit si vlastní uživatelský profil, na němž může následně sdílet své fotografie či krátká videa. Podmínkou je pouze dosažení věku 13 let. Sdílené fotografie ani jiný sdílený obsah podle podmínek použití nesmí vyobrazovat násilí, nahotu, částečnou nahotu, diskriminaci, nezákonné nebo nenávistné jednání, pornografii, sexuálně explicitní obsah a fotografie nebo obsah v rozporu se zákonem.[7]

[6] Oxford Dictionaries [online]. [cit. 28. 2. 2018]. Dostupné z: <http://en.oxforddictionaries.com/definition/selfie>
[7] Instagram.com [online]. [cit. 28. 2. 2018]. Dostupné z: <http://help.instagram.com/478745558852511>

Podle informací na webových stránkách sociální sítě Instagram sdružuje celosvětově více než 800 miliónů lidí.[8]

Instagram dále umožňuje prohlížet profily dalších uživatelů a přihlásit se k pravidelnému odběru jejich sdíleného obsahu. Instagram se stal tolik populární především proto, že ho ke své propagaci využívají mnohé celebrity, nejdříve americké, později i celebrity z dalších států i z České republiky. Cílem většinu uživatelů je získat co nejvíce sledujících svých profilů („followerů“), čehož se snaží dosáhnout zajímavostí a atraktivností svých sdílených fotografií. Proto často bývají sdíleny fotografie, ve kterých se jejich autoři snaží připodobnit ke svým oblíbeným celebritám, ukázat zajímavá místa z cestování, předvést svoji krásu a sexuální přitažlivost, případně šokovat a upoutat nebezpečím a adrenalinem při pořizování takových fotografií. Úrazy a dokonce i úmrtí při pořizování takových fotografií přímo pro sdílení na Instagramu bohužel nejsou výjimkou – pády z výšek, napadení dravými zvířaty a podobně. Uživatelům, kteří mají nejvíce followerů, Instagram přináší i bohatství, protože získávají podíl z reklamy a z propagace produktů.

3.1.9 Tinder

Tinder je moderní sociální síť, která není univerzální, ale je zaměřená a koncipovaná primárně jako seznamovací. Spuštěna byla v roce 2012. Na síti Tinder si uživatel může založit svůj profil, ve kterém je povinen vložit svou fotografii a věk, případně další nepovinné údaje. Aplikace této sociální sítě využívá geolokační údaje, takže umožňuje vyhledat další uživatele ve svém okolí podle nastavené vzdálenosti. Princip sítě funguje na ohodnocování dalších uživatelských profilů podle fotografie. V případě, kdy dojde ke shodě v pozitivním hodnocení mezi dvěma uživateli, síť jim umožní mezi sebou navázat vzájemnou soukromou komunikaci. Je všeobecně známo, že aplikace bývá nejčastěji využívána pro navazování krátkodobých sexuálních kontaktů. Riziko této sítě spočívá v anonymním setkávání cizích lidí. Za atraktivními uživatelskými profily se mohou skrývat nebezpeční agresoři. Proto by se i při používání Tinderu měly dodržovat základní zásady bezpečnosti, jako je domlouvání schůzek na veřejných místech, kde je běžný pohyb dalších osob, nesdělování většího než nezbytného množství osobních a soukromých údajů. Jako další negativní přínos této

[8] Instagram.com [online]. [cit. 28. 2. 2018]. Dostupné z: <http://www.instagram.com/about/us/>

sociální sítě bývá často zmiňována tendence nárůstu výskytu pohlavně přenosných chorob.

Sociálních sítí na stejném principu, jako je Tinder, existuje celá řada, i když nejsou tolik rozšířené. Příkladem může být Grinder určený pro homosexuální komunitu, případně Badoo. Samotný Tinder počet svých uživatelů nezveřejňuje, ale podle neověřeného sdělení Hospodářských novin z roku 2015 má celosvětově více než 50 miliónů uživatelů, přičemž tento počet stále roste.

3.1.10 Pinterest

Velmi oblíbenou sociální sítí je i Pinterest. Tato sociální síť byla spuštěna v roce 2010 americkou obchodní společností Cold Brew Labs, Inc. Podle vlastního sdělení měl Pinterest v září roku 2017 po 7 letech v provozu více než 200 miliónů uživatelů, kteří stránky Pinterestu navštěvovali minimálně jednou za měsíc.[9]

Pinterest se od ostatních sociálních sítí odlišuje tím, že je zaměřen na sdružování lidí na základě jejich společných zájmů. Umožňuje založit si uživatelský profil stejně jako ostatní sociální sítě. Dále ale umožňuje uživatelům vytvářet tzv. nástěnky, na kterých se zveřejňují tematicky sladěné fotografie či texty z různých oborů. Většinou se jedná o vaření, módu, kutilství, motorismus, cestování a mnoho dalších zájmových oblastí.

Používat se Pinterest dá různými způsoby. Uživatel se může zaměřit na sebevzdělávání, prezentaci svých zájmů, řemeslníkům či živnostníkům dává možnost sebeprezentace a marketingu.

3.1.11 Ask.fm

Ask.fm je sociální síť založená v roce 2010 Iljou Terebinem. Ask.fm pochází z Lotyšska, avšak populární se stala po celém světě, nejvíce v Itálii, Polsku, Velké Británii, Německu, Slovenské republice a České republice. Na této síti je registrováno okolo 215 miliónů lidí a je dostupná ve 49 jazykových verzích.[10] Nejoblíbenější se stala mezi dětmi ve věku mezi 13 a 18 lety.

[9] Pinterest.com [online]. [cit. 5. 3. 2018]. Dostupné z: <https://newsroom.pinterest.com/en/post/celebrating-the-200-million-people-of-pinterest>
[10] Ask.fm [online]. [cit. 6. 3. 2018]. Dostupné z: <https://about.ask.fm/about/>

Princip této sociální sítě je založen na kladení otázek a odpovídání na ně. Uživatel na svoji profilovou zeď může zadat svoji otázku nebo dotazník a ostatní uživatelé zde mohou odpovídat. Většinou to bývají otázky typu: „Co si o mně myslíš? Jak se ti líbím?“ a podobně. Nemusí se jednat o klasickou otázku, ale třeba o hodnocení fotografie, písničky nebo jiného obsahu.

Sociální síť Ask.fm byla často kritizována za to, že se stávala nástrojem kyberšikany. K několika sebevraždám dětí došlo z důvodu kyberšikany, která se děla prostřednictvím Ask.fm.

3.1.12 Snapchat

Snapchat je sociální síť založená v roce 2010 ve Spojených státech amerických autory Evanem Spiegelem, Bobby Murphym a Reggie Brownem. Ve čtvrtém čtvrtletí roku 2017 měla 187 miliónu aktivních uživatelů.[11]

Hlavní funkcí této sociální sítě je sdílení a zasílání fotografií a krátkých videí. Zajímavostí této sítě je, že odeslané a sdílené fotografie jsou ostatním dostupné pouze omezenou dobu, poté se sama smaže. Z tohoto důvodu se stal Snapchat ve velké míře nástrojem pro provozování tzv. sextingu (rozesílání sexuálně motivovaných zpráv a dalšího obsahu). Lidé získali dojem, že když se jimi odeslaná fotografie po krátké době sama smaže, tak už nemůže být dále využita a rozeslána dál. To je však velký omyl, protože žádným způsobem zneužití takových fotografií nelze zabránit, a to ani prostřednictvím služby Snapchat. Vždy existuje možnost, že si někdo fotografii na displeji vyfotografuje jiným zařízením nebo aplikací Screen Shot a dále ji zneužije nekontrolovaným způsobem. Nebezpečí tohoto jednání spočívá v tom, že se ho často dopouštějí nezletilé osoby, přestože to je proti podmínkám používání služby Snapchat, i proti zákonům jednotlivých států.

3.1.13 Spolužáci

Kdybychom chtěli nalézt sociální sítě, které jsou ryze české, došli bychom k síti Spolužáci.cz. Spolužáci.cz je komunitní server založený společností InternetPb.cz v roce 1999, od které ho zakoupila v letech 2004 – 2005 česká internetová společnost Seznam.cz, která ho dodnes spravuje a provozuje. Jednalo se o první českou sociální síť, která vešla v povědomost širšího obyvatelstva České republiky. Účel sítě je vyhledání

[11] Statista.com [online]. [cit. 6. 3. 2018]. Dostupné z: <https://www.statista.com/statistics/545967/snapchat-app-dau/>

a komunikace s bývalými i současnými spolužáky. Princip sítě je vytvoření účtu jako jednotlivého spolužáka a jeho vložení do jednotlivých tříd a škol a následná komunikace v nich s ostatními spolužáky či učiteli.

3.1.14 Lidé

Další českou sociální sítí, kterou provozuje společnost Seznam.cz, je Lidé.cz. Tato síť byla původně vytvořena a spuštěna v roce 1997 jako služba pro vyhledávání v e-mailových schránkách, ale postupně se přetvořila v sociální síť, kde každý registrovaný uživatel má svoji profilovou stránku s fotografií a s popisem a s ostatními uživateli může komunikovat buď přímo pomocí soukromých zpráv nebo veřejně prostřednictvím tematicky rozdělených diskuzních fór či chatovacích místností.

3.1.15 Líbímseti

Na obdobném principu jako Lidé.cz stojí i sociální síť Líbímseti.cz, která měla mezi českými uživateli před nástupem Facebooku značnou popularitu. Jednalo se o síť s profilovými stránkami a možností komunikace jako na Lidé.cz, avšak zde byla komunikace zaměřena již konkrétněji na seznámení.

4 Sociálně patologické jevy na internetu a sociálních sítích

Sociální patologie (z řeckého pathos – utrpení, choroba) je souhrnné označení pro nezdravé, abnormální a obecně nežádoucí společenské jevy, tzn. společensky nebezpečné, negativně sankciované formy deviantního chování, které není v souladu s morálními a právními normami společnosti.[12]

Sociálně patologické jevy byly historicky posazeny do běžného lidského života, mezilidských vztahů a fyzických projevů. Avšak vývoj internetu a sociálních sítí nám ukázal, že sociálně patologické jevy mohou existovat a fungovat i v prostředí virtuálním, tedy v prostředí internetu, a nestávají se tím o nic méně nebezpečnými nebo škodlivými, spíše naopak, protože anonymita internetu jim poskytuje účinné krytí od dohledu veřejnosti.

Takových sociálně patologických jevů je celá řada. V první řadě zahrnují kyberkriminalitu jako projev kriminálního chování, dále i další negativní jevy, který sice nemusí být trestně postižitelné, ale přesto představují hrozbu.

Podle jednoho z více druhů členění se kyberkriminalita dělí:

- kriminalita spojená s integritou informačního systému a dat,
- kriminalita spojená s obsahem (sexuální obsah, násilný obsah, obsah porušující práva duševního vlastnictví),
- kyberšikana,
- kriminalita spojená s nenávistným projevem (rasismus, xenofobie).[13]

Některé ze závažných negativních jevů spojených s používáním internetu a sociálních sítí si nyní představíme.

[12] LINHART, J., PETRUSEK, M., VODÁKOVÁ, A. *Velký sociologický slovník, svazek 2*. Praha: Karolinum, 2010. 1627s. ISBN 978-80-718-4311-5.
[13] ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. s. 15-32. ISBN 978-80-7552-758-5.

4.1 Závislost na sociálních sítích

Samotná závislost je typickým příkladem sociálně patologického jevu. Jako definici závislosti můžeme použít základní definici, která je uvedena pod souborem diagnóz F10.2 - F19.2 v 10. revizi Mezinárodní klasifikace nemocí jako Syndrom závislostí, který je definován následovně: "Je to skupina fyziologických, behaviorálních a kognitivních fenoménů, v nichž užívání nějaké látky nebo třídy látek má u daného jedince mnohem větší přednost než jednání, kterého si kdysi cenil více. Centrální popisnou charakteristikou syndromu závislosti je touha (často silná, někdy přemáhající) brát psychoaktivní látky, alkohol, nebo tabák."[14] Závislost na sociálních sítích sice nemůže splnit všechny podmínky této oficiální definice, protože v jejím případě se nejedná o aplikování žádné látky, ale v případě pochopení výrazu užívání nějaké látky jako používání sociální sítě je tato definice zcela dostačující.

Závislostí na alkoholu nebo drogách se zabývají rozsáhlé vědecké studie, existují oddělení v nemocnicích pro léčbu takových závislostí, avšak řešení závislosti na sociálních sítích je dosud spíše v pozadí, přestože se jedná o fenomén stále narůstající.

V případě, že o někom řekneme, že je závislý na sociálních sítích, je pravděpodobně závislý na sociální síti Facebook, protože ta je celosvětově a celospolečensky bezkonkurenčně nejrozšířenější a název Facebook se ve společnosti postupně stává synonymem pro sociální síť obecně. O závislosti na sociálních sítích můžeme začít mluvit v případě, že jejich nadměrné používání už ovlivňuje normální fungování člověka v běžném životě. Mohlo by se zdát, že samotné sezení u počítače nebo neustále držení mobilního telefonu či tabletu v ruce nemůže být tak škodlivé jako třeba chorobné hraní na hracích automatech, ale existují příklady, které dokazují opak. Lidé závislí na sociálních sítích či internetu jsou obecně schopni být připojeni k internetu a používat sociální síť svůj veškerý volný čas. To samozřejmě ovlivňuje jejich soukromý život, nedokáží navázat vztahy běžným způsobem, ztrácejí přátele, chybí jim rodinný život, často se mohou přidat problémy v zaměstnání nebo ve škole. Výsledek potom může být stejný jako u patologického hráče. Zatím jedinou klinikou

[14] Ústav zdravotnických informací a statistiky ČR [online]. [cit. 15. 1. 2018]. Dostupné z: <http://www.uzis.cz/zpravy/upravena-verze-mkn-10>

v České republice, která se touto problematikou zabývá, je Klinika adiktologie patřící pod 1. Lékařskou fakultu Univerzity Karlovy a Všeobecnou fakultní nemocnici v Praze.[15]

4.2 Kyberšikana

Kyberšikana je jedním ze sociálně patologických jevů, které se rozšířily spolu s rozmachem sociálních sítí. Za kyberšikanu považujeme jednání mající znaky šikany prováděné zcela či jen z části v rámci počítačové sítě, internetu nebo jiné informační technologie.

Jestliže chceme definovat, co je to kyberšikana, zároveň musíme definovat samotnou šikanu. Šikana je jakékoliv škodlivé chování, jehož cílem je ublížit jedinci nebo skupině, ohrozit nebo zastrašovat jiného jedince, případně jejich skupiny. Je to cílené a obvykle opakované užívání násilí jedincem nebo skupinou vůči jedinci nebo skupině, kteří se neumí nebo z nejrůznějších důvodů nemohou bránit. Zahrnuje jak fyzické útoky v podobě bití, vydírání, loupeží poškozování věcí druhé osobě, tak i útoky slovní v podobě nadávek, pomluv, vyhrožování či ponižování. Může mít i formu sexuálního obtěžování až zneužívání.[16] V případě kyberšikany se nejčastěji jedná o dlouhodobé urážení v prostředí internetu, jak v přímé soukromé komunikaci, tak veřejně na sociálních sítích a webových stránkách, zveřejňování zesměšňujících a dehonestujících obrázků a videí apod. V mnoha případech ovšem prvky klasické šikany bývají kombinovány i s prvky kyberšikany.[17]

Nejčastější projevy kyberšikany jsou:

a) zasílání urážlivých a zastrašujících zpráv nebo pomluv
b) pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit vybranou osobu
c) vytváření internetových stránek, které urážejí, pomlouvají nebo ponižují konkrétní osobu

[15] Klinika adiktologie 1. LF UK a VFN v Praze [online]. [cit. 15. 1. 2018]. Dostupné z: <http://www.poradna.adiktologie.cz>
[16] Národní informační centrum pro mládež [online]. [cit. 20. 2. 2018]. Dostupné z: <http://www.nicm.cz/sikana-charakteristika>
[17] HULANOVÁ, L. *Internetová kriminalita páchaná na dětec*h. Praha: Stanislav Juhaňák – Triton, 2012. s 36-51. ISBN 978-80-7387-545-9.

d) zneužívání cizího účtu – krádež identity
e) provokování a napadání uživatelů v diskuzních fórech
f) odhalování cizích tajemství
g) vydírání pomocí mobilního telefonu nebo internetu
h) obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním[18]

Základními znaky kyberšikany jsou:

1) úmyslný čin,
2) s cílem poškodit jednotlivce nebo skupinu,
3) prováděný dlouhodobě,
4) prostřednictvím počítačů, mobilních telefonů, internetu nebo dalších informačních technologií.

Kyberšikana se od „běžné“ šikany odlišuje v několika prvcích. V první řadě se jedná o vztah mezi obětí a agresorem. V případě kyberšikany oběť svého agresora vůbec nemusí znát. Buď si svou oběť vybral náhodně prostřednictvím sociálních sítí či jiných internetových služeb, aniž by jí někdy v životě osobně viděl, nebo agresor oběť zná z běžného života, ale v prostředí internetu záměrně tají svou totožnost. Dále neplatí, že oběť by musela být fyzicky slabší než agresor, protože v případě kyberšikany k přímé konfrontaci většinou nikdy nedojde a agresor je chráněn anonymitou internetu. Neplatí ani to, že by oběť musela být méně oblíbená v kolektivu nebo méně zdatnější v sociálních interakcích, protože agresor v prostředí internetu má spoustu času si své kroky rozmyslet a připravit. Zároveň v případě kyberšikany může být skupina agresorů velice široká. V případech běžné šikany je agresor jednotlivec nebo více členů kolektivu, vždy se ale bude jednat o řádově maximálně jednotky až desítky jednotlivců. V případě kyberšikany se ale pro oběť mohou stát agresory až tisíce lidí v případě, že se například sdílením rozšíří dehonestující video oběti, na kterou následně sledující dlouhodobě útočí, uráží ji zprávami, komentáři a dalším rozšiřováním videa.

Další odlišnost můžeme pozorovat v čase a místě působení šikany na oběť. S šikanou se nejčastěji můžeme setkat ve škole mezi dětmi a mládeží, méně již na pracovištích. Škola jako prostředí, kde k projevům šikany dochází, je místo uzavřené jak z hlediska místního, tak časového. Oběť je projevům šikany vystavena na určitém

[18] Policie ČR [online]. [cit. 28. 2. 2018]. Dostupné z: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>

místě a v určitém čase – v prostoru školy a v době vyučování. Po skončení vyučování odejde ze školy domů a projevům šikany se tak vyhne. V případech kyberšikany je ale situace opačná, protože její projevy na oběť působí všude, na kterémkoliv místě i v jakémkoliv čase.

Obr. 2 – Propagační materiál[19]

Nejcitovanějším příkladem kyberšikany je pravděpodobně případ čtrnáctileté Anny z Gdaňska v Polsku. Anna Halmanová se v roce 2006 stala obětí svých pěti spolužáků, kteří ji ve škole sexuálně napadli a osahávali na intimních místech. Svoje počínání si nahráli na mobilní telefon a video následně rozšířili na internetu. Anna následující den spáchala sebevraždu. Oběsila se ve svém pokoji na švihadle. Nezletilí útočníci byli soudem umístěni do ústavu pro nezletilé, avšak po třech měsících byli všichni propuštěni. Případ vyvolal velký zájem veřejnosti o kyberšikanu a stal se podnětem pro školské reformy.[20]

[19] Propagační materiál. [online]. [cit. 12. 3. 2018]. Dostupné z: <http://kybersikana.eu/2010/11/?m=1>
[20] iDnes.cz. [online]. [cit. 11. 2. 2018]. Dostupné z: <http://www.zpravy.idnes.cz/smrt-zneuctene-polske-studentky-zacal-resit-soud-fvu-/zahranicni.aspx?c=A070517_164440_zahranicni_adb>

Obětí kyberšikany se může stát úplně každý. Jak ale zabránit tomu, aby se člověk takovou obětí stal? Předně je třeba konstatovat, že riziko toho, že se člověk stane obětí kyberšikany, existuje a zcela ho odstranit nelze a stoprocentně účinný způsob, jak se jí bránit, neexistuje. Ovšem taková rizika je možné účinně snížit tím, že nebudeme agresorům sami dávat „zbraně do rukou“. Tedy sdílet na sociálních sítích jen takový obsah, který v budoucnu nebude moct být použitý proti nám, využívat všechna dostupná zabezpečení uživatelských účtů, přidávat si do přátel pouze takové uživatele, které známe a můžeme jim důvěřovat.

4.3 Sexting

Sextingem se rozumí rizikové sdílení a šíření materiálů sexuální povahy s použitím internetu či mobilních telefonů. Sexting je velmi riziková a nebezpečná činnost, která bývá často lidmi provozována bez toho, aby si dostatečně všechna rizika uvědomili a zvážili. Již samotné posílání materiálů sexuální povahy může být trestné, protože velmi častými účastníky tohoto jednání jsou děti mladší 18 let. Navíc takové materiály se mohou stát a také často stávají prostředky pro kyberšikanu. Nebezpečí spočívá i v trvalosti takových materiálů. Fotografie může být uchována a použita klidně až za několik let.

Výzkumem na populačních vzorcích v České republice bylo zjištěno, že sexting provozuje přibližně 7 - 9 % dětí ve věku od 11 do 17 let.[21] Takové jednání je ale již možné kvalifikovat jako trestný čin výroba a jiné nakládání s dětskou pornografií dle § 192 trestního zákoníku.

Řadou výzkumů bylo potvrzeno, že sexting je často vnímán jako běžná součást romantický vztahů, slouží jako nástroj pro upoutání pozornosti partnera, flirtování, vzrušení apod. Dalším důvodem pro vznik sextingu je prostá nuda. V řadě zdokumentovaných případů sexting vzniká v rámci tlaku konkrétní sociální skupiny, například spolužáků/spolužaček, partnera/partnerky. Mnoho lidí posílá svým partnerům sexuálně motivované fotografie proto, že se to od nich prostě očekává. Řada výzkumníků

[21] KOPECKÝ, K., SZOTKOWSKI, R., KREJČÍ, V. Risks of Internet Communication IV. Palacký University Olomouc: 2014. s. 98 ISBN 978-80-244-4105-4.

upozorňuje na to, že existuje souvislost mezi sextingem a požadavky současné konzumní společnosti, kdy jsou médii předkládány vzory fyzické krásy, ke kterým patří být "sexy".[22]

Že je sexting významným tématem i v České republice dokazuje případ, který se stal v roce 2009 ve Velkém Meziříčí. Patnáctiletá dívka nafotila sexuálně motivované snímky své osoby a zaslala je svému kamarádovi, aby u něj vyvolala zájem. Ten si tyto snímky nenechal pro sebe a rozeslal je dalším kamarádům. Tak se tyto snímky dostaly do ruky i učitelům z jejich základní školy, kteří celou záležitost oznámili na Policii ČR. Samotná dívka sobě způsobila velkou ostudu a možné problémy v dalším životě a její mladistvý kamarád, jehož věk nebyl upřesněn a který snímky rozeslal dál, čelil trestnímu stíhání.

4.4 Kybergrooming

Jako kybergrooming se označuje chování, kdy si pachatel na internetu vytipovává oběť, snaží se získat její důvěru, vybudovat s ní blízký vztah a vylákat ji k osobní schůzce. Cílem osobního setkání je oběť zneužít.

Do takové rizikové situace se děti a teenageři mohou dostat snadno – s cizími lidmi na internetu komunikují takřka denně. Pak stačí, aby se dítě cítilo trochu osaměle, právě přišlo o kamaráda nebo první lásku. Když nový (ale cizí) virtuální přítel správně zvolí slova a trochu zahraje na city, dítě snadno podlehne manipulaci a k osobnímu setkání svolí.

Pachatelé kybergroomingu se obvykle nejprve snaží získat osobní kontakty na svou oběť (telefonní číslo, adresu, číslo ICQ apod.). V další fázi potom zjišťují životní situaci oběti (zda žije s oběma rodiči, zda má sourozence, zda má hodně kamarádů) a na tom pak staví další komunikaci: snaží se navázat přátelský a důvěrný vztah, potom už je snadné navrhnout osobní schůzku.

[22] E-Bezpečí [online]. [cit. 16. 2. 2018]. Dostupné z: <https://www.e-bezpeci.cz/index.php/temata/sexting/923-pro-vlastne-deti-realizuji-sexting>

Pachatelé se často vydávají za někoho úplně jiného, než ve skutečnosti jsou: pokud se chtějí dostat do přízně osmileté dívky, často si hrají na stejně starou holčičku a povídají si s ní třeba o domácích mazlíčcích. U starších děvčat se jim může vyplatit vydávat se za osmnáctiletého chlapce a podobně.

Důležitým rysem komunikace je trpělivost: pachatelé si vydrží i dlouhé měsíce jen tak povídat, aby si k sobě svou oběť pevně připoutali a s jistotou získali její důvěru. Často k tomu využívají i dárky a podplácení, dítěti například posílají kredit na mobilní telefon. Součástí kybergroomingu může být i vydírání – pachatel od oběti získá např. intimní fotografie. Jakmile je má jednou v ruce, může dítě pod pohrůžkou zveřejnění nutit k čemukoliv. Třeba i k opakovanému osobnímu setkání, kde pachatel oběť zneužívá.[23]

Nejznámějším příkladem kybergroomingu v České republice je kauza Pavla Hovorky. Ten se seznamoval s nezletilými hochy na různých internetových seznamkách a vystupoval i jako sponzor dětských domovů. Své oběti lákal k sobě na vrátnici (pracoval jako ostraha), kde je pohlavně zneužíval. Při odmítání osobní schůzky své oběti vydíral pohrůžkou zveřejnění fotografií, které mu předtím chlapci sami dobrovolně poslali, či šířením zpráv o jejich údajné homosexualitě atp. Pavel Hovorka byl obviněn z trestných činů pohlavní zneužívání, vydírání, ohrožování výchovy mládeže, svádění k pohlavnímu styku a znásilnění, a nakonec odsouzen k úhrnnému trestu odnětí svobody na 6,5 let věznici s ostrahou a byla mu nařízena sexuologická léčba.[24]

Protože se kybergrooming stal rozmáhajícím se nebezpečným celospolečenským fenoménem, zákonodárci České republiky na to zareagovali a zavedli do trestního zákoníku nový trestný čin navazování nedovolených kontaktů s dítětem. Toto ustanovení nabylo účinnosti dne 1. 8. 2014 jako § 193b trestního zákoníku. Za tento trestný čin hrozí trest odnětí svobody až na dvě léta.

[23] Bezpečně online [online]. [cit. 3. 2. 2018]. Dostupné z: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybergrooming.html>
[24] NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU, 2012. *Kybergrooming a kyberstalking*. Metodický materiál pro pedagogické pracovníky. s. 1-34.

4.5 Kyberstalking

Stalkingem označujeme opakované a stupňované nebezpečné pronásledování, které může mít různé formy. V českém právním řádu je upraveno jako trestný čin pronásledování podle ustanovení § 354 trestního zákoníku. Ustanovení tohoto paragrafu zní: "Kdo jiného dlouhodobě pronásleduje tím, že vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým, vyhledává jeho osobní blízkost nebo jej sleduje, vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, omezuje jej v jeho obvyklém způsobu života, nebo zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

Pojem kyberstalking spadá pod tuto definici stalkingu pouze s omezením na použití prostředků elektronické komunikace a internetu. Mezi znaky kyberstalingu patří to, že se pachatel dlouhodobě pokouší kontaktovat svou oběť přes sms zprávy, e-maily, telefonáty, pomocí zpráv na chatech, Skype, Facebook a dalších sociálních sítích. Charakter kontaktování může být zpočátku příjemný, obdivný a pozorný, pachatel si získává o oběti informace (kde žije, s kým, co má ráda). Pokud oběť nereaguje na kontakt dle představ pachatele, dochází k intenzivnějšímu kontaktování s prvky agrese, urážek, zastrašování či nevkusných komentářů. Pachatel vyvolává v oběti pocity viny, vydírá ji a vyhrožuje. Stalker dává oběti najevo svou sílu a moc skrze výhrůžky, ať přímé či nepřímé, které vyvolávají v oběti strach. Většinou oběti vyhrožuje tím, co o ní v předešlé, dosud ještě nezávadné, komunikaci zjistil, například tím, že ví, kde bydlí, kde pracuje apod. Další fází kyberstalkingu může být například posílání virů e-mailovou poštou, elektronické nabourávání do osobních údajů, rozšiřování nepravdivých údajů o oběti na internetu a sociálních sítí za účelem jejího poškození před rodinou, přáteli či zaměstnavatelem.[25]

[25] Centrum pro oběti domácího a sexuálního násilí [online]. [cit. 1. 3. 2018]. Dostupné z: <http://www.profem.cz/clanek.aspx?a=97>

4.6 Krádež identity

S krádeží identity se setkáváme již od nepaměti. V současné době se změnila pouze její podoba. Místo fyzického vydávání se za jinou osobu, ať již na základě ukradených listin, či pouhým zevnějškem, jsme dnes uváděni v omyl na základě počítačové masky. Oběťmi mohou být bankovní ústavy, velké nadnárodní korporace, známé osobnosti, ale i prostí občané. Kdo dnes ztratí svoji počítačovou masku, ztrácí svou elektronickou tvář.

Z pohledu práva je krádež identity považována za dvoustupňový trestný čin. Pachatel musí nejprve získat cizí počítačovou identitu. Děje se tak nejčastěji odcizením elektronických dat (hesla, přístupové údaje atd.), a to zpravidla neoprávněným kopírováním dat (skimming), lstivým vylákáním údajů (phishing) či nedovoleným vniknutím do cizího počítače (hacking). Jedná se o tzv. identity theft. V druhé fázi pachatel zneužije neoprávněně nabytou identitu. Cílem bývá většinou majetkový prospěch, tzv. identity fraud. Z právního hlediska se jedná o klasický podvod a judikatura v tomto směru přizpůsobuje výklad novým informačním technologiím. V dalších případech může být cílem pouhé poškození oběti, např. tím, že bude pod jejím jménem vystupovat na sociálních sítích typu Facebook, a může se dopustit např. trestného činu poškozování cizích práv.[26]

V trestním zákoníku č. 40/2009 Sb. je definována řada trestných činů, které se týkají výše uvedeného jednání:

- neoprávněný přístup k počítačovému systému a nosiči informací - § 230 trestního zákoníku
- porušení tajemství dopravovaných zpráv - § 182 trestního zákoníku
- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat - § 231 trestního zákoníku
- poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti - § 232 trestního zákoníku

[26] Bezpečný internet [online]. [cit. 1. 2. 2018]. Dostupné z: <http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx>

4.7 Fake News

S pojmem fake news se už pravděpodobně setkal každý, kdo sleduje televizní události, čte zprávy na internetu, nebo alespoň občas čte denní tisk. Samotný výraz je převzatý z anglického jazyka a v překladu znamená falešné zprávy. V současné době se používá jako ustálené vyjádření pro úmyslně nepravdivé či přímo lživé zveřejněné informace. Významově je stejný výraz dezinformace, často se používá i výraz hoax. Česky bychom mohli říct fáma.[27]

Dezinformace samozřejmě existovaly dávno před tím, než někdo vůbec začal přemýšlet o tom, že někdy by mohly existovat počítače nebo snad dokonce internet. Dezinformace se používaly jako součást válek už ve starověku, přes obě světové války, až po studenou válku, kdy ji využívaly všechny strany konfliktu. V současné době ale šíření dezinformací získalo na významu jako součást asymetrického, resp. hybridního způsobu vedení války právě proto, že došlo k rozšíření internetu mezi drtivou většinu běžné populace.

O asymetrickou válku se jedná v případě, že válčící strany jsou výrazně odlišné ve velikosti, ekonomické či vojenské síle, případně ve způsobu boje. V rámci asymetrické války se často používají hybridní způsoby boje. Hybridní způsob boje se vyznačuje svou odlišností od konvenčního vedení války. Podle vojenského teoretika Liddella Harta se jedná o tzv. nepřímé postupy. Jedná se například o nasazení malých speciálních jednotek bez označení a následné oficiální popíraní vojenského zásahu, vedení boje bez vyhlášení války, využívání vnitřní opozice a politické síly uvnitř nepřátelského státu, manipulace s politickým smýšlením širokého obyvatelstva nepřátelského státu a demoralizace společnosti. K takovým účelům skvěle slouží právě šíření dezinformace.

Nejznámější příkladem v současnosti vedené hybridní války může být Ruská federace. V únoru roku 2013 sepsal pro zpravodajský server Vojensko-průmyslový kurýr Valerij Gerasimov, náčelník ruského generálního štábu článek, ve kterém představil nový koncept vedení válek. V tomto článku je průběh války rozdělen na několik fází. Mezi jedny z prvních fází patří intenzivní informační kampaň zaměřená na zastrašení a klamání politických představitelů, masivní propaganda vedená s cílem zvýšit nespokojenost

[27] GREGOR, M., VEJVODOVÁ, P. *Nejlepší kniha o fake news!!!*. Brno: CPress, 2018. 8-10 s. ISBN 978-80-264-1805-4.

obyvatelstva, dále rozšiřování falešných dat a informací.[28] Článek byl zveřejněn v únoru roku 2013. V listopadu roku 2013 došlo k nepokojům na náměstí Majdan v ukrajinském Kyjevu, které následovaly události na poloostrově Krym a mezinárodně neuznané vyhlášení nezávislosti povstaleckých území Doněcko a Luhansko. Všechny tyto události provázela mocná dezinformační kampaň ze strany Ruska, přesně podle dříve zveřejněné Gerasimovy doktríny.

Obr. 3 – generál Valerij Vasilijevič Gerasimov[29]

Jak se ale dezinformační kampaně projevují v rámci České republiky? Je všeobecně přijímán názor, že v zájmu Ruské federace je destabilizace Evropské unie. S tímto záměrem se snaží ovlivnit veřejné mínění obyvatelstva v neprospěch Unie. K tomu využívá tzv. dezinformační weby, na kterých bývají zveřejňovány manipulativní, polopravdivé, či přímo lživé články. Tyto články bývají sdíleny prostřednictvím sociálních sítí, nejčastěji Facebooku a Twitteru a tím se dostávají do širokého povědomí lidí. Jako nejznámější dezinformační web bývá zmiňován Aeronet.cz.

Jako příklad dezinformační zprávy zveřejněné v České republice můžeme uvést článek zveřejněný dne 6. 10. 2017 na webových stránkách Krajských listů. Tento článek sděluje informaci, že právníci Evropské unie tvrdí, že připojení Krymu k Rusku je legální. Konkrétně je zde uvedeno toto tvrzení: „Právníci EU prokázali, že vstup Krymu do Ruské federace v roce 2014 byl proveden v souladu se zákony a ústavou Ukrajiny, stejně jako s mezinárodním právem.“[30] Server Manipulátoři.cz zaměření na odhalování dezinformací tento článek označil jako „hoax“ s odůvodněním, že článek se opírá

[28] Военно-промышленный курьер [online]. [cit. 6. 3. 2018]. Dostupné z <https://www.vpk-news.ru/articles/14632>
[29] Generál Valerij Vasilijevič Gerasimov. [online]. [cit. 12. 3. 2018]. Dostupné z: <https://www.geopolitica.ru/en/article/general-gerasimov-and-modern-war>
[30] Krajské listy [online]. [cit. 6. 3. 2018]. Dostupné z: <https://www.krajskelisty.cz/stredocesky-kraj/17890-pripojeni-krymu-k-rusku-je-legalni-tvrdi-pravnici-evropske-unie-skonci-tedy-sankce-patecni-komentar-stepana-chaba.htm>

o analýzu Christiana de Fouloy, který je šéfem organizace, která mezi zástupci Evropské unie pouze lobbuje, se samotnou Unií však nemá nic společného.[31]

Nebezpečí těchto dezinformačních zpráv však není v tom, že by bylo nemožné je ověřit. To lze ve většině případů celkem snadno. Avšak prostřednictvím sociálních sítí se takové zprávy sdílením dokáží rozšířit mezi široké obyvatelstvo. Při četbě takových zpráv, které sdílí někdo z přátel, pak lidé mají tendenci jim věřit, aniž by se vůbec podívali, odkud takové informace pocházejí. Takto se informace dostávají do širokého povědomí lidí, kteří je poté považuje za obecnou pravdu. Taková situace může být velice škodlivá zejména v situaci, kdy probíhají například volby, případně v situaci, kdy by bylo vyhlášeno všeobecné referendum např. o vystoupení České republiky z Evropské unie.

4.8 Modrá velryba

Začátkem dubna roku 2017 se českými médii začaly šířit zprávy o internetové hře zvané Modrá velryba, která údajně měla nezanedbatelný počet dětí dohnat k sebevraždě. Hra měla své počátky na území Ruské federace na sociální síti VKontakte. Později se rozšířila i za hranice Ruska i ruskojazyčných zemí a začala se hrát i prostřednictvím sociálních sítí jako je Facebook nebo Instagram. Princip hry je v plnění úkolů, který uživateli zasílá administrátor hry. Úkoly jsou z počátku jednoduché, jako třeba vydržet celou noc vzhůru nebo projít přes nějaké strašidelné místo, ale další úkoly stupňují svoji obtížnost. Následují úkoly typu zabití zvířete nebo sebepoškozování vyřezáváním obrazců do kůže. A posledním a hlavním úkolem je spáchat sebevraždu.

Protože i Policie České republiky fenomén Modrá velryba zcela vážně vnímala jako hrozbu, vydala dne 13. 4. 2017 tiskovou zprávu s varováním o existenci této hry a radami pro děti, rodiče i pedagogy, jak se chovat při kontaktu s takovou hrou.[32] Policie ČR byla následně několikrát obviněna z toho, že šíří tzv. hoax (falešnou zprávu), protože

[31] Manipulátoři.cz [online]. [cit. 6. 3. 2018]. Dostupné z: <http://manipulatori.cz/hoax-pravnici-eu-prokazali-ze-vstup-krymu-ruske-federace-roce-2014-proveden-souladu-se-zakony/>
[32] Policie České republiky [online]. [cit. 3. 3. 2018]. Dostupné z: <http://www.policie.cz/clanek/modra-velryba.aspx>

Modrá velryba neexistuje. Proti tomu se však Policie opakovaně ohradila s tím, že o existenci hry má důkazy.[33]

Obr. 4 – ilustrační obrázek[34]

Za tvůrce hry je považován Filipp Budeikin. Budeikin byl administrátor skupiny s názvem F57 na sociální síti VKontkate. Tato skupina sice už dnes neexistuje, ale v době svého založení kolem roku 2013 až 2014 sdružovala lidi, ve většině případů děti a mládež, kteří zde sdíleli obrázky se sebevražednou tématikou, citáty a texty o sebevraždách. Jedna z dívek na této skupině však sebevraždu skutečně spáchala. Šestnáctiletá Rina z malého města Ussurisjk na východě Ruské federace si lehla na koleje před projíždějící vlak. Ještě předtím si ale na nádraží vyfotila „selfie“ a sdílela

[33] Policie České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.policie.cz/clanek/vyjadreni-k-internetove-hre.aspx>
[34] Ilustrační obrázek. [online]. [cit. 12. 3. 2018]. Dostupné z: <https://im.tiscali.cz/press/2017/04/13/792427-modra-velryba-na-ceskem-netu-484x845.jpg>

ho na svém profilu na VKontkate. Její případ se stal mediálně známým a toho se rozhodl využít správce skupiny F57 Filipp Budeikin. Z Riny vytvořil vzor a vymyslel legendu, podle které Rina hrála hru Modrá velryba a prostřednictvím sebevraždy dosáhla poznání pravdy. Skupina F57 byla společností VKontakte následně zrušena, ale prakticky hned se začaly objevovat nové skupiny na stejné téma. Mnoho z nich založil sám Budeikin a prostřednictvím nich si vybíral děti a mládež, které snadno podlehly manipulaci, a snažil se je dohnat k sebevraždě. Fillip Budeikin byl v květnu roku 2017 v Rusku zatčen a byl obviněn z donucení k sebevraždě v nejméně šestnácti případech. Trestně stíhán je vazebně. Ve výsleších se měl policistům ke svému jednání doznat, ale soud dosud neproběhl.

Nebezpečí fenoménu Modrá velryba je v tom, že přestože jeho zakladatel a původce je sice ve vazbě a sám dále již nikoho ohrožovat nemůže, ale samotný fenomén se již šíří dál sám o sobě bez jeho pomoci. Nadále se zakládají a provozují skupiny na sociálních sítích podle jeho vzoru v různých jazykových verzích.

5 Prevence rizik na sociálních sítích

Jak již bylo popsáno, používání sociálních sítí s sebou přináší spoustu rizik, která mohou mít velmi závažné následky. Proto je nutné těmto rizikům předcházet vhodnou prevencí. Prevencí chápeme soubor vhodných opatření pro zamezení vzniku a rozšiřování negativních jevů. V této oblasti působí v České republice několik institucí a programů.

5.1 Národní centrum bezpečnějšího internetu

Přední institucí, která v České republice působí v oblasti prevence negativních jevů v oblasti chování na internetu a sociálních sítích je Národní centrum bezpečnějšího internetu (NCBI). NCBI je neziskové nevládní sdružení založené v roce 2007. Jeho posláním je přispívat ke zvýšení bezpečnosti užívání internetu, moderních informačních a komunikačních technologií, zvyšovat povědomí uživatelů o jejich kladech a možných nebezpečích, přispívat k osvojování etických norem v online prostředí, napomáhat předcházení a snižování možných sociálních rizik spojených s jejich užíváním.

K dosažení svých cílů sdružení podporuje účinné formy spolupráce neziskového sektoru, škol, knihoven, podnikatelské sféry a veřejné správy. Realizuje projekty zaměřené na zvyšování povědomí o hrozbách internetu, snižování bezpečnostních rizik užívání internetu a nových médií, boj proti ilegálnímu obsahu a pomoc dětem a jejich rodičům, které se na internetu ocitli v nesnázích. NCBI je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE a spolupracuje s mezinárodní sítí horkých linek INHOPE. NCBI realizuje řadu projektů, z nichž nejdůležitější je Safeinternet.cz, zaměřený na zvyšování povědomí o bezpečnějším užívání internetu. Podporuje vzdělávání v této oblasti, a to zejména dětí, kterým ubližuje nevhodné a závadné chování na internetu. Projekt je spolufinancovaný Evropskou komisí.[35]

[35] Národní centrum bezpečnějšího internetu [online]. [cit. 12. 1. 2018]. Dostupné z: <http://www.ncbi.cz>

5.2 Seznam se bezpečně

Projekt Seznam se bezpečně byl založen společností Seznam.cz za účelem osvěty a prevence v oblasti chování lidí na internetu. Impuls k založení tohoto projektu byl příběh mladé patnáctileté dívky, která v roce 2007 spáchala sebevraždu poté, co unikly její nahé fotky na internet. Společnost v rámci prevence natáčí filmy a krátké spoty, pořádá přednášky ve školách, ve spolupráci s nakladatelstvím GRADA vydala publikaci "Bezpečně na internetu" a ve spolupráci se Studiem Ypsilon připravila divadelní inscenaci #jsi_user.[36]

5.3 E-Bezpečí

Projekt E-Bezpečí je celorepublikový projekt zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény. Projekt je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi. Projekt je časově neohraničený.

Projekt se zaměřuje na nebezpečné internetové fenomény, které ohrožují jak děti, tak i dospělé uživatele internetu. Specializuje se zejména na kyberšikanu a sexting, kybergrooming, kyberstalking, rizika sociálních sítí (zejména sítě Facebook), hoax a spam, zneužití osobních údajů v prostředí elektronických médií.

Základním východiskem činnosti projektu je terénní práce s nejrůznějšími cílovými skupinami, přednášková činnost, preventivní vzdělávací akce apod. Přednášky 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.

[36] Seznam se bezpečně [online]. [cit. 12. 1. 2018]. Dostupné z: <https://www.seznamsebezpecne.cz/o-projektu>

Mezi cílové skupiny projektu E-Bezpečí patří žáci a studenti, učitelé, preventisté sociálně patologických jevů, metodici prevence, policisté a strážníci, manažeři prevence kriminality, vychovatelé, pracovníci OSPOD a v neposlední řadě také rodiče.

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 a učitele a realizuje řadu dalších aktivit.[37]

5.4 Centrum proti terorismu a hybridním hrozbám

Centrum proti terorismu a hybridním hrozbám vzniklo ke dni 1. ledna 2017 pod Ministerstvem vnitra České republiky. O jeho zřízení rozhodl ministr vnitra České republiky Milan Chovanec na jaře roku 2016 jako reakci na přítomnost rizika dezinformační kampaně ze zahraničí jako závažné hrozby pro vnitřní bezpečnost státu. Dezinformační kampaň je běžná součást asymetrických či hybridních hrozeb. Tvrzení, že Česká republika v současné době čelí hybridním hrozbám, v největší míře ze strany Ruské federace, je podepřeno veřejně dostupnou výroční zprávou bezpečnostní informační služby za rok 2016.[38]

Centrum je zřízeno pod Ministerstvem vnitra, protože řeší otázky týkající se vnitřní bezpečnosti státu, která pod Ministerstvo vnitra kompetenčně spadá. V praxi se jedná o odborné analytické a komunikační pracoviště, jehož primární náplň práce má být vyhledávání hrozeb spojených přímo s vnitřní bezpečností státu, což spočívá mimo jiné i v monitorování situace v oblasti dezinformačních kampaní.[39] Tyto kampaně jsou ve velké míře vedeny právě prostřednictví internetu a sociálních sítí, tudíž mezi činnosti Centra patří i monitorování sociálních sítí. Navzdory obavám veřejnosti, které byly podpořeny i vyjádřením prezidenta České republiky Miloše Zemana ve svém vánočním poselství, se nejedná o žádný nový úřad, který by mohl uplatňovat cenzuru či omezovat

[37] E-Bezpečí [online]. [cit. 1. 3. 2018]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>
[38] Bezpečnostní informační služba [online]. [cit. 5. 3. 2018]. Dostupné z: <https:/www.bis.cz/vyrocni-zprava16e1.html?AricleID=1136>
[39] Ministerstvo vnitra České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.mvcr.cz/cthh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx>

internet. Jedná se o tým odborníků, který by měl být v počtu okolo 20 lidí, kteří pracují s veřejnými zdroji. Na svá zjištění mají povinnost reagovat oznámení příslušným orgánům. V případě zjištění zveřejněné dezinformační zprávy na tuto reagují svým vyjádřením, které zveřejňují prostřednictvím webových stránek Ministerstva vnitra, případně svého profilu na sociální síti Twitter.

To, jak Centrum proti terorismu a hybridním hrozbám funguje v praxi, si můžeme ukázat na praktickém příkladu. Dne 27. 12. 2017 byl na webových stránkách politické strany SPD Tomia Okamury zveřejněn článek s názvem ČR hrozí teroristické útoky.[40] Tento článek obsahoval i video s vyjádřením Tomia Okamury. Článek s videem čtenářům sděloval informaci, že v České republice došlo ke zhoršení bezpečnosti a hrozí teroristické útoky. Jako důvod této situace uvádí členství České republiky v Evropské unii spolu s migrační krizí. Pracovníci Centra proti terorismu a hybridním hrozbám tento článek vyhodnotili jako dezinformační, na základě čehož ministr vnitra Lubomír Metnar vydal na webových stránkách Ministerstva vnitra prohlášení, ve kterém výroky Tomia Okamury odmítl s odůvodněním, že Česká republika zůstává jednou z nejbezpečnějších zemí světa a podle objektivních bezpečnostních parametrů se její bezpečnostní situace nezhoršuje.[41] Odkaz na tento článek byl také sdílen na twitterovém profilu Centra proti terorismu a hybridním hrozbám.

5.5 Společnost pro podporu lidí s mentálním postižením

V roce 2016 vyšla v České republice publikace s názvem Sexuální násilí v rámci edice „Už Vím! Srozumitelně o těle a duši pro ženy s mentálním postižením“. Tato publikace byla vydána Společností pro podporu lidí s mentálním postižením v České republice za podpory grantů z Islandu, Lichtenštejnska a Norska v rámci EHP fondů. Jedná se o krátkou brožuru s ilustracemi, která jednoduchou a srozumitelnou formou ženám s mentálním postižením vysvětluje co to je sexuální násilí a jak se mu bránit. V jedné ze svých částí se brožura věnuje rizikům seznámení na internetu

[40] SPD.cz [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.spd.cz/novinky/tomio-okamura-cr-hrozi-teroristicke-utoky>
[41] Ministerstvo vnitra České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.mvcr.cz/clanek/reakce-ministra-vnitra-na-vyroky-tomia-okamury.aspx>

a hlavně na Facebooku, předestírá rizika takových seznámení a radí, jak se v prostředí internetu a Facebooku chovat.[42]

Preventivní práce s mentálně hendikepovanými osobami je velice důležitá, protože by bylo iluzorní a naivní domnívat se, že mentálně postižení lidé se budou internetu vyhýbat.

5.6 Prevence proti dezinformacím

Prevence proti dezinformacím v České republice bohužel ještě není na vysoké úrovni a nemá dlouhou tradici. Již bylo zmíněno, že dezinformacím jako součást hybridních hrozeb se věnuje Centrum proti terorismu a hybridním hrozbám organizačně spadající pod Ministerstvo vnitra České republiky. Kromě tohoto státního útvaru se ale věnují i nezávislé projekty.

Za jednu z těchto aktivit se dá považovat i projekt Demagog. Tento projekt byl založen už v roce 2012 studenty politologie z Masarykovy univerzity. Projekt funguje na webových stránkách demagog.cz a jeho cílem je upozorňovat na nepravdivá a manipulativní tvrzení. Jeho činnost spočívá v ověřování takových tvrzení a zveřejňování zpráv o výsledcích.[43]

Dalšími projekty mající obdobnou činnost a cíle jako Demagog jsou Manipulátoři.cz, StopFake.org, Hoax.cz a další.

5.7 Nezávislé publikace

V rámci osvěty v oblasti prevence negativních jevů v prostředí internetu v poslední době vychází spoustu publikací nezávislých autorů, ať českých nebo i zahraničních.

[42] UHLÍŘOVÁ, B. a spol. *Sexuální násilí*. Praha: Společnost pro podporu lidí s mentálním postižení, 2016. s 1-43. ISBN 978-80-906224-8-7.
[43] Demagog.cz [online]. [cit. 7. 3. 2018]. Dostupné z: <https://demagog.cz/diskuze/o-nas>

Z těch českých můžeme jmenovat knihu Mojmíra Krále *Bezpečný internet – Chraňte sebe i svůj počítač*. Kniha se věnuje obecně rizikům při používání počítačů a internetu. Předkládá obecné zásady chování v kyberprostoru i se zaměřením na sociální sítě. Základní poselství této knihy je chovat se co nejvíce bezpečně. Využívat silná hesla, nikomu a ničemu nevěřit.[44]

Zahraniční publikací, která vyšla již v roce 2002 ve spojených státech amerických je obsáhlá kniha autora Terriho Bidwella *Hack Proofing Your Identity in the Information Age*. Přestože tato kniha vyšla již před 16 lety, informace týkající se chování v prostředí internetu jsou stále platná. Část této knihy se věnuje problematice používání internetu dětmi. Autor připouští, že je nereálné hlídat děti celý čas při práci s počítačem, proto uvádí, že je nezbytné věnovat se výchově a vštěpování zásad, jak se mají děti v digitálním světě chovat.[45]

[44] KRÁL, M. *Bezpečný internet – Chraňte sebe i svůj počítač*. Praha: Grada Publishing, a.s., 2015. s. 107-110. ISBN 978-80-247-5453-6.
[45] BIDWELL, T. Hack Proofing Your Identity in the Information Age. Rockland, MA, USA: Syngress Publishing, Inc, 2002. s 241-260. ISBN 1-931836-51-5.

6 Praktická část – experiment

V teoretické části této bakalářské práce byl představen svět sociálních sítí a byly zmapovány rizika, s kterými se uživatelé při jejich používání mohou setkat. Abychom ale zjistili, jak ve skutečnosti jednoduché nebo složité je stát se potencionální obětí těchto rizik, případně taková rizika vyvolat, využijeme metodu experimentu jako formu řízeného pozorování. Pro účely experimentu bude využita sociální síť Facebook. Facebook byl zvolen proto, že se jedná o nejrozšířenější sociální síť na světě, bývá považován za sociální síť v pravém slova smyslu a výsledky experimentu mohou být analogicky použity pro sociální sítě obecně.

Experiment bude proveden v mezích všech platných a účinných zákonů České republiky. V případě, že v rámci experimentu budou zjištěny přesné osobní údaje osob, přestože budou zjištěny z veřejných zdrojů, budou v této práci z etických důvodů uvedeny pouze v obecné rovině, případně budou anonymizovány.

6.1 Stanovení hypotéz

Pro následující experiment budou stanoveny hypotézy. Tyto hypotézy budou vycházet z všeobecně přijímaných stanovisek k bezpečnosti a dalším okolnostem spojených s využíváním sociálních sítí.

1) Zaregistrovat se na sociální síť může každý bez ohledu na podmínky používání.

2) Na sociálních sítí lze snadno navázat komunikaci s neznámými lidmi.

3) Na sociálních sítích lze jednoduše vystupovat pod smyšlenou identitou.

4) Na sociálních sítích je snadné vytvořit situaci příznivou pro páchání škodlivého a nebezpečného jednání.

6.2 Provedení experimentu

Experiment zahajujeme dne 5. března 2018 v 18:00 hodin. Základním krokem, který pro náš experiment potřebujeme provést, je zaregistrovat se na sociální síti Facebook. Po otevření webových stránek https://www.facebook.com je jako první zobrazena nabídka k registraci nového uživatelského účtu. Pro registraci je třeba zadat buď číslo mobilního telefonu nebo e-mailová adresa. Mobilní telefon pro účely experimentu nemáme, proto si založíme e-mailovou schránku. Zvolíme poskytovatele e-mailových schránek Proton Mail na webových stránkách https://www.protonmail.com. Tohoto poskytovatele volíme proto, že se umožňuje založení e-mailové schránky na velmi vysoké úrovni anonymity. Veškerá fyzická datová úložiště provozuje ve Švýcarsku, všechna data šifruje a odmítá poskytovat komukoliv, včetně orgánů činných v trestním řízení. Jako e-mailová adresa byla zvolena young.sporter@protonmail.com. Do adresy byl záměrně zvolen tvar neobsahující žádné jméno ani údaj o věku. Jako heslo bylo zvoleno osmimístné číslo. Vytvoření e-mailové schránky trvalo i s otevřením webové stránky poskytovatele a vyplnění registračních údajů méně než 2 minuty.

6.2.1 Vytvoření registrace na Facebooku

Poté, co vlastníme e-mailovou schránku, můžeme přejít k vytvoření registrace na Facebooku. První údaj, který musíme při registraci zadat, je jméno a příjmení. Jako křestní jméno bylo náhodně zvoleno Majk. Jako příjmení bylo zvoleno náhodný shluk písmen Emem. Další údaj, který je nutné vyplnit, je datum narození. Náhodně zadáme datum 2. března 2002. Tím dáváme najevo věk 16 let. Jako pohlaví zadáváme možnost muž. Nyní nám již zbývá potvrdit tlačítko „Vytvořit účet“. Na tímto tlačítkem se menším a nevýraznějším písmem nachází poučení: *„Kliknutím na tlačítko Vytvořit účet vyjádříte svůj souhlas s našimi podmínkami a potvrdíte, že jste obeznámeni s našimi zásadami používání dat včetně informací o použití souborů cookie. Můžete od Facebooku dostávat SMS upozornění, jejichž příjem se dá kdykoli zrušit.“* V tomto poučení je odkaz na podmínky a zásady používání. Tyto otvíráme, ale nyní je číst nebudeme, protože vycházíme z předpokladu, že běžný uživatel při zakládání uživatelského účtu podmínky použití nečte. Po dokončení registrace tyto podmínky ovšem pečlivě prostudujeme. Nyní tlačítkem necháváme vytvořit účet. Takřka okamžitě nám do naší e-mailové schránky přichází kód pro potvrzení registrace. Registraci

potvrzujeme. Tímto jsme proces registrace dokončili a nezabralo nám to více než 2 minuty, do čehož zahrnujeme i vymýšlení registračních údajů.

6.2.2 Podmínky používání

Nyní prostudujeme podmínky používání služby Facebook. Tyto podmínky jsou veřejně dostupné na webových stránkách Facebooku, jejich vyhledání a otevření je snadné. Nepůsobí dojmem, že bylo záměrem je jakkoliv skrýt či znepřehlednit. Jediným problémem se zdá být jejich obsáhlost a neatraktivnost. Stěží si lze představit, že takový rozsáhlý seznam podmínek by si třináctileté dítě, které si již uživatelský profil na Facebooku může založit, před potvrzením registrace řádně prostudovalo. Podmínky používání jsou rozdělené do několika kapitol. Popsány budou jen některé z nich související se zkoumanou problematikou.

Velmi podstatné informace jsou uvedeny v kapitole Sdílení vašeho obsahu a informací. Zde se dozvídáme, že sdílením jakéhokoliv obsahu (fotografie, videa a další) výslovně udělujeme společnosti Facebook licenci k použití veškerého obsahu. Tato licence končí odstraněním obsahu ze svého účtu, s výjimkou případů, kdy jsme daný obsah sdíleli s dalšími uživateli. Z této informace vyplývá, že v případě, kdy například na svůj účet nahrajeme svoji vlastní fotografii a následně ji sdílíme s přáteli, navždy nad ní ztrácíme kontrolu a dáváme společnosti Facebook právo s ní volně nakládat.

V kapitole s názvem bezpečnost se dozvídáme, že používáním služby Facebook bereme na vědomí mimo jiné následující závazky: nebudeme se pokoušet zjistit přihlašovací údaje ani získat přístup k účtu patřícímu někomu jinému; nebudeme šikanovat, zastrašovat ani obtěžovat žádného uživatele; nebudeme zveřejňovat nenávistné projevy, výhružky nebo pornografii, podněty k násilí nebo obsah s nahotou či realisticky vyobrazené bezdůvodné násilí; nepoužijeme Facebook k činnostem nezákonným, klamavým, škodlivým nebo diskriminačním.

Další kapitola se věnuje bezpečnosti registrace a účtu. Tato kapitola obsahuje prohlášení týkající se dodržování následujících závazků. Neposkytneme Facebooku falešné osobní informace ani bez povolení nevytvoříme účet pro nikoho jiného. Nebudeme vytvářet víc než jeden uživatelský účet. Nebudeme Facebook používat, pokud je nám méně než 13 let. Nebudeme Facebook používat, pokud jsme odsouzeným sexuálním delikventem.

6.2.3 Vytvoření uživatelského profilu

To hlavní, registraci na Facebooku, již máme. Nyní si potřebujeme upravit náš uživatelský profil. Ústředním motivem takového profilu je profilová fotografie. Jelikož nemáme v úmyslu zveřejnit svoji skutečnou podobu, zvolíme nějakou fotografii vyhledanou pomocí vyhledávače Google. Protože v rámci experimentu nemáme v úmyslu zneužít podobu existující osoby, vybereme logo emotikonu – klasického žlutého smajlíka. Jako současné místo pobytu zadáme Prahu. Jako další informace o sobě bychom mohli zadat rodinný stav, školu, zaměstnání, kontaktní údaje, svoje záliby, životní události a další. Tím vším bychom profilu dodali na důvěryhodnosti, ale pro potvrzení stanovených hypotéz nám bude stačit uživatelský profil vyplněný základními údaji.

6.2.4 Vyhledání „přátel“

Aby se náš uživatelský profil stal plnohodnotnou součástí Facebooku a také tak fungoval, je třeba propojit se s dalšími uživateli, což v prostředí Facebooku znamená přidat si někoho do přátel. Pro vyhledání přátel je dostupných více způsobů. Buď můžeme přímo přes vyhledávací pole najít někoho koho známe podle jména, e-mailu nebo telefonního čísla. Tuto možnost z našeho experimentu předem vylučujeme, protože chceme vyhodnotit hypotézu, zda je možné navázat komunikaci s neznámými osobami. Volíme tedy takovou variantu, že vyhledáme osobnost, která v současné době láká velké množství fanoušků, a na jejích stránkách vyhledáme jednotlivé uživatele, které následně požádáme o přidání do přátel.

Vzhledem k aktuální situaci v souvislosti s Olympijskými hrami jsme vybrali Ester Ledeckou. Vycházíme z toho, že fanoušci Ester Ledecké pokrývají všechny věkové skupiny lidí nezávisle na pohlaví. Vyhledáním jejího jména jsme se dostali na její fanouškovskou stránku. Tato stránka má ke dni 5. 3. 2018 více než 148 tisíc jednotlivých sledujících. Zjišťujeme, že není možné otevřít přehledný seznam všech těchto uživatelů. Je ale možné snadno otevřít jednotlivé seznamy uživatelů, kteří přidali ke konkrétním příspěvkům na stránce své komentáře, případně je ohodnotili jako „To se mi líbí“. To pro účely našeho experimentu plně postačuje. Proto budeme otevírat jednotlivé příspěvky na stránce, náhodně vybírat jednotlivé uživatelské profily a žádat je o přidání do přátel. Tímto způsobem je požádáno o přidání do přátel přesně 100 různých uživatelů. Tito uživatelé jsou vybráni naprosto náhodně bez jakéhokoliv klíče. Není přihlíženo k věku, pohlaví, ani profilové fotografie. Jelikož byly žádosti o přidání

do přátel zasílány vzápětí za sebou, osmkrát se zobrazilo upozornění s textem „Doporučujeme posílat žádosti přátel jen lidem, které znáte osobně.“ Po prostém klepnutí na tlačítko Potvrdit systém umožní odesílat žádosti dál. Následně budou žádosti o přidání do přátel zasílány uživatelům, kteří budou nalezeni v seznamech přátel původně oslovených uživatelů ze stránky Ester Ledecké. Plán je celkově takto odeslat 1 tisíc žádostí. Tento způsob rozesílání žádostí bude použit z důvodu zajištění diverzity oslovených uživatelů z různých vrstev obyvatelstva ve všech ohledech. Tato činnost probíhá v době od 5. 3. 2018 19:30 do 19:36 hodin.

První uživatel přijal žádost o přátelství do 2 minut po odeslání žádosti. Po zobrazení toho uživatelského profilu s názvem Eva Leipnerova si můžeme prohlédnout profilovou fotografii i další sdílené fotografie uživatelky, fotografie jejího zjevně nezletilého dítěte, město pobytu i přesné místo i pozici v zaměstnání, datum narození, odkaz na uživatelské profily rodinných příslušníků jako jsou otec, matka, sourozenci, bratranci a sestřenice. Po zběžném projití profilové stránky uživatelky Evy zjišťujeme, že se dne 3. června roku 2017 nacházela na dovolené u moře v Itálii, je zde uvedena přesná poloha, její fotografie a z kontextu se dozvídáme, že příspěvek byl sdílen v reálném čase při pořízení fotografie. Dále je nám přístupný i úplný seznam přátel, s kterými je uživatelka Eva ve spojení.

6.2.5 Blokace ze strany Facebooku

Po odeslání 110 žádostí o přidání do přátel náhodným uživatelům došlo k zablokování této funkce. Bylo zobrazeno upozornění ve znění: „*Facebook Varování - Chceme, aby bylo na Facebooku bezpečno. Musíme proto čas od času blokovat určitý obsah a akce. Pokud si myslíte, že jsme udělali chybu, dejte nám prosím vědět. Přestože nedokážeme prověřit všechna hlášení jednotlivě, vaše zpětná vazba nám pomůže zlepšovat bezpečnost prostředí na Facebooku.*“ Po rozbalení podrobností se dozvídáme následující: „*Odesílání žádostí o přátelství můžete mít zablokované z několika důvodů. Mohlo se třeba stát, že vámi poslané žádosti o přátelství zůstaly nezodpovězené, nebo byly označené jako nevítané. Příště posílejte žádosti o přátelství lidem, se kterými se znáte ve skutečném životě. Mezi takové lidi patří například vaši přátelé, rodina, kolegové nebo spolužáci.*“ Blokování je časově omezené, ale při opakování stejného jednání se vystavujeme riziku, že náš uživatelský účet bude zablokován trvale. Proto nenaplníme náš původní plán rozeslat 1 tisíc žádostí o přátelství a spokojíme se s počtem žádostí 110, které jsme již rozeslali. Na reakci

oslovených uživatelů vyčkáme přesně 4 dny, které jsou dostačující. Následně výsledek vyhodnotíme.

6.2.6 Přijetí do přátel a komunikace

Dne 9. 3. 2018 v 19:30 hodin, tedy přesně po 4 dnech, vyhodnotíme úspěch odeslaných žádostí o přijetí do přátel na Facebooku. Z počtu 110 odeslaných žádostí jich bylo kladně přijato celkem 7. Všechny osoby, které žádosti přijaly, byly starší 18 let. Jeden byl muž, šest bylo žen. Ani jeden z těchto sedmi uživatelů si dotazem neověřil, jestli se jedná o žádost jemu známého člověka. U čtyřech z těchto sedmi osob byl vyplněn celý datum narození. Město pobytu bylo sdíleno u všech. Bohužel nelze ověřit, že tyto vyplněné údaje jsou pravdivé, avšak působily věrohodným dojmem. Další dvě osoby, kterým byly odeslány žádosti o přidání do přátel, reagovaly zasláním zprávy s dotazem, zda se známe. Obě osoby byly ženy starší osmnácti let. Po odpovědi, že neznáme, ukončily komunikaci a žádost nepotvrdily. Zbylých 101 osob nereagovalo vůbec.

Následně byl proveden pokus o navázání komunikaci s každou ze sedmi osob přidaných do přátel. Každému jednotlivému uživateli byla odeslána soukromá zpráva s pozdravem a zahájením konverzace. Ani jedna z těchto osob na zprávu během dalších třech dnů nezareagovala.

6.3 Vyhodnocení experimentu

V rámci experimentu byl založen e-mailový účet u anonymního poskytovatele bez použití jakýchkoliv identifikačních údajů. Založení účtu trvalo necelé 2 minuty a obtížnost tohoto úkonu nebyla téměř žádná.

Pomocí anonymního e-mailového účtu byl založen uživatelský profil na smyšlené, zjevně nereálné jméno se smyšleným datem narození (s věkem méně než 18 let) bez použití skutečné fotografie. Tento úkon byl proveden s naprostou jednoduchostí s časovou náročností do 2 minut. Z uvedeného zjištění vyplývá skutečnost, že stejně jednoduše by bylo možné založit uživatelský účet s věrohodně znějícím jménem a profilovou fotografií, který by budil důvěru.

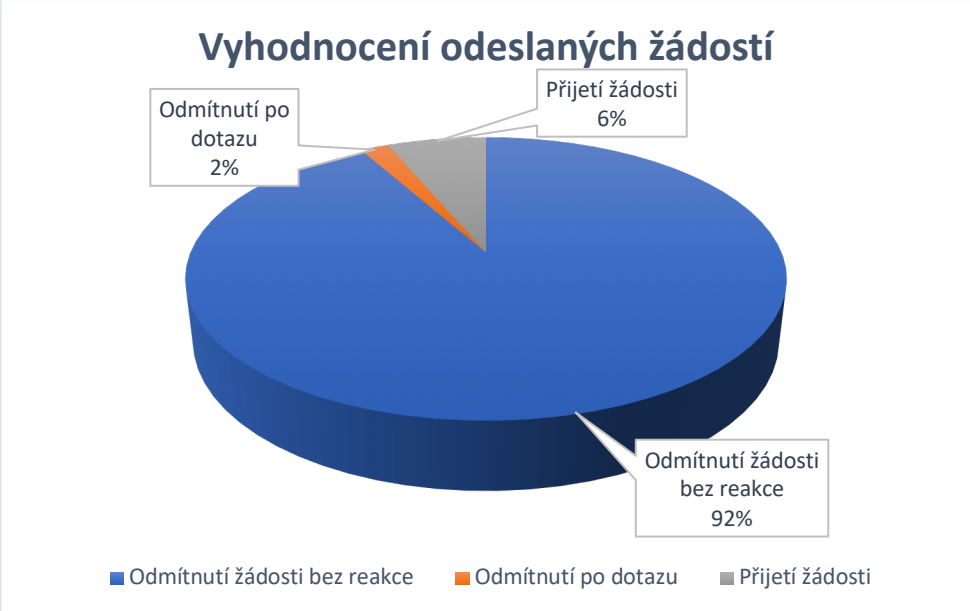
Následovalo vyhledávání náhodných uživatelských účtů, kterým byly odeslány žádosti o přidání do přátel. V našem případě byly žádosti rozeslány náhodně bez jakéhokoliv klíče, odesílání žádostí trvalo 6 minut. Po odeslání 110 náhodných žádostí o přidání do přátel byla tato funkce automatickým bezpečnostním systémem Facebooku zablokována z důvodu vyhodnocení škodlivé činnosti. Původní plán experimentu odeslat 1 tisíc žádostí tedy nebyl naplněn, ale bylo zjištěno, že Facebook disponuje účinným nástrojem pro zamezení hromadného rozesílání žádostí o přidání do přátel neznámým osobám.

Ze vzorku 110 odeslaných žádostí o přidání do přátel tuto žádost bez dalšího ověřování potvrdilo 7 osob, všechny byly starší 18 let. U čtyřech z těchto osob byly na jejich uživatelských profilech nalezeny zneužitelné osobní údaje. S nikým z uvedených sedmi osob se nepodařilo navázat komunikaci. Další dvě osoby, kterým byly žádosti odeslány, si zprávou ověřovaly, zda se jedná o žádost od jim známé osoby. Po zjištění, že ne, komunikaci ukončily a žádost odmítly.

Tab. č. 1: Přehled žádostí o přijetí do přátel

Odesláno žádostí celkem	110
Odmítnutí žádosti bez reakce	101
Odmítnutí po dotazu	2
Přijato žádostí	7

Graf č. 1: Přehled žádostí o přijetí do přátel



6.3.1 Zhodnocení hypotéz

1) Zaregistrovat se na sociální síť může každý bez ohledu na podmínky používání. *Hypotéza byla potvrzena. Registrace na sociální síť je snadná a bez jakýchkoliv faktických omezení.*

2) Na sociálních sítí lze snadno navázat komunikaci s neznámými lidmi. *Hypotéza byla vyvrácena. Proti hromadnému navázání komunikace s neznámými lidmi aktivně působí Facebook se svými automatickými bezpečnostními nástroji. Samotní uživatelé na komunikaci od neznámých osob ve většině případů nereagují.*

3) Na sociálních sítích lze jednoduše vystupovat pod smyšlenou identitou. *Hypotéza byla potvrzena. Na sociální sítí Facebook neexistuje účinný nástroj zamezující nebo stěžující použití smyšlené identity.*

4) Na sociálních sítích je snadné vytvořit situaci příznivou pro páchání škodlivého a nebezpečného jednání.
Hypotéza byla vyvrácena. Není snadné navázat komunikaci s neznámými osobami, tedy není snadné ani vytvořit situaci příznivou pro páchání škodlivého jednání. Vytvoření takové situace by vyžadovalo vynaložení značnějšího úsilí.

7 Návrhy prevence a vlastní sociální síť

V bakalářské práci byly představeny jednotlivé druhy sociálních sítí a byly zmapovány preventivní programy a opatření aplikované v rámci České republiky. Nyní budou navrhnuta další opatření v rámce prevence a také bude navrhnuta „ideální“ sociální síť s využitím poznatků získaných provedeným experimentem.

7.1 Návrh prevence

Používání internetu a život na sociálních sítích je velmi komplexní problematika. V současné době sociální sítě používá většinová část populace, včetně dětí. Rizika, která práci s internetem a sociálními sítěmi provázejí, mohou mít dalekosáhlé dopady. Proto je nezbytné tato rizika omezovat účinnou prevencí. Tato prevence by měla být zaměřena na osvětovou činnost – zvyšování povědomí široké populace o těchto rizicích a výchovné a vzdělávací působení na potencionální oběti.

Účinný způsob prevence by bylo zavedení vzdělávacích programů problematiky rizik internetu a sociálních sítí do osnov učiva základních a středních škol do předmětů typu informatika či občanská a rodinná výchova. Obsáhlost této problematiky určitě nemůže obsáhnout jedna přednáška. Úspěch takové prevence závisí na skutečném pochopení problematiky, povědomí o existujících hrozbách a na získání návyků bezpečného a zodpovědného chování v rámci internetu a sociálních sítí.

Další účinný systém prevence by bylo široké zvyšování povědomí o rizicích internetu a sociálních sítí celé populace. Jako vhodné by se jevily krátké vzdělávací spoty v televizním vysílání, v rámci upoutávek před promítáním filmů v kinech, případně v rámci reklam před videi na serverech YouTube.com, Stream.cz a podobných.

Protože na chování dětí má v nejvyšší míře význam dohled rodičů, je nezbytné zvyšovat povědomost o uvedené problematice i u nich. Pro tyto účely by se jako nejvhodnější jevily informační brožury rozdávané ve školách na třídních schůzkách a podobně.

7.2 Návrh „ideální“ sociální sítě

V bakalářské práci byly představeny různé sociální sítě používané po celém světě, byla zmapována rizika jejich používání a v rámci experimentu byl ověřen způsob běžného fungování sociální sítě Facebook, ve kterém bylo mnoho prvků kritizováno. Proto bude nyní představen návrh sociální sítě, která by mohla naplnit pojem „ideální“ sociální síť z hlediska bezpečnosti proti negativním jevům sociální sítě provázející.

V současné době je celosvětově nejpoužívanější sociální síť Facebook. Facebook bývá považován za prototyp univerzální sociální sítě, jejíž funkce uživatelé vyžadují. Proto princip Facebooku budeme považovat za základní kámen „ideální“ sociální sítě.

7.2.1 Registrace

Registrace nového uživatelského účtu by měla být postavená na autorizace každého jednotlivého uživatele. V praxi by to bylo proveditelné podle způsobu autorizované registrace na aukčním serveru Aukro.cz. Uživatel by při registraci musel zadat svou skutečnou adresu (ta by pro ostatní uživatele nebyla viditelná), na kterou by mu poštovní zásilkou přišel autorizační kód, pomocí kterého by registraci dokončil. Tímto způsobem by se dal ověřit i věk registrujících se uživatelů, přičemž osobám mladším, než je stanovený minimální věk, by registrace nebyla umožněna. Zároveň minimální věk pro registraci by musel zavdávat trestní odpovědnost (v České republice dovršení 15 let věku). Anonymita mezi jednotlivými uživateli by zůstala na stejné úrovni jako v případě Facebooku a zároveň by orgány činné v trestním řízení dostaly účinný nástroj pro objasňování trestné činnosti páchané v rámci sociálních sítí.

7.2.2 Podmínky a zásady používání

Jako nedostatečné je nutno považovat potvrzení souhlasu s podmínkami a zásadami používání zaškrtnutím jednoho tlačítka bez nutnosti tyto podmínky vůbec číst. Jako nejvhodnější by se jevilo uživateli při registraci předkládat postupně a jednotlivě nejdůležitější zásady a podmínky používání. Tím by se docílilo toho, že každý registrovaný uživatel by měl o takových podmínkách a zásadách povědomí.

7.2.3 Kontrola obsahu

Už v současné době společnost Facebook zaměstnává pracovníky, jejichž činnost spočívá v kontrole obsahu sdíleného na sociální síti. Tato kontrola by však

v „ideální“ sociální sítě měla být intenzivnější založená na dostatečném množství takových pracovníků s využitím účinných nástrojů pro automatické kontroly a blokace závadného obsahu. Zároveň by měla probíhat intenzivnější a rychlejší spolupráce s orgány činnými v trestním řízení jednotlivých států, kde by sociální síť působila.

Závěr

Internet představuje jeden z nejvýznamnějších vynálezů lidské historie. Prakticky všechny oblasti lidské činnosti se nějakým způsobem internetu dotýkají, byly na internet přeneseny, případně byly internetem zjednodušeny. Lidská komunikace nikdy v historii nebyla jednodušší než dnes. Naprosto bez komplikací s mizivou finanční nákladností můžeme komunikovat s člověkem na druhé straně zeměkoule a takové možnosti jsou dostupné většině populace.

Rozmach internetu je pro lidstvo velkým přínosem, avšak přinesl s sebou i svá rizika. Cílem bakalářské práce bylo tato rizika zmapovat a definovat, především ve vztahu k problematice sociálních sítí, protože právě sociální sítě v současné době zažívají rozšíření mezi široké vrstvy populace jako významného komunikačního nástroje.

V úvodní části práce bylo definováno, že sociální sítě v současném chápání znamenají internetové služby umožňující registraci jednotlivých uživatelů za účelem komunikace s dalšími uživateli prostřednictvím soukromých zpráv a veřejného sdílení obsahu. Byly představeny jednotlivé druhy sociálních sítí, které jsou považovány za nejrozšířenější, jako je Facebook, Twitter, Instagram a další.

V další části práce byly představeny negativní jevy a rizika, která uživatele internetu, resp. sociálních sítí, provázejí a jejichž se mohou stát obětmi. Mezi ty patří kyberšikana, kyberstalking, šíření falešných zpráv a další.

Následně byly přehledně představeny preventivní programy proti negativním jevům souvisejícím s používáním internetu a sociálních sítí, které jsou uplatňovány v rámci České republiky.

V praktické části práce byl proveden experiment v podobě praktického založení uživatelského účtu na sociální síti Facebook za užití smyšlených osobních údajů. Následně byly prováděny pokusy o navázání komunikace s neznámými osobami za účelem zjištění, zda je skutečně tak jednoduché v rámci sociálních sítí vytvořit situace příznivé pro vznik negativních a škodlivých jevů. Experimentem bylo zjištěno, že sociální síť Facebook má vlastní automatické bezpečností mechanismy, které takovému jednání zamezuje. Bylo tedy zjištěno, že vytvoření rizikových situací není úplně snadné a pro jeho úspěšné provedení by bylo třeba větší míry námahy a časové investice.

Na základě zjištění z teoretické části práce a z výsledků experimentu byly vytvořeny návrhy na další preventivní opatření, která by se dala v České republice aplikovat. Hlavním cílem těchto preventivních opatření by mělo být zvyšování povědomosti veřejnosti o možných rizicích používání sociálních sítí a internetu.

Dále byl vytvořen návrh na fungování „ideální“ sociální sítě z pohledu bezpečnosti proti negativním jevům. V takové sociální síti by měl být kladen důraz na autorizaci jednotlivých uživatelských účtů a na důsledné kontrolování a vymáhání dodržování podmínek a zásad použití sociální sítě.

Je nezpochybnitelné, že přes všechny své přínosy masové rozšíření internetu a sociálních sítí nese jistá rizika, která mají značnou společenskou nebezpečnost. Pro zamezení těmto rizikům se jeví jako nejúčelnější nasazení účinné prevence a celospolečenské vzdělávací a výchovné působení v uvedené problematice. Internet i samotné sociální sítě se ze své podstaty velkou rychlostí vyvíjejí a posouvaní dál, i za pouhý rok nebo dva už situace může být značně odlišná od té dnešní. Proto je nutné problematiku dále zkoumat a preventivní a vzdělávací materiály neustále přizpůsobovat aktuálním rizikům.

Seznam použitých zdrojů

Literární zdroje

1. BIDWELL, T. Hack Proofing Your Identity in the Information Age. Rockland, MA, USA: Syngress Publishing, Inc, 2002. 370 s. ISBN 1-931836-51-5.
2. GREGOR, M., VEJVODOVÁ, P. *Nejlepší kniha o fake news!!!*. Brno: CPress, 2018. 142 s. ISBN 978-80-264-1805-4.
3. HULANOVÁ, L. *Internetová kriminalita páchaná na dětec*h. Praha: Stanislav Juhaňák – Triton, 2012. 217 s. ISBN 978-80-7387-545-9.
4. KOPECKÝ, K., SZOTKOWSKI, R., KREJČÍ, V. *Risks of Internet Communication IV*. Palacký University Olomouc: 2014. 151 s. ISBN 978-80-244-4105-4.
5. KRÁL, M. *Bezpečný internet – Chraňte sebe i svůj počítač*. Praha: Grada Publishing, a.s., 2015. 184 s. ISBN 978-80-247-5453-6.
6. LINHART, J., PETRUSEK, M., VODÁKOVÁ, A. *Velký sociologický slovník, svazek 2*. Praha: Karolinum, 2010. 1627 s. ISBN 978-80-718-4311-5.
7. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU, 2012. *Kybergrooming a kyberstalking*. Metodický materiál pro pedagogické pracovníky. s. 1-34.
8. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. 636 s. ISBN 978-80-7380-501-2.
9. UHLÍŘOVÁ, B. a spol. *Sexuální násilí*. Praha: Společnost pro podporu lidí s mentálním postižení, 2016. 43 s. ISBN 978-80-906224-8-7.
10. ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. 148 s. ISBN 978-80-7552-758-5.

Elektronické zdroje

1. Ask.fm [online]. [cit. 6. 3. 2018]. Dostupné z: <https://about.ask.fm/about/>
2. Bezpečnostní informační služba [online]. [cit. 5. 3. 2018]. Dostupné z: <https:/www.bis.cz/vyrocni-zprava16e1.html?AricleID=1136>
3. Bezpečně online [online]. [cit. 3. 2. 2018]. Dostupné z: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybergrooming.html>

4. Bezpečný internet [online]. [cit. 1. 2. 2018]. Dostupné z: <http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx>
5. Военно-промышленный курьер [online]. [cit. 6. 3. 2018]. Dostupné z <https://www.vpk-news.ru/articles/14632>
6. Centrum pro oběti domácího a sexuálního násilí [online]. [cit. 1. 3. 2018]. Dostupné z: <http://www.profem.cz/clanek.aspx?a=97>
7. Demagog.cz [online]. [cit. 7. 3. 2018]. Dostupné z: <https://demagog.cz/diskuze/o-nas>
8. DSL.cz [online]. [cit. 1. 2. 2018]. Dostupné z: <http://www.dsl.cz/jak-na-to/jak-se-pripojit-k-internetu>
9. E-Bezpečí [online]. [cit. 16. 2. 2018]. Dostupné z: <https://www.e-bezpeci.cz/index.php/temata/sexting/923-pro-vlastne-deti-realizuji-sexting>
10. E-Bezpečí [online]. [cit. 1. 3. 2018]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>
11. iDnes.cz. [online]. [cit. 11. 2. 2018]. Dostupné z: <http://www.zpravy.idnes.cz/smrt-zneuctene-polske-studentky-zacal-resit-soud-fvu-/zahranicni.aspx?c=A070517_164440_zahranicni_adb>
12. Instagram.com [online]. [cit. 28. 2. 2018]. Dostupné z: <http://help.instagram.com/478745558852511>
13. Instagram.com [online]. [cit. 28. 2. 2018]. Dostupné z: <http://www.instagram.com/about/us/>
14. Klinika adiktologie 1. LF UK a VFN v Praze [online]. [cit. 15. 1. 2018]. Dostupné z: <http://www.poradna.adiktologie.cz>
15. Krajské listy [online]. [cit. 6. 3. 2018]. Dostupné z: <https://www.krajskelisty.cz/stredocesky-kraj/17890-pripojeni-krymu-k-rusku-je-legalni-tvrdi-pravnici-evropske-unie-skonci-tedy-sankce-patecni-komentar-stepana-chaba.htm>
16. LinkedIn.com [online]. [cit. 28. 2. 2018]. Dostupné z: <https://about.linkedin.com/cs-cz>
17. Manipulátoři.cz [online]. [cit. 6. 3. 2018]. Dostupné z: <http://manipulatori.cz/hoax-pravnici-eu-prokazali-ze-vstup-krymu-ruske-federace-roce-2014-proveden-souladu-se-zakony/>
18. Microsoft.com [online]. [cit. 28. 2. 2018]. Dostupné z: <https://news.microsoft.com/2016/06/13/microsoft-to-acquire-linkedin/#sm.00000b7idtbygdtjwcl1kxxr4mvby>

19. Ministerstvo vnitra České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.mvcr.cz/cthh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx>
20. Ministerstvo vnitra České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.mvcr.cz/clanek/reakce-ministra-vnitra-na-vyroky-tomia-okamury.aspx>
21. Národní informační centrum pro mládež [online]. [cit. 20. 2. 2018]. Dostupné z: <http://www.nicm.cz/sikana-charakteristika>
22. Národní centrum bezpečnějšího internetu [online]. [cit. 12. 1. 2018]. Dostupné z: <http://www.ncbi.cz>
23. Oxford Dictionaries [online]. [cit. 28. 2. 2018]. Dostupné z: <http://en.oxforddictionaries.com/definition/selfie>
24. Pinterest.com [online]. [cit. 5. 3. 2018]. Dostupné z: <https://newsroom.pinterest.com/en/post/celebrating-the-200-million-people-of-pinterest>
25. Policie ČR [online]. [cit. 28. 2. 2018]. Dostupné z: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>
26. Policie České republiky [online]. [cit. 3. 3. 2018]. Dostupné z: <http://www.policie.cz/clanek/modra-velryba.aspx>
27. Policie České republiky [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.policie.cz/clanek/vyjadreni-k-internetove-hre.aspx>
28. Seznam se bezpečně [online]. [cit. 12. 1. 2018]. Dostupné z: <https://www.seznamsebezpecne.cz/o-projektu>
29. SPD.cz [online]. [cit. 5. 3. 2018]. Dostupné z: <http://www.spd.cz/novinky/tomio-okamura-cr-hrozi-teroristicke-utoky>
30. Statista.com [online]. [cit. 6. 3. 2018]. Dostupné z: <https://www.statista.com/statistics/545967/snapchat-app-dau/>
31. Ústav zdravotnických informací a statistiky ČR [online]. [cit. 15. 1. 2018]. Dostupné z: <http://www.uzis.cz/zpravy/upravena-verze-mkn-10>

Legislativní dokumenty

1. ČESKO. Zákon č. 40/2009 ze dne 8. ledna 2009 Zákon trestní zákoník. Dostupné také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy>

Seznam tabulek a grafů

Tabulky

Grafy

Seznam obrázků