

Vybrané aspekty bezpečnosti na sociálních sítích

Chris Horváth

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Chris Horváth
Osobní číslo: A22218
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Vybrané aspekty bezpečnosti na sociálních sítích
Téma práce anglicky: Selected Aspects of Security on Social Networks

Zásady pro vypracování

1. Uvedte základní terminologii související s tématem práce.
2. Rozeberte nejpoužívanější sociální sítě a hrozby s nimi spojené.
3. Diskutujte konkrétní případy, kdy došlo k poškození.
4. Zaměřte se na bezpečnost a na rizikové chování na sociálních sítích.
5. Vytvořte návod k bezpečnému chování.

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

Seznam doporučené literatury:

1. KOPECKÝ, Kamil a KREJČÍ, Veronika. *Sociální sítě – úvod do problematiky*. Online. Vydavatelství univerzity Plackého, 2023. ISBN 978-80-244-6370-4. Dostupné z: https://vupshop.cz/cs/domu/2887-2579-socialni-site-uvod-do-problematiky.html#/51-format-e_kniha_pdf. [cit. 2024-09-27].
2. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.
3. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
4. KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
5. GOLDSMITH, Jack L. a WU, Tim. *Kdo řídí Internet?: iluze o světě bez hranic*. Praha: Dokořán, 2008. ISBN 978-80-257-0044-0.

Vedoucí bakalářské práce: **prof. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**
Termín odevzdání bakalářské práce: **2. června 2025**



doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Táto bakalárska práca sa venuje vybraným aspektom bezpečnosti na sociálnych sieťach. V teoretickej časti je rozpracovaný vplyv psychologických javov ako FOMO, dopamínová slučka, parasociálne vzťahy či manipulácia pozornosti. Ďalej sú analyzované bezpečnostné hrozby vrátane sociálneho inžinierstva, phishingu, únikov údajov, ako aj monetizačné stratégie platforiem a ich algoritmické fungovanie. Súčasťou práce je aj pohľad na šírenie dezinformácií a regulačné výzvy v kyberpriestore. Praktická časť sa venuje identifikácii a analýze rizík spojených so sociálnymi sieťami prostredníctvom použitia analýzy metód. Práca zdôrazňuje význam kritického myslenia, zodpovedného správania a ochrany súkromia v kyberpriestore. Zároveň ponúka odporúčania na zvýšenie povedomia o bezpečnostných hrozbách a efektívnych opatreniach na ich minimalizáciu. Cieľom práce je komplexne zhodnotiť výhody a riziká používania sociálnych médií a poukázať na potrebu digitálnej gramotnosti a prevencie v online prostredí.

Kľúčové slová: bezpečnosť, dezinformácie, manipulácia, ochrana osobných údajov, psychologické dopady, riziká, sociálne siete.

ABSTRACT

This bachelor thesis focuses on selected aspects of security on social networks. The theoretical part elaborates on the influence of psychological phenomena such as FOMO, the dopamine loop, parasocial relationships, and attention manipulation. Furthermore, security challenges are analyzed, including social engineering, phishing, data leaks, as well as platform monetization strategies and their algorithmic functioning. The thesis also includes a look at the spread of disinformation and regulatory challenges in cyberspace. The practical part is devoted to the identification and analysis of risks associated with social networks. The thesis emphasizes the importance of critical thinking, responsible behavior, and privacy protection in the online environment. At the same time, it offers recommendations for raising awareness of security threats and effective measures to minimize them. The aim of the thesis is to comprehensively assess the benefits and risks of using social media and to highlight the need for digital literacy and prevention in the online environment.

Keywords: Manipulation, Misinformation, Personal Data Protection, Psychological Impacts, Risks, Security, Social Networks.

Rád by som sa poďakoval pánovi profesorovi Ing. Martinovi Hromadovi, Ph.D. za všetky podnety, pripomienky a myšlienky, s ktorými ma počas celej práce obohacoval, smeroval a sprevádzal.

Prehlasujem, že odovzdaná verzia bakalárskej/diplomovej práce a verzia elektronicky nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČÁST	11
1 SOCIÁLNE SIETE	12
1.1 DEFINÍCIA SOCIÁLNYCH SIETÍ.....	12
1.2 SOCIÁLNE SIETE V KONTEXTE MODERNEJ KOMUNIKÁCIE	13
1.3 TYPY SOCIÁLNYCH SIETÍ A ICH ROLA V ŠÍRENÍ INFORMÁCIE.....	17
1.4 POPULARITA SOCIÁLNYCH SIETÍ	21
1.5 SPRÁVANIE UŽÍVATEĽOV NA SOCIÁLNYCH SIEŤACH	22
1.6 PSYCHOLOGICKÉ DOPADY SOCIÁLNYCH SIETÍ	27
1.7 OBCHODNÝ MODEL SOCIÁLNYCH SIETÍ.....	34
2 VYBRANÉ BEZPEČNOSTNÉ HROZBY NA SOCIÁLNYCH SIEŤACH A ANALÝZA RIZÍK.....	38
2.1 MANIPULÁCIA	39
2.2 REGULAČNÉ MECHANIZMY A CENZÚRA NA SOCIÁLNYCH SIEŤACH	43
2.3 HOAXY A DEZINFORMÁCIE	44
2.4 NEBEZPEČNÉ SPRÁVANIE UŽÍVATEĽOV NA SOCIÁLNYCH SIEŤACH.....	46
2.5 ÚNIK INFORMÁCIÍ.....	49
2.6 METÓDY ANALÝZY RIZÍK	62
3.1 OCHRANA OSOBNÝCH ÚDAJOV NA SOCIÁLNYCH SIEŤACH	72
II PRAKTICKÁ ČÁST.....	80
5.1 METÓDA CARVER.....	83
5.2 MODIFIKOVANÁ METÓDA FMEA/PNH.....	88
5.3 METÓDA KARS	91
6 SYNTÉZA VYBRANÝCH RIZÍK NA SOCIÁLNYCH SIEŤACH A NÁVOD K BEZPEČNÉMU SPRÁVANIU SA	107
ZÁVER	113
ZOZNAM POUŽITEJ LITERATÚRY	114
ZOZNAM OBRÁZKOV	126
ZOZNAM TABULIEK	127
ZOZNAM GRAFOV	129
ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	130
ZOZNAM PRÍLOH.....	132

ÚVOD

Sociálne siete sa stali neoddeliteľnou súčasťou každodenného života modernej spoločnosti. Od svojho vzniku priniesli radikálne zmeny v spôsobe, akým ľudia komunikujú, zdieľajú informácie a vytvárajú sociálne väzby či každodenné žijú. Zároveň však so sebou priniesli množstvo výziev, ktoré súvisia najmä s otázkami súkromia, bezpečnosti, psychologických dopadov a šírenia dezinformácií. Vzhľadom na ich rastúci význam a vplyv je potrebné venovať im pozornosť nielen z technického, ale aj z psychologického a sociologického hľadiska.

Táto bakalárska práca sa zameriava na analýzu vybraných aspektov bezpečnosti na sociálnych sieťach. Cieľom práce je identifikovať hlavné riziká, ktoré tieto platformy predstavujú pre svojich používateľov, a zároveň navrhnúť odporúčania na zvýšenie ich povedomia o bezpečnosti. Teoretická časť práce poskytuje systematický prehľad problematiky sociálnych sietí a ich významu v dnešnej spoločnosti. Obsahuje definície a klasifikácie sociálnych sietí, analyzuje ich vplyv na súčasnú komunikáciu a medziľudské vzťahy, ako aj ich úlohu pri šírení informácií. Skúma aj vybrané aspekty bezpečnosti - najmä manipuláciu, šírenie dezinformácií a únik citlivých údajov. V texte je aj zahrnuté posudzovanie psychologického vplyvu používania sociálnych platforiem, najčastejšie mýty spojené so sociálnymi sieťami a ich vplyv vo verejnej sfére. Náplňou praktickej časti je identifikovať, zanalyzovať jednotlivé vybrané riziká a následne ponúknuť súbor odporúčaní a návrhov na zvýšenie bezpečnosti a ochrany súkromia v kyberpriestore.

I TEORETICKÁ ČÁST

1 SOCIÁLNE SIETE

Základným problémom otázok bezpečnosti na sociálnych sieťach je nízka vzdelanosť v oboch oblastiach. Či už ide o oblasť bezpečnosti na Internete samotnom alebo v oblasti informovanosti o sociálnych sieťach. Ľudia ich používajú denne, ale často si ani neuvedomujú, čo sociálna sieť už je. Dôsledkom toho sa stráca aj vedomosť ako sú informácie, ktoré zdieľame ľahko zneužiteľné v neprospech ľudí, ich užívateľov.

1.1 Definícia sociálnych sietí

Na Internete sa dajú nájsť rôzne definície sociálnych sietí, všetky však majú viacero bodov spoločných, ale zároveň aj nesprávne alebo nepresné označenia. Niektoré tvrdia, že sociálne siete sú platformy alebo webové služby, či v jednoduchosti len komunikačné kanály a niektoré definície sa takému zaradeniu úplne vyhýbajú a hovoria o nich len ako o webovej stránke.

Problém vzniká aj v kontexte faktu, že sociálne siete samé o sebe zvyknú tvoriť vlastné definície, ktoré môžu miasť alebo zakrývať samotné nebezpečenstvo, ktoré na sieťach môže vzniknúť. Pre príklad, Wikipédia sa tiež radí medzi sociálne siete, ale ponúka vlastnú definíciu. Paradoxom ostáva, že práve daný článok, ktorý sa venuje problematike o sociálnych sieťach sa považuje podľa samotnej stránky za neúplný a nedostatočný.

Definícia

Vhodnou definíciou sa stáva na základe získaných informácií z rôznych zdrojov:

Sociálne siete sú online platformy alebo aplikácie, ktoré umožňujú užívateľom tvoriť a zdieľať obsah, komunikovať, budovať sociálne vzťahy a vytvárať komunity. Ide o digitálne priestory, kde jednotlivci alebo organizácie môžu zdieľať svoje záujmy, informácie a skúsenosti. [1][2][3]

Terminologické upresnenie

V práci sa používa pojem sociálne siete v širšom význame, pod ktorý spadá aj koncept sociálnych médií. Pod týmto označením sa nejde výlučne o platformy umožňujúce zdieľanie obsahu, interakcie a komunitnú tvorbu, medzi ktoré napríklad patrí YT(Youtube), Tiktok, Reddit alebo Pinterest.

Vzhľadom na praktickú orientáciu práce a všeobecné rozšírenie tohto označenia vzniklo rozhodnutie pre používanie výrazu sociálne siete ako zastrešujúci pojem. Všetky zmienky o „sociálnych sieťach“ v texte preto odkazujú na tento širší význam.

[6][4][5][6]

1.2 Sociálne siete v kontexte modernej komunikácie

Aj keď evolúcia ľudského druhu prebieha neskutočne pomaly k dĺžke ľudských životov a minimálny progres dosiahneme v priebehu pár desať tisícoch rokov, za posledných 30 rokov ľudstvo pokročilo v oblasti technológie neskutočne rýchlo. Rovnako tak sa neustále mení náš jazyk, ktorý sa musí prispôbiť novým predmetom výroby alebo k snahe ľudstva byť, čo najviac efektívny a šetriť náš drahocenný čas. [7]

Informácia, že sa spôsob samotnej komunikácie mohol v priebehu desaťročí zmeniť natoľko, že keby sa čas vrátil o 30 rokov a človek, ktorý vtedy žil uvidí, ako sa komunikuje dnes úplne bežne pomocou mobilných telefónov a bezdrôtového internetového pripojenia, bol by šokovaný, aj keď súčasnému ľudstvu príde tento pokrok úplne prirodzený. Hlavne pre mladšie generácie, ktoré rástli, spolu s technológiami. Pre nich nebol objav a nové inovácie ničím prelomovým, skôr ničím, čo prichádza, keď dosiahnu určitý vek. Je až ťažké uveriť, ako rýchlo sa technologický pokrok uchytil – stačilo drobné vylepšenie a behom niekoľkých rokov sa rozšíril medzi ľuďmi tak prirodzene, až to pôsobí ako zázrak. Dá sa usudzovať, že otázka či ide o dar alebo prekliatie je na mieste, keďže ľudský mozog nebol vytvorený na toľké stimuly, ktoré vytvárajú až nezdravo vysoké hodnoty hormónu dopamínu. Vynálezom sociálnych sietí ide síce o veľkú pomoc v rôznych škálach a miestach a vo veľa smeroch, avšak rovnako dochádza aj k presýteniu a možnému vzniku rôznych psychických problémov z celého spektra dôvodov. Mať hojnosť sa nerovná aj byť v lepšej psychickej pohode. [7]

Zmena tradičných komunikačných modelov

a) Od jednosmernej komunikácií k interaktivite

Pod pojmom tradičných médií sa dá vnímať televíziu, rozhlas, rádio alebo tlač, ktoré boli založené na modeli jednosmernej komunikácie. Daný model funguje na princípe - publikum pasívne prijíma informácie. Avšak sociálne siete nám ponúkli model, v ktorom máme na výber či budeme len absorbovať alebo budeme aj samotnými tvorcami obsahu. [8];[9]

b) Komunikácia je demokratizovaná

Daný bod sa netýka možnosti zdieľať čokoľvek, čo užívatelia chcú bez ohľadu na následky, ale poukazuje práve na možnosť stať sa tvorcom obsahu, ktorý bude na sieťach zdieľaný. Informácie v dnešnej dobe môže zdieľať ktokoľvek, ak neporušuje základné pravidlá komunity. Práve v tomto smere sa objavuje veľa nevýhod. [8][9]

Rýchlosť a okamžitosť komunikácie

a) V reálnom čase

Jedným z najväčších prínosov, ktoré so sebou vynález sociálnych sietí priniesol, je schopnosť okamžitého zdieľania informácií a spojenia s užívateľmi v reálnom čase bez ohľadu na geografickú polohu alebo časové pásmo, v ktorom užívatelia práve prebývajú. Ide o zefektívnenie osobnej a profesionálnej komunikácie v takmer všetkých smeroch. [10]

b) Šírenie správ virálnym spôsobom

Obsah na sociálnych sieťach sa môže šíriť bleskovou rýchlosťou. Avšak nielen, keď ide o pozitívne správy, ale platí to aj pre negatívne. Následky takéhoto zdieľania môžu byť naozaj mocné, pretože virálne príspevky majú poväčšine veľký dopad na verejnú mienku. [11]

Premena medziľudskej komunikácie

a) Digitalizácia medziľudskej komunikácie

Sociálne siete umožňujú ľuďom zostať spolu v kontakte bez ohľadu na časové a priestorové obmedzenie. Avšak, objavuje sa týmto automaticky aj negatívum – strata osobného rozmeru komunikácie. Neverbálnu komunikáciu, medzi ktorú patrí výraz tváre, tón hlasu, gestá, postoj, atď. nahradzujú emotikony. Ak vôbec sú v takomto type komunikácie použité. Nie sú podmienkou. [12]

b) Rozdelenie verejnej a súkromnej sféry

Na sociálnych sieťach sa vie veľmi ľahko stratiť hranica medzi súkromím a verejným životom. Ľudia zdieľajú informácie s ďalšími ľuďmi, ktorým by naživo pravdepodobne dané veci neukázali a ani nepísali. Stráca sa tým bezpečie, ktoré by im v meatspace v skupine medzi takýmito ľuďmi nechýbalo. [13]

Vplyv na psychiku a sociálne väzby

a) Sebavyjadrenie

Na sociálnych sieťach existuje príležitosť si vytvárať svoju digitálnu identitu. Častokrát nejde o pravdivé zobrazenie. Ľudia majú v povahe si profil upravovať a vytvárať, aby pôsobili v lepšom svetle, čo môže vytvárať rôzne psychické ťažkosti.

Taktiež môžu ľudia dávať na siete len, čo chcú, aby videli ostatní užívatelia a teda zdieľaný obsah je len jedna ich stránku, časť, ktorá môže viesť k mylnej predstave o tom aké úžasné životy žijú, pri tom tiež majú svoje nedokonalosti a nevyriešené veci vo svojom živote. [14]

Ak na základe týchto profilov vznikajú vzťahy medzi jednotlivými užívateľmi, môže ísť o veľmi neúprimné väzby vytvorené na falošných domnienkach a informáciách, čo opäť spôsobuje neželané psychické problémy a rôzne komplikácie do budúcnosti.

b) Závislosť

Závislosť sa prejavuje konkrétne k potrebe byť neustále online, aby užívateľ nezmeškal nejakú udalosť alebo interakciu. Tento druh závislosti nesie pomenovanie FOMO (Fear of Missing Out). Človeku potom uniká meatspace priamo pred očami, ale viac sa strachuje o to, aby mu neušiel ten virtuálny priestor.

Avšak dané FOMO sa viaže aj k obsahu, ktorý tam užívatelia zdieľajú. Ak tam zdieľajú mnohí, že boli napríklad na dovolenke či koncerte, konzument obsahu môže pociťovať FOMO, lebo má pocit, že zmeškal niečo na čom musel byť a prišiel oveľa. Nemusí ani ísť o zážitky, ktoré by mu skutočne chýbali alebo ich chcel niekedy zažiť, ale jedinca požíra pocit, že ostatní „viac“ žijú život ako dotýčny. Tieto situácie môžu oslabiť medziľudské vzťahy na rôznych frontoch. Či už vytvoria negatívne emócie voči tým, čo zažívajú tie fantastické zážitky alebo neustála online aktivita berie čas, ktorý môžu užívatelia tráviť v reálnom svete. [15]

Role sociálnych sietí vo verejnom priestore

Okrem užívania sociálnych sietí pre vlastné potreby – zábavu, kontakt s ľuďmi majú sociálne siete rolu aj v ďalších odvetviach:

a) Sociálne siete ako nástroj politickej a občianskej angažovanosti

Poskytujú platformu pre organizáciu protestov, kampaní, petícií a iných foriem politickej aktivity. Príkladom sú politické hnutia ako „Arabská jar“, zvolávanie na pochody politikmi či ľuďmi zainteresovanými v politike alebo klimatickými hnutiami, ktoré využívajú silu online komunity k mobilizácii veľkých skupín ľudí. [16]

b) Sociálne siete a žurnalistika

Okamžité zdieľanie informácií vytvára možnosť získať okamžité správy. Často krátke a výstižné a nie dvojstranové stránky v novinách plné „zbytočných“ informácií. S touto situáciou sa však aj vynára otázka spoľahlivosti zdrojov a šírenie neoverených informácií. [17]

Komunikácia vo firemnom prostredí

a) Firemný marketing a budovanie značky

V dnešnej dobe sú sociálne siete kľúčovým nástrojom pre komunikáciu medzi firmami a ich zákazníkmi. Ak si firma vytvorí osobný vzťah so zákazníkom, je väčšia pravdepodobnosť, že jej služby využije v budúcnosti znovu. Preto sa snažia zamestnanci firmy komunikáciu a svoju značku spríjemniť ako je to možné. Stály zákazník je príjemnejší pre biznis ako príležitostný. [18]

b) Krízová komunikácia

V prípade krízových situácií (napr.¹ produktového zlyhania alebo kontroverzie) môžu sociálne siete slúžiť ako efektívny kanál pre rýchlu reakciu a komunikáciu s verejnosťou. K upokojeniu a vyjadreniu sa k situácii môže stačiť len jeden status na Facebooku.[19]

Sociálne siete zásadne zmenili spôsob komunikácie medzi ľuďmi. Zjednodušili prístup k informáciám vo všetkých smeroch, umožnili okamžitú a multimediálnu komunikáciu a stali sa nástrojom pre sebavyjadrenie a sociálne interakcie. Zároveň však priniesli výzvy súvisiace so súkromím, manipuláciou a šírením dezinformácií. Vplyv sociálnych sietí na modernú komunikáciu je preto obojstranný - ponúka nové príležitosti, ale aj nové riziká. Môže sa hovoriť o tom ako sa komunikácia zefektívnila a zrýchlila, avšak zároveň sa komunikácii v meatspace nič nevyrovná.

¹ Napríklad

1.3 Typy sociálních sítí a ich rola v šíření informácie

Jeden zo základných problémov užívateľov spočíva v nevedomosti, čo sa za sociálne siete považuje alebo nie. Mnoho z nich si myslí, že medzi sociálne siete patrí len Facebook alebo Instagram, avšak medzi siete sa radia napr. aj chatovacie aplikácie či Youtube.

Osobné sociálne siete

Facebook, Instagram, X:

Charakteristika: Užívatelia môžu vytvárať osobné alebo firemné profily, na ktorých môžu zdieľať príspevky, fotografie, videá a odkazy, ktoré sa dajú následne komentovať alebo sa dá reagovať tzv. (to znamená) *Páči sa mi to*. Tak isto môžu medzi sebou jednotlivci alebo skupiny komunikovať. Orientácia komunikácie smeruje na osobnú interakciu. [10]

Rola v šírení informácií: Na platformách ako Facebook alebo X môžu používatelia ľahko zdieľať správy, články a svoje názory. Vďaka algoritmom sa obsah stáva virálnym, čo môže viesť k rýchlemu šíreniu dôležitých informácií, ale aj hoaxov a dezinformácií. X sa často používa na šírenie aktuálnych správ, zatiaľ čo na Facebooku sa informácie šíria v širších komunitách a prostredníctvom skupín. [10]

Výhody a nevýhody: Výhodou je možnosť rýchlo šíriť informácie a osloviť široké publikum. Nevýhodou je možnosť šírenia neoverených informácií a dezinformácií. Algoritmy, ktoré uprednostňujú obsah s vysokým počtom interakcií, môžu podporovať „informačné bubliny“, v ktorých používatelia vidia len informácie potvrdzujúce ich názory. Nemusí ísť potom o pravdivé informácie, keďže algoritmy sú stavané na princípe získavania finančných ziskov a nie na morálke. [10]

Profesionálne a kariérne orientované sociálne siete

LinkedIn:

Charakteristika: LinkedIn je sociálna sieť zameraná na profesionálne a obchodné účely. Používatelia zdieľajú informácie o svojej kariére, skúsenostiach, zručnostiach a profesionálnych úspechoch. [20]

Rola pri šírení informácií: LinkedIn je predovšetkým platformou na šírenie odborných informácií a obchodných novínok. Slúži ako nástroj na budovanie profesionálnych kontaktov, zdieľanie pracovných ponúk a odborných článkov. Informácie, ktoré sa tu šíria, sa často týkajú pracovných trendov, inovácií a vývoja v odvetví. [20]

Výhody a nevýhody: LinkedIn sa zameriava na špecifické priemyselné a profesijné komunity, čo môže zaručiť vyššiu kvalitu a odbornú hodnotu šírených informácií. Nevýhodou je obmedzený dosah mimo profesionálnej sféry a menej interakcií so širokou verejnosťou. [20]

Siete zamerané na multimediálny obsah

YouTube, TikTok, Pinterest, Twitch:

Charakteristika: Tieto siete sú zamerané na zdieľanie video obsahu. YouTube umožňuje používateľom nahrávať a zdieľať dlhé videá, zatiaľ čo TikTok sa špecializuje na krátke, často zábavné alebo informatívne videoklipy. [21]

Rola pri šírení informácií: Obe platformy sú výkonnými nástrojmi na šírenie vizuálneho obsahu. YouTube sa často používa ako vyhľadávač informačných videí, návodov alebo dokumentárnych filmov. TikTok sa stal nástrojom na šírenie virálneho obsahu, ale aj dezinformácií, keďže videá sa ľahko zdieľajú a sú prístupné širokej verejnosti. Pomocou oboch platforiem môžu influenceri a tvorcovia obsahu ovplyvňovať verejnú mienku a šíriť informácie rýchlym a atraktívnym spôsobom. [21]

Výhody a nevýhody: Nevýhodou je ľahké šírenie dezinformácií, ktoré môžu byť zábavné a rýchlo si získajú pozornosť, aj keď sú nepravdivé alebo nie sú ničím podložené. [21]

Siete pre zdieľanie fotografií a obrázkov

Instagram, Pinterest:

Charakteristika: Tieto platformy sú zamerané na zdieľanie vizuálneho obsahu. Instagram je zameraný jedine na sociálnu interakciu okolo fotografií, krátkych videí a chatov medzi užívateľmi, zatiaľ čo Pinterest sa používa na ukladanie a zdieľanie inšpiratívnych obrázkov a nápadov. [22]

Rola v šírení informácií: Instagram zohráva kľúčovú úlohu pri šírení informácií prostredníctvom influencerov a značiek, ktoré zdieľajú obsah zameraný na produkty, životný štýl a sociálne otázky. Pinterest, hoci je menej interaktívny, slúži ako vizuálny vyhľadávač inšpirácie a nápadov. Rovnako tam užívateľ môže zdieľať aj svoje výtvary. [22]

Výhody a nevýhody: Výhodou je estetický a vizuálne príťažlivý obsah, ktorý dokáže rýchlo upútať pozornosť. Nevýhodou je často povrchný obsah a obmedzený priestor na hlbšiu analýzu alebo diskusiu o zložitých témach. [22]

Mikroblogovacie siete

X, Tumblr:

Charakteristika: Mikroblogovacie siete umožňujú používateľom zdieľať krátke príspevky so zaužívaným názvom tweet, blogový príspevok, ktoré môžu obsahovať text, odkazy, obrázky alebo videá. [23][24]

Rola v šírení informácií: X je obzvlášť účinný na zdieľanie aktuálnych správ a názorov v reálnom čase. Používatelia sledujú rôzne účty a reagujú na aktuálne udalosti prostredníctvom krátkych a rýchlych príspevkov. Twitter sa stal jedným z hlavných zdrojov informácií počas kríz, politických udalostí a verejných diskusií. Tumblr, hoci je menej populárny, podobne slúži ako platforma na krátke a vizuálne príťažlivé zdieľanie obsahu. [23];[24]

Výhody a nevýhody: Výhodou je rýchlosť a možnosť šíriť informácie takmer okamžite. Nevýhodou je obmedzená hĺbka diskusie a možnosť šírenia nepravdivých informácií, keďže na Twitteri sa často rýchlo šíria neoverené správy. [23][24]

Diskusné fóra a komunitné platformy

Reddit, Quora:

Charakteristika: tieto fóra umožňujú používateľom zdieľať textové príspevky a diskutovať o konkrétnych témach. Reddit sa zameriava na komunitné diskusie a zdieľanie informácií, zatiaľ čo Quora je viac zameraná na otázky a odpovede na širokú škálu tém. [1]

Rola pri šírení informácií: Reddit a Quora zohrávajú dôležitú úlohu pri vytváraní komunit, v ktorých sa vymieňajú poznatky, názory a skúsenosti. Používatelia môžu získať informácie, ktoré nie sú bežne dostupné v hlavných médiách a môžu sa zapojiť do diskusií o konkrétnych otázkach. V prípade žiadosti o radu, sú toto správne platformy na využitie. [1]

Výhody a nevýhody: Výhodou je hlbšia úroveň diskusie a možnosť dozvedieť sa viac o konkrétnych témach z rôznych uhlov pohľadu. Nevýhodou je náchylnosť na šírenie dezinformácií, keďže obsah nie je vždy overený a môže ísť len o osobné skúsenosti či domnienky. [1]

Chatovacie siete

WhatsApp, Messenger, Telegram, Signal, Viber, Discord a mnoho ďalších

Charakteristika: Chatovacie aplikácie umožňujú používateľom komunikovať v reálnom čase prostredníctvom textových správ, hlasových hovorov, videohovorov alebo zdieľaním multimediálneho obsahu, pod ktorým berieme do úvahy fotografie, videá a rôzne druhy súborov.

Rola pri šírení informácií:

Uzavreté skupiny a komunity: Tieto aplikácie umožňujú tvorbu skupín a kanálov, kde môžu používatelia šíriť informácie, názory, ale aj dezinformácie.

Rýchlosť komunikácie: Používatelia môžu okamžite zdieľať správy a súbory bez ohľadu na časové pásma, kde sa nachádzajú. Limit je len ich mobilné dátové rozhranie alebo internet.

Špecifické použitie aplikácií: Napríklad Telegram sa často využíva na politické alebo aktivistické kampane, Discord pre komunitné diskusie o hrách, ale aj pre odborné témy. Zvyšné spomínané sú viac-menej osobnými komunikačnými kanálmi.

Výhody:

Rýchlosť a dostupnosť: Informácie sa šíria okamžite, kedykoľvek a kdekoľvek.

Bezpečnosť a anonymita: Šifrovanie (napr. Signal, Telegram) zvyšuje ochranu súkromia.

Flexibilita: Umožňujú organizovať diskusie, posilať súbory alebo streamovať obsah.

Nevýhody:

Riziko šírenia dezinformácií: Uzavreté skupiny a nedostatočne kontrolovaný obsah sú často problémom a dôvodom k nedôvere k získaným informáciám. Na druhej strane ide o rovnakú situáciu ako keď by sa daná skupina stretla v meatspace a komunikovala pospolu na tú istú tému bez toho, aby boli špeciálne vzdelaní v obore.

Zneužívanie anonymity: Môže podporovať nelegálne aktivity alebo koordináciu škodlivých akcií.

Závislosť: Neustála dostupnosť môže viesť k preťaženiu informáciami alebo psychologickému stresu.

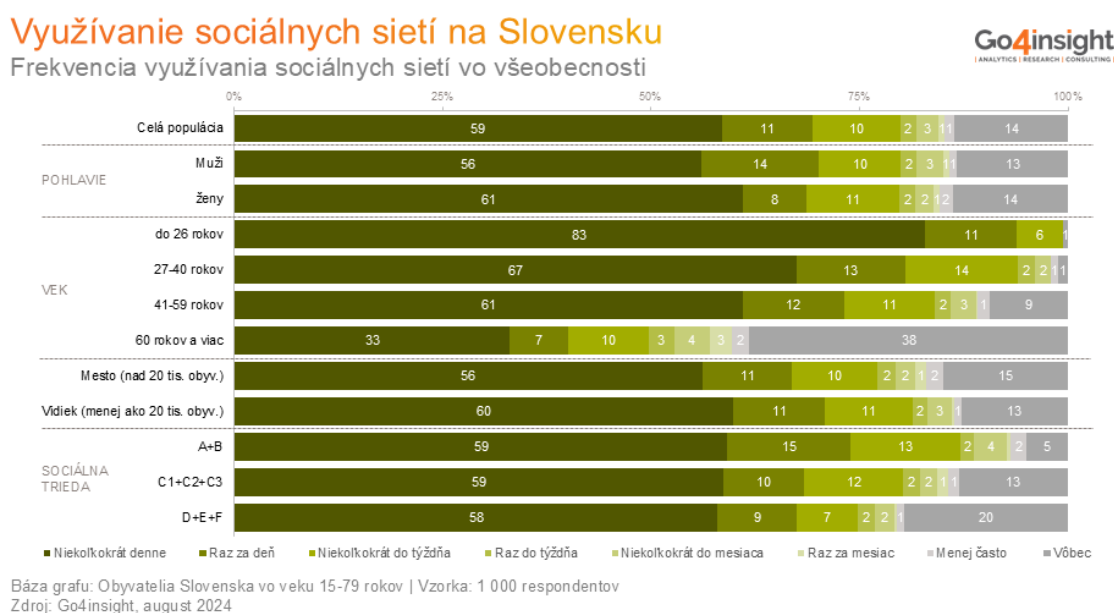
Každý typ sociálnej siete zohráva pri šírení informácií inú úlohu. Niektoré platformy sú výrazne zamerané na okamžité zdieľanie správ a názorov (Twitter), zatiaľ čo iné

poskytujú priestor na zdieľanie vizuálneho obsahu (Instagram) alebo odborných informácií (LinkedIn). Vplyv týchto platforiem na šírenie informácií je obrovský a zahŕňa pozitívne aspekty (rýchlosť, dostupnosť) aj negatívne riziká (dezinformácie, manipulácia).

[25];[26][27][28][25][26][27][28]

1.4 Popularita sociálnych sietí

Sociálne siete sú vo svete veľmi populárne. Dokazuje to aj graf 1, z ktorého až 70% obyvateľov Slovenskej republiky užívajú sociálne siete minimálne raz za deň.



Graf 1 Využívanie sociálnych sietí na Slovensku

(Zdroj:[29])

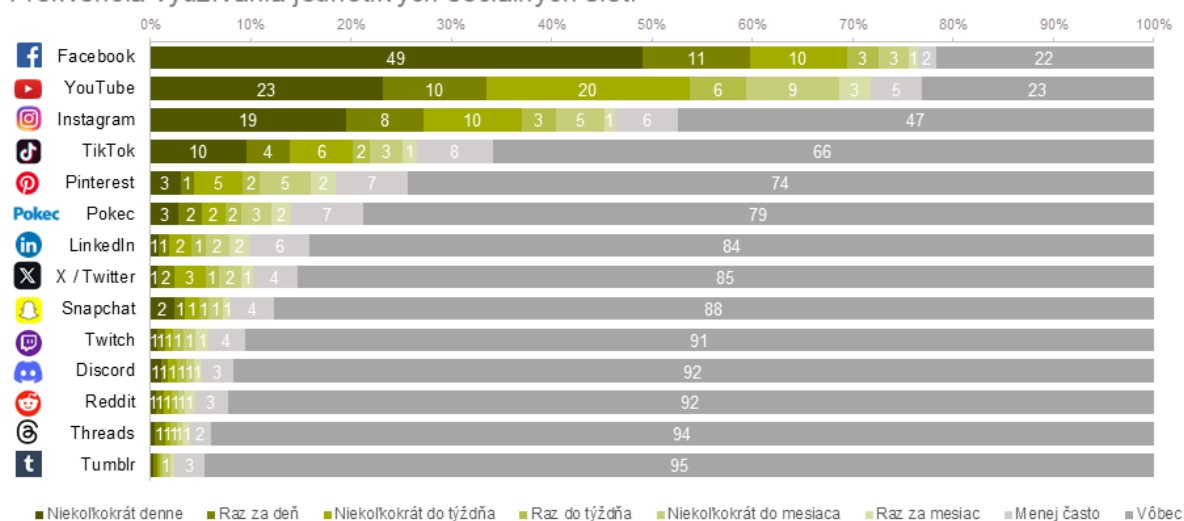
Z grafu 1 je prehľadne vidieť ako 59% slovenskej populácie vo veku od 15 až do 79 rokov, využíva sociálne siete niekoľkokrát denne. Ide o hodnotu ľahko za polovicou, a predsa poukazuje na silnú integráciu sociálnych sietí do života bežných ľudí.

Z grafu 2 sa dá vyčítať častosť využívania jednotlivých sociálnych sietí, z ktorých favoritom sa stáva Facebook. Druhé miesto s vyše o polovicu nižším percentom si nesie Youtube a prvú trojicu ukončuje Instagram.

Využívanie sociálnych sietí

Frekvencia využívania jednotlivých sociálnych sietí

Go4insight
[ANALYTICS | RESEARCH | CONSULTING]



Báza grafu: Obyvatelia Slovenska vo veku 15-79 rokov | Vzorka: 1000 respondentov
Zdroj: Go4insight, august 2024

2

Graf 2 Využívanie sociálnych sietí na Slovensku

(Zdroj:[29])

1.5 Správanie užívateľov na sociálnych sieťach

V dnešnej spoločnosti koluje myšlienka, že sa žije v lenivej dobe, kedy už nie lenže sa menej hýbe, ale ešte menej premýšľa a necháva sa za ľudí uvažovať alebo dokonca rozhodovať. Buď umelou inteligenciou, alebo dokonca hociktorým inteligentným zariadením. Máme vo svojej podstate si veci uľahčovať a čo najmenej sa namáhať, ak je to možné. Avšak v takýchto prípadoch, ako je voľný pohyb po Internete a využívanie všetkých ľahko dostupných možnostiach pre uľahčenie života, ide o vážne riziko zneužitia našich údajov.

Platenie za nehmotné služby

Ľudia užívajú výhody, ktoré sú zdanlivo zadarmo dostupné, pretože si ešte nezvykli platiť za nehmotné produkty. Príde im preto rozumná situácia, v ktorej sa prechádza tisíceky stránok za súkromnými, pracovnými alebo školskými účelmi bez minúty ani koruny. Predsa len si užívatelia platia za internet, potreba platiť pre ďalší obsah súkromníkom, ktorí pre svojich konzumentov vytvorili obsah, ktorý môžu sledovať môže byť nepochopená. [30]

Nehmotné služby na sociálnych sieťach

O to horšie sa vníma, keď sa zrazu na stránke objaví označenie *Len pre predplatiteľov* a konzumenti nemôžu dočítať článok, ktorý ich oslovil ak nie sú ochotní zaplatiť.

Rovnako však ide aj o streamovacie platformy. V mobilnom alebo počítačovom zariadení zmena nastáva – zrazu je udelený prístup do aplikácie, ktorá neplatiteľov nepustila do svojho vnútra, ale môžeme to vnímať len ako súčasť balíka (nášho zariadenia). Vtedy môže dochádzať k nevedomosti a síce, ide o cudziu platformu, aplikáciu, službu, avšak „už sa nachádza“ prístupná v zariadení užívateľa, takže vlastne patrí dotyčnému.

Povinnosť platiť za jednotlivé služby na Internete, je ale prirodzená, keďže ak si chce používateľ prečítať noviny alebo pozrieť TV, musí si zaplatiť. Pri online obsahu je to úplne rovnaké, a predsa na pocit iné.

Keď sa hovorí o nehmotných službách, myslíme digitálne produkty a predplatné služby. Medzi ne patrí platenie za prémiové funkcie, exkluzívny obsah alebo jednoducho len služby, ktoré inak ako po zaplatení nie sú dostupné.

Dané služby a produkty môžu byť YouTube Premium, Twitter Blue, Patreon, alebo spomínané streamovacie služby, alebo mnoho ďalších. Trendy naznačujú vývoj nie k výnimočne platenému obsahu, ale skôr práve naopak. Ak bude niečo bez spoplatnenia k dispozícii, bude to nezvyčajné. Užívateľ bude časom viac peňazí investovať do týchto digitálnych služieb ako do fyzických.

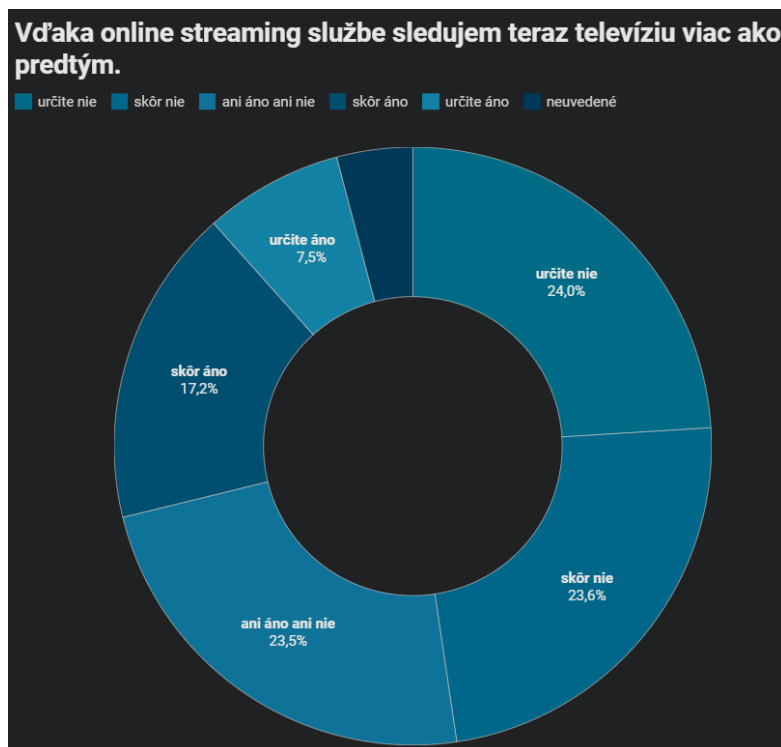
[30][31][32][33][34][35]



Obrázok 1 Štruktúra globálnych investícií do obsahu

Zdroj: [34]

Obrázok 1 nám poukazuje na trendy postupného rastu predplatenia streamovacích služieb, zatiaľ čo dochádza k malému poklesu predplatného za televízne vysielanie.



Graf 3 Sledovanie streamovacích platforiem
a dopad na sledovanie TV (2022)

(Zdroj:[36])

Z grafu 3, na ktorom sú vyobrazené záujmy ľudí o streamovacie služby oproti televízii môžeme vidieť, že odpovede sa držia približne v rovnakej rovine, ale predsa len prevažuje odpoveď, ktorá naznačuje úpadok záujmu o sledovanie televízií ak už ste majiteľom digitálnej streamovacej služby. [36]

V neposlednom rade sa nesmie zabudnúť na platbu, vďaka ktorej si firmy propagujú reklamy alebo influenceri svoj obsah. Vďaka týmto investíciám máme k dispozícii napr. Instagram zdarma, pretože sa zaň platí skrze sledovanie reklám, ktoré môžu užívateľov naviesť na kúpu daného sortimentu či na stiahnutie rôznych aplikácií. Nebyť týchto prvkov, pravdepodobne by daná aplikácia nebola schopná byť dostupná bez spoplatnenia. A toto je práve jeden z negatívnych faktorov, ktorý si jeho užívatelia neuvedomujú, keďže považujú službu za úplne zadarmo. [37][38]

Riziká platenia za nehmotné služby

Riziko, ktoré sa dá vidieť v kúpe nehmotných služieb, často spočíva v ich neprehľadných podmienkach a v mechanizme predplatného, ktorý môže pôsobiť až manipulatívne. Bežným javom je automatická obnova predplatného, pri ktorej sa nám mesačne odpočíta platba za službu – aj vtedy, keď sme ju plánovali zrušiť. Používateľ si chce ešte do konca užiť výhody služby, napríklad prístup k obľúbenému seriálu či hudbe, ale nakoniec na zrušenie zabudne. Táto oneskorená akcia nás môže uväzniť v cykle predplatného, z ktorého je náročné vystúpiť – najmä ak sú kroky k zrušeniu zámerne skryté alebo neintuitívne. Ešte v horších prípadoch, keď ide o platformy, kde si ľudia určujú cenu svojich služieb jednotlivo, natesno si zmenia výšku poplatku a odoberateľ príde o väčšiu finančnú čiastku ako predpokladal. [39][40][41]

Ďalším problémom je závislosť na konkrétnej platforme. Používateľ si síce zakúpi digitálny obsah, ako sú filmy, hry, alebo e-knihy, ale v skutočnosti často nevlastní daný obsah, len dočasný prístup. V praxi to znamená, že ak platforma zmení svoje podmienky, zruší službu alebo konkrétny obsah odstráni, stráca používateľ prístup k tomu, za čo si zaplatil – bez nároku na náhradu. To vytvára asymetriu moci medzi poskytovateľom a spotrebiteľom, ktorú si mnohí neuvedomujú. Je to diametrálny rozdiel oproti minulosti, kedy si jedinec zakúpil CD/DVD (Kompaktný Disk/Digitálny Videodisk) za cenu, ktorú si teraz účtujú digitálne služby. V minulosti vám daný produkt fungoval dokiaľ sa nepokazil, v dnešnej dobe nám patrí len do momentu, pokiaľ sa nezmenia podmienky k užívaniu alebo nevyprší dĺžka predplatného. [42][43][44]

Zároveň je dôležité venovať pozornosť bezpečnosti samotnej platby, najmä pri zadávaní údajov o karte do viacerých streamovacích a digitálnych služieb. V online prostredí existuje vysoké riziko phishingových podvodov, únikov dát, či zneužitia osobných údajov, ktoré môžu viesť k neoprávneným transakciám. Útočníci často napodobňujú oficiálne e-maily od známych platforiem s cieľom vylákať prihlasovacie alebo platobné údaje. [45][46][47]

Tieto riziká sú ešte závažnejšie v kontexte rastúceho využívania digitálneho obsahu mladšími generáciami, ktoré už trávajú výrazne menej času pred klasickými televíznymi obrazovkami. To však neznamená, že zanevreli na obrazovky ako také – len ich spotreba sa presunula na zariadenia so streamovacími službami. Je preto pravdepodobné, že namiesto klasického vysielania budú moderné obrazovky čoraz viac slúžiť ako vstupná brána

k platenému online obsahu, čím sa vyššie uvedené riziká stanú ešte bežnejšou súčasťou digitálneho života. [32][34][35]

Zverejňovanie súkromia

Už od útleho detstva majú ľudia v sebe chuť sa pochváliť, ukázať. Ľudskí jedinci sú veľmi sebestrední a sociálne siete ponúkajú možnosť sa v tomto smere uvoľniť. Užívatelia často žijú v mylnej predstave, že ich profil na sociálnej sieti je miesto, kde si môžu robiť, čo chcú, aj čo sa týka zverejňovania. Aj keď je náročné monitorovať všetko, čo sa na sociálnych sieťach deje, je možné podať trestné oznámenie ak existuje podozrenie, že sa dotýčny dopustil trestného činu. Naopak, ak existujú dôkazy o niekoho vine, nie je s právnym poriadkom v poriadku ich zverejňovať na sociálnych sieťach, lebo stratia svoju vážnosť a nebudú môcť byť použité pri súde ako riadne dôkazy. [48][49]

Najviac túto nevedomosť ohľadom „užívateľ si môže robiť na svojom profile, čo chce, lebo je jeho vlastníkom“ môžeme pozorovať na generáciách, ktoré s mobilným telefónom nevyrástli, ale učili sa s ním narábať. Títo ľudia si dosť často neuvedomujú, že ak si nenastavia súkromný profil, k ich obsahu sa dostane skutočne ktokoľvek. Ak vie ich užívateľské meno, tak dokonca aj človek, ktorý nemusí práve byť registrovaný na danej sociálnej sieti. A potom z opačnej časti spektra – keď si dotýční myslia, že ich nastavenie súkromného profilu skutočne bude chrániť pred ostatnými účtami či samotným digitálnym priestorom. [48][49]

Problém nemusí byť v otázke legality ich príspevkov, ale skôr v tom, koľko toho zo svojho života sú schopní publikovať. Ak pridávajú pravidelné fotky, najlepšie so zdieľanou polohou, môžu byť ľahkou obeťou únoscov – ak sa prezentujú na svojom profile s dieťaťom alebo pre zlodějov, keď zverejňujú obsah v súčasnom čase, kedy sú na dovolenke. Vykradnutý dom počas toho ako rodina vyrazila na dovolenku nie je žiadna anomália. [48][49][50][51]

Základný mýlnik neúspechu spočíva v myšlienke súkromia. Ak niekto z dotýčných si neuvedomuje, čo spôsobí zverejnenie svojho príspevku na svojom profil verejne, môže dôjsť k škodám, ktoré by sa v skutočnom živote nikdy nestali. Napríklad, niekto zverejní na svojom profile fotku seba v nemocnici po chýlostivej operácii s domnienkou, že svojím sledovateľom dáva informácie o svojom živote. Sledovateľov skutočne môže byť len hŕstka jeho najbližších, ale dané veci môže uvidieť desiatka ďalších ľudí. [48][49][50]

1.6 Psychologické dopady sociálních sítí

Sociální sítě se stali běžnou součástí každodenního života milionů lidí. Zatiaľ čo ich užívatelia vnímajú poväčšine len tú ponuku množstva výhod, ktorá predstavuje jednoduchú komunikáciu, dostupnosť informácií či nové formy sebakomunikácie - vplývajú aj na ich psychiku rovnako ako všetky ostatné aspekty života. Kvôli častému využívaniu sociálnych sietí sú však ich stimuly ešte intenzívnejšie.[48]

Používanie týchto platforiem totiž nie je len otázkou techniky, ale aj prežívania, emócií a medziľudských vzťahov. Prostredníctvom notifikácií, lajkov, komentárov či vizuálne atraktívneho obsahu neustále stimulujú používateľovu pozornosť a vytvárajú nové formy závislosti a neistoty. [48][52]

Táto kapitola sa preto zameriava na vybrané psychologické javy, ktoré sú s používaním sociálnych sietí úzko späté. Cieľom je pochopiť, ako tieto javy vznikajú, prečo sú také silné.

Dopamínová slučka a závislosť na sociálnych sieťach

O tom ako algoritmy zneužívajú ľudskú psychiku na udržiavanie pozornosti sa v tejto bakalárskej práci píše veľakrát, pretože z hľadiska ľudského zdravia je veľmi dôležité pochopiť, ako veľmi nám scrollovanie na sociálnych sieťach škodí ak je neprimerané a neregulované. [48]

Kedy je scrollovanie regulované alebo primerané je ťažké určiť, avšak mať priemerne denne 3 hodiny screentime na Tiktoku medzi tú zdravú mieru určite nepatrí. Priemer z výskumov sa pohybuje práve okolo tohto času. [48][52]

Dopamín je tzv. hormón šťastia, ktorý je zodpovedný za prenášanie informácií medzi jednotlivými nervovými bunkami. Pohoda ľudského jedinca, predovšetkým emocionálna, závisí od tohto hormónu. Pre lepšie pochopenie dôležitosti jeho úlohy, ktorú koná pre ľudský organizmus, netreba vedieť význam všetkých chemických reakcií a biologických procesov, ktoré sa dejú v tele. Staršia generácia má v povahe človeka nedeliť na dve časti – psychiku a telo, avšak dopamín vďaka svojim reakciám v tele zasahuje výrazne do psychiky človeka.[48][54][55][56]

V modernej spoločnosti sa sociálne sítě stali neoddeliteľnou súčasťou životov ľudí. Sú navrhnuté tak, aby neustále ponúkali atraktívny obsah, ktorý predlžuje čas strávený za obrazovkou smartfónu. Každý lajk, nový komentár alebo zdieľanie pôsobí na mozog ako odmena, ktorá spôsobí pocit šťastia. Akurát, odmenu dnes človek dostane za to, že len

potiahol párkrát prstom po obrazovke. Nič prospešné však nespravil a jeho hlava to vie a v tom spočíva súboj medzi nervovou sústavou a ľudským vedomím. Ľudské vedomie rozpoznáva, že odmena vo forme dopamínu neprišla po skutočnej námahe. Tento rozpor môže spôsobovať frustráciu a pocit prázdnoty. [48][53][54][55][56]

Algoritmus sa rýchlo učí a ponúka svojim užívateľom neustále nový obsah, ktorý je pre nich individuálne pritažlivý. Pocit okamžitého uspokojenia z neustále prichádzajúceho obsahu je silný stimul pre mozog. Motivuje ľudí, aby sa opakovane vracali na sociálne siete a kontrolovali ich. Z krátkodobého hľadiska to môže pôsobiť ako neškodné alebo príjemné potešenie vo voľnom čas, ale z dlhodobého hľadiska je to cyklus, ktorý vedie k závislosti. Hlavne ak jedinec začne siahnuť po smartfóne aj mimo voľného času. [48][52][53]

Tento neustály cyklus odmieta a stimulov vytvára tzv. dopamínovú slučku, kde mozog neustále túži po ďalších podnetoch, čo môže viesť k závislosti na sociálnych sieťach. Preto je dôležité si uvedomiť tieto mechanizmy a snažiť sa regulovať čas strávený na sociálnych platformách, aby sa predišlo negatívnym dopadom na duševné zdravie užívateľov. [48][53]

Nadmerné používanie sociálnych sietí sa spája s množstvom negatívnych duševných stavov, vrátane úzkosti, depresie a osamelosti. Nereálne vykreslenie života iných jej užívateľov privádza k skreslenému vnímaniu reality. Sledovanie tzv. „toxického“ obsahu môže vyvolať v človeku nesprávne vnímanie samého seba, navodí pocit menejcennosti, ktorý ho privedie k nespokojnosti s vlastným životom. [48][54][55][56]

Niekomu môže prísť neskutočné, že by sa mohol cítiť zle z pozerania videí, ktoré robia radosť a prinášajú úľavu od dennodenných starostí. Zlom však spočíva v prebytku. Nervový a hormonálny systém človeka nikdy nebol stavaný na také stimuly dopamínom. A keď je niečoho priveľa, väčšinou to znamená negatívne následky. Kedysi ľudia necítili dopamín, ak „nič“ nespravili. V dnešnej dobe sa pociťuje vyššia dávka zakaždým, keď jedinec potiahne prstom po obrazovke a zobrazí sa mu nové video. To potiahnutie prstom je gesto, vďaka ktorému dostane náš mozog také množstvo dopamínu ako ľudia z minulosti, keď úspešne dokončili náročnú prácu. O to viac je častý aj syndróm vyhorenia, keďže existuje väčšia tendencia byť preťažený neustálym prívalom informácií v krátkom čase a zároveň byť ohodnotený vlastne za „nič“. Ľuďom potom chýba schopnosť cítiť skutočnú satisfakciu za úspech ak sa hladina skrze to „nič“ môže rovnať hladine dopamínu

za skutočný úspech. Rovnako však, tak ako pri každej závislosti, po čase treba zvýšiť množstvo dopamínu. [48][54][55][56][57]

Do tejto kategórie sa dá zaradiť aj FOMO. Tento strach ako sa už spomínalo v podkapitole, Vplyv na psychiku a sociálne väzby, v užívateľoch vytvára tlak, aby boli neustále online, aby neprišli o niečo dôležité alebo pre nich zaujímavé. Avšak, pretavuje sa to aj do skutočného života, ak vidia svojich priateľov na sociálnych sieťach ako sa zabávajú v realite, ale oni tam neboli prítomní, aj keď nemali čas a prostriedky. Aspekt ako používateľov ovplyvňuje táto túžba byť vždy všade a informovaný o všetkom, je však oveľa viac problémovnejší v skutočnom živote. Medziľudské vzťahy strácajú svoju silu, emóciu a ľudia skôr zažívajú samotu a túžbu po fyzickom dotyku, prítomnosti niekoho druhého, avšak, keď s tým človekom sú, nevenujú sa jemu, ale mobilnému telefónu. Z tohto kruhu alebo teda slučky je neuveriteľne náročné sa vymotať o to viac, že ak sa o to jedinec pokúsi, bude sa cítiť ešte horšie. Presne ako človek s drogovým deficitom. Všetko však chce čas a ak sa chce užívateľ skutočne oslobodiť, niekde začať musí. Inak to „pravé“ a nie len umelo vytvorené uspokojenie, pomocou sociálnych sietí nikdy nenájde. [15][48][58]

Pretáženie informáciami

Keď užívateľ otvorí Instagram, Tiktok alebo Facebook, vyskočí na neho obrovské množstvo textu, obrázkov či videí, ktoré akoby túžili byť skonsumované niekým. Je to ako keď sa so svojimi neoblúbenými známymi, ktorých človek už nevidel pár rokov, stretne náhodou na ulici a známy mu chce zreferovať všetko, čo sa za ten čas stalo. Niekedy je ten dotýčny celkom zaujímavý a človek ho absolútne hltá s otvorenými ústami, ale po čase sa pretážia receptory a poslucháč už nemáme dobrý pocit z prijímania daných informácií a chce sa z tejto nepríjemnej situácie vymotať. [48][59][60][61]

Táto téma nadväzuje na dopamínovú slučku, keďže priveľké množstvo dopamínu už užívateľovi nerobí takú radosť ako na začiatku. Rovnako však, ako sa vyššie spomínalo – jedinec sa už necíti ani lepšie, keď prisun hormónu šťastia preruší. Dôkazom toho je táto štúdia:

- *„72% ľudí je frustrovaných z hľadania niečoho zaujímavého na sledovanie,*
- *55% ľudí sa cíti byť zahltenými množstvom streamovacích služieb, z ktorých si môže vyberať,*

- 26% strávi viac ako 10 minút hľadaním dostatočne zaujímavého obsahu na sledovanie,
- 44 % zatažuje prepínanie medzi rôznymi aplikáciami s rozdielnym servisom,
- 86% by uvítalo jednu jednoduchú aplikáciu, ktorá by poskytovala viacero potrebných služieb na jednej platforme a takmer polovica z nich (41%) by bola ochotná za ňu aj platiť.“

[62]

Človek je časom oveľa viac prierberčivý v obsahu, ktorý ho zabaví alebo naplní, lebo potrebuje navýšiť úroveň prijímaného dopamínu. [48][59][60]

Nesmie sa aj zabúdať na všetky tie chatovacie aplikácie, ktoré jednotliví užívatelia používajú podľa toho, ktorou im je najpríjemnejšie komunikovať s ďalšími ľuďmi. Aj v takomto prípade by bolo oveľa užitočnejšie, keby existovala jedna aplikáciu, ktorá by zastrešovala všetky chatovacie služby a užívatelia by sa nemuseli trápiť s tým, že určitému človeku neodpísali pár mesiacov, lebo daná konverzácia sa stratila a zapadla pod urgentnejšími chatmi. [48][63]

Sociálne porovnávanie a jeho vplyv na sebavedomie

Na sociálnych sieťach nie je nič nové, ak ľudia nevyzerajú tak isto ako v realite. Takéto situácie zahŕňa pojem catfishing, kedy užívateľ na sociálnej sieti vyzerá diametrálne odlišne oproti svojmu prezentujúcemu sa avataru na sieti. Na sociálnych sieťach máme k dispozícii rôzne filtre, úpravy fotografií, videí alebo aplikácie, ktoré tieto úpravy, zmeny jasu, ostrosti a retušovanie umožňujú. Ak ide o známu osobnosť, napr. ženu, môže to mať negatívny vplyv na ženy, ktoré k nej vzhládajú. Môžu mať pocit menejcennosti, nedostatočnosti, pretože nie sú tak dokonalé ako ona. Z týchto pocitov sa môžu vyvinúť rôzne poruchy príjmu potravy, depresie a úzkosti. [48][64][65]

Muži, ktorým sa ženy takto prezentujú na sieťach môžu mať pocit, že ženy v ich okolí, možno aj tie najbližšie ako ich priateľky či manželky, nie sú dosť dobré a môže dôjsť k problémom v intímnom živote. [48][65]

Problém však nie je len v prezentovaní sa žien na sociálnych sieťach. Rovnaké idealistické prezentovanie je v rovnako škodlivé pre ďalších ľudí ak nie aj pre samotných tvorcov na sieti, keďže robia všetko pre to, aby sa svojim sledovateľom zapáčili. [48][65]

Celý tento problém, kedy realita Instagramu alebo teda kyberpriestoru nie je realitou meatspace, by sa dal pomenovať ako „instagramový efekt“. Rôzne efekty a úpravy vedú k túžbam po estetických úpravách, ktoré sú vo svete dostupné. A aj keď je na každom dospelom jedincovi na vlastnom uvážení či je vhodné alebo nevhodné tieto zmeny podstúpiť či už z psychického alebo zdravotného hľadiska, treba zobrať do úvahy, že možno nebyť práve týchto skreslených videní, nemuselo by dôjsť k takým ťažkým rozhodnutiam. [48][65][66]

Informačné bubliny

Veľmi dôležitou vecou, ktorú si treba uvedomiť pri sociálnych sieťach je, že algoritmus, ktorý vyzerá byť veľmi nevinný a nápomocný je v skutočnosti veľmi nebezpečný. Je schopný posilniť naše presvedčenia a polarizovať tým spoločnosť. Algoritmus nám sľubuje ponúkanie obsahu, ktorý nás zaujíma a ktorý chceme vidieť, avšak s tým prichádza tvrdý úder vo forme informácií len jednej strany a vytvára tzv. informačnú bublinu, kedy je pravdepodobné, že užívatelia budú spoznávať len užívateľov a skupiny užívateľov tvorené ľuďmi uväznenými v rovnakých bublinách. [48][53][61]

Je na mieste pochybovať v tomto smere či ide skutočne o problematickú situáciu ak užívatelia vlastne majú záujem presne o tieto informácie a nie o iné. Nie každý človek je otvorený kritickému mysleniu, ale ak v ľudstve existuje túžba, aby jedinci skutočne nezabudli používať rozum a neverili v hoaxy a dezinformácie, je na mieste, aby sme konzumáciu len jednej strany nepovažovali za tú správnu. [48][53][61]

Algoritmy a inžinieri sociálnych sietí ponúkajú svojim užívateľom po čom ich vnútro túži skrze potahey jednotlivých užívateľov cez obrazovku, dĺžku pozerania sa a preklikol v tzv. stalkovaní iných užívateľov. Aby užívatelia neprepadli sieťam, tak by nemali ťukať na každú ponuku navrhovaného príspevku či mixu, čo im daná sociálna sieť ponúkne. Algoritmus pôsobí ako dobrý sluha, ale v skutočnosti je to zlý pán. Jeho misiou je, aby svojich užívateľov udržal pri obrazovke, čo najdlhšie alebo v najlepšom – aby nikdy neupustili oči od displeju. Ich strávený čas na sieti tvorí peniaze pre jej majiteľov. [8][48][53][61][67]

Jedným z dôvodov, prečo sa dezinformácie šíria v uzavretých online komunitách tak efektívne, je prítomnosť názorovej jednotvárnosti, ktorá vytvára vhodné podmienky na nekritické prijímanie a ďalšie šírenie obsahu. Ako uvádza Castells, nové formy komunikácie v digitálnom prostredí vytvárajú tzv. „reálnu virtualitu“ – priestor, v ktorom sa

mediálny obraz a digitálna realita prelínajú do jednotného zážitku. V takomto prostredí dochádza k rozmazaniu hraníc medzi faktami a fikciou, najmä keď sú informácie zdieľané medzi osobami s rovnakými názormi [8][48][53][61]

Dôležitú úlohu v tomto procese zohrávajú algoritmy sociálnych sietí. Ich cieľom nie je sprostredkovať objektívny alebo vyvážený obraz reality, ale zabezpečiť, aby používatelia trávili na platforme čo najviac času. Z tohto dôvodu je im odporúčaný obsah, ktorý vyvoláva silné emocionálne reakcie – najmä rozhorčenie, šok alebo potvrdenie existujúcich presvedčení. Tak vzniká tzv. efekt spätného zosilňovania: čím častejšie je určitý typ obsahu zobrazovaný, tým viac mu používatelia dôverujú a tým menej ho spochybňujú. Postupne tak dochádza k oslabeniu kritického myslenia a otupeniu vnímania. [8][48][53][61][67]

Podľa Marka Bergena boli platformy ako YouTube nastavené tak, aby ich odporúčacie algoritmy aktívne uprednostňovali kontroverzný alebo extrémny obsah – práve preto, že generoval vyššiu mieru interakcie. V uzavretých komunitách, ktoré sa vyznačujú silnou vnútornou lojalitou a nedôverou voči vonkajšiemu svetu, sa takýto obsah šíri mimoriadne rýchlo a často nadobúda charakter „utajenej pravdy“, ktorú údajne tradičné médiá zatajujú. Aj na Slovensku vznikli v rámci týchto interakcií rôzne dezinformačné a extrémistické skupiny, ktoré fungujú vo vlastnej informačnej bubline a považujú každého, kto má iný názor, za klamára [8][48][53][61][66]

Tieto skupiny zároveň trpia nedostatkom korekčných mechanizmov – často v nich chýbajú osoby, ktoré by predkladali alternatívne pohľady alebo kládli kritické otázky. V dôsledku toho môže dochádzať k uzatváraniu do vlastného informačného priestoru, v ktorom si komunita vytvára vlastnú verziu reality a súčasne odmieta akékoľvek vonkajšie zdroje ako zmanipulované či nepriateľské. [53][61][67]

Príklady z praxe

- a) Počas pandémie COVID-19 (choroba spôsobená koronavírusom) boli vytvorené skupiny odporcov očkovania, ktoré medzi sebou zdieľali dezinformácie o účinkoch vakcín, čipovaní prostredníctvom testovania alebo konšpiračné teórie o pôvode vírusu. V uzavretých skupinách na platformách ako Facebook či Telegram sa tieto názory šíрили bez kontroly, pričom akákoľvek kritika bola označovaná ako „cenzúra“ alebo „propaganda farmaceutických spoločností“ [68][69]
- b) V období amerických prezidentských volieb v roku 2020 vznikli online komunity, ktoré spochybňovali výsledky hlasovania a šířili naratív o údajne „ukradnutých

voľbách“. Tieto skupiny pôsobili najmä na platformách ako YouTube, Parler alebo Reddit, kde sa ich členovia navzájom utvrdzovali vo svojich presvedčeniach. Dôsledkom týchto aktivít bol aj útok na Kapitol 6. januára 2021 [70]

- c) Konšpiračné fóra zamerané na „globálne elity“ a „nový svetový poriadok“ predstavujú ďalšie prostredie, v ktorom sa dezinformácie šíria s mimoriadnou ľahkosťou. V rámci týchto uzavretých komunít sú často vytvárané tzv. „alternatívne fakty“, ktoré síce môžu pôsobiť dôveryhodne pre ich členov, no neobstoja pri vedeckej alebo žurnalistickej verifikácii [71][72]

Parasociálne vzťahy a vplyv influencerov

Sociálne siete vytvorili priestor pre vznik fenoménu tzv. parasociálnych vzťahov – teda jednostranných emocionálnych väzieb, ktoré si používatelia vytvárajú k verejným osobnostiam, najčastejšie k influencerom. Aj keď nejde o obojstranný vzťah, z pohľadu používateľa je prežívaný ako autentický a emocionálne reálny – sledované sú každodenné aktivity influencera, jeho hlas, prejav, názory, a zdieľané sú s ním hodnoty či emócie.[73]

Tieto väzby bývajú posilňované formátmi ako vlogy, live streamy alebo Q&A (otázky a odpovede), ktoré vytvárajú ilúziu osobného kontaktu a blízkosti. Výskumy ukazujú, že parasociálne vzťahy sú najčastejšie nadväzované dospelými a mladými dospelými, ktorí influencerov vnímajú ako vzory, dôverníkov, prípadne náhradu reálnych priateľských vzťahov. [48][73]

Psychologické dôsledky takýchto vzťahov však nie sú zanedbateľné. Jedným z rizík je, keď je sebaobraz používateľa budovaný na základe reakcií influencera alebo prostredníctvom interakcií s jeho obsahom – napríklad cez komentovanie, zdieľanie či posielanie správ. V prípade odpovede influencera dochádza k prehĺbeniu pocitu uznania, čo posilňuje odmeňovací mechanizmus. Naopak, pri nedostatku spätnej väzby môže vzniknúť pocit odmietnutia či menejcennosti – obzvlášť vtedy, keď je daná osobnosť vnímaná ako niekto výnimočný, kto „odmieta“ kontakt. [66][73]

Ďalším problémom sú nerealistické očakávania, ktoré môžu ovplyvniť sebaobraz a duševnú pohodu užívateľov. Život influencerov je zriedkavo prezentovaný autenticky – často ide o skreslený a upravený obraz, ktorý navodzuje dojem ideálneho života. Aj keď mnohí tvorcovia deklarujú snahu byť úprimní a otvorení, kyberpriestor im ponúka len obmedzené možnosti na reálnu seba-prezentáciu. V dôsledku toho dochádza k častému

porovnávaniu vlastného života s digitálnou ilúziou, čo môže viesť k pocitom nespokojnosti, menejcennosti alebo úzkosti [8][73]

Ako upozorňuje aj Castells, v digitálnej spoločnosti vznikajú nové typy identity a emocionálne väzby, ktoré nemusia byť vytvorené zdravo a prirodzene a na základe tohto faktoru trpia aj ich vzťahy v meatspace. Vplyv influencerov sa tak stáva nielen ekonomickým fenoménom (keďže zarábajú na svojich sledovateľoch a motivujú ich si zakúpiť propagované produkty), ale aj kultúrno-psychologickým javom, ktorý má vplyv na hodnoty, postoje a správanie používateľov. [8][73]

Jedným z príkladov silného parasociálneho puta je americká youtuberka a influencerka Emma Chamberlain. Jej štýl komunikácie pôsobí veľmi osobne – vo vlogoch sa prihovára priamo do kamery, ukazuje aj svoje zraniteľnejšie stránky a venuje sa bežným činnostiam ako varenie, cestovanie či trávenie času v aute. Mnohí fanúšikovia uvádzajú, že „majú pocit, akoby bola ich kamarátka“, napriek tomu, že sa s ňou nikdy nestretli. [74]

Emma sa vedome stavia do pozície osobnosti, s ktorou sa dá stotožniť – tým u divákov vytvára pocit blízkosti, aj keď ide len o jednostranný vzťah. V niektorých prípadoch sa však u fanúšikov vyvinula emocionálna závislosť – priznávajú, že sledujú jej obsah v momentoch osamelosti alebo keď cítia potrebu spoločnosti. Keď si Emma dočasne zobrala prestávku od YouTube, mnohí reagovali znepokojením až úzkosťou – pretože stratili „digitálnu kamarátku“ [74]

Tento príklad ukazuje, ako silno môže digitálna prítomnosť ovplyvniť emocionálny svet jednotlivca, najmä v období dospievania. Aj keď ide o jednostranný vzťah, parasociálna väzba vyvoláva u ľudí reálne psychologické reakcie a potreby, ktoré sú bežne spájané s priateľstvom alebo osobným kontaktom.

1.7 Obchodný model sociálnych sietí

Aj keď sa sociálne siete na prvý pohľad javia ako bezplatné nástroje na komunikáciu a zábavu, v skutočnosti ide o sofistikované komerčné platformy, ktorých hlavnou prioritou je zisk. Ich fungovanie je založené na obchodnom modeli, v ktorom sú speňažované pozornosť používateľov, ich osobné údaje a správanie. Každý klik, pohyb prsta po obrazovke, interakcia či zdieľanie predstavujú dátové vstupy pre algoritmy, ktoré sú využívané na zefektívnenie cielenia reklamy a maximalizáciu výnosov. [8][48]

Základom tohto modelu je tzv. ekonomika pozornosti – systém, v ktorom je výhodou schopnosť udržať používateľa online čo najdlhšie. To ovplyvňuje mnohé dizajnové rozhodnutia – od spôsobu zobrazovania obsahu, cez formát notifikácií, až po fungovanie odporúčacích algoritmov. Týmto nastavením sa prirodzene vytvára napätie medzi záujmami platforiem a potrebami používateľov, čo sa môže prejaviť vo forme závislosti, straty súkromia či zvýšenej náchylnosti na manipuláciu. [8][48]

V tejto časti kapitoly je preto odhalený ekonomický mechanizmus, ktorý si mnohí používatelia neuvedomujú, alebo ho vedome ignorujú.

Základné princípy monetizácie

Podľa Manuela Castellsa prechádza globálna ekonomika zásadnou premenou smerom k informačnej ekonomike, v ktorej dominujú dáta, digitálne siete a technologická infraštruktúra. V tomto novom modeli kapitalizmu – označovanom ako digitálny alebo sieťový – sa hlavnými komoditami stávajú informácie, pozornosť a interakcia používateľov. [8][48]

Sociálne siete sú v tomto systéme využívané ako nástroje trhového ovplyvňovania, pretože umožňujú presné cielenie reklám a obsahu na základe spracovania správania používateľov. Každá ich interakcia – označenie „páči sa mi to“, komentár, kliknutie alebo zdieľanie – je premenená na dátový vstup, ktorý slúži na optimalizáciu marketingových stratégií. Sociálne siete tak plnia úlohu nielen komunikačných nástrojov, ale aj výkonných platforiem na generovanie zisku z používateľskej aktivity, pričom si veľká časť používateľov túto skutočnosť neuvedomuje. [8][48]

Castells zároveň poukazuje na to, že sieťové technológie umožnili globalizáciu trhu v reálnom čase – firmy v ňom súťažia o pozornosť používateľa na celosvetovej úrovni. V dôsledku toho sa posilnila hodnota schopnosti zaujať a udržať pozornosť, čo priamo ovplyvňuje dizajn aj monetizáciu platforiem. [8][48]

Z pohľadu používateľa to znamená, že jeho pozornosť sa stáva tovarom, ktorý je speňažovaný prostredníctvom reklám, plateného obsahu a dátovej analýzy. Uprednostňovaný je pritom najmä obsah vyvolávajúci silné emócie – či už pozitívne alebo negatívne – keďže ten zabezpečuje vyššiu mieru interakcie a tým aj väčšie zisky pre platformy. [8][48]

Aj napriek skutočnosti, ktorej užívatelia čelia z hľadiska toho, že ide o literatúru starú 16 rokov, autor už v tom čase varoval pred rizikom, ktoré prinášajú sociálne siete so sebou.

V čom skutočne spočíva ich zloba a po čom túžia. Ešte desivejšou časťou ostáva, že jeho predpoklady sa naplnili a ľudstvo v tomto biznise padlo do slučky, z ktorej je priam nemožné odísť len ju prehľbiť. [8][48]

Čím dlhšie zostanú používatelia pri obrazovkách, o to viac ich z toho budú inžinieri poznať a budú vedieť určiť, ktorý obsah ich tam zdrží, čo najdlhšie. Nočné nezmyselné scrollovanie aj zdanlivo obohacujúceho obsahu nekončí ako pozitívna skúsenosť. Nekvalitný spánok spôsobuje množstvo zdravotných problémov, ktoré sa môžu prejaviť až po rokoch. [8][48]

Ak by ste sa užívateľa spýtali po tom, čo odložil mobil po čo i len pár minútach scrollovaniach o čom bolo posledných 5 videí, bol by úspech ak by vedel povedať aspoň o jednom. O čo viac inžinieri poznajú užívateľa, nie lenže vedia využiť svoje znalosti, aby jedinec zdržali na platforme, ale vedia mu aj podhodiť reklamu, na ktorú pravdepodobne klikne a možno si niečo aj kúpi alebo o tom produkte povie niekomu inému. Z niečoho tie siete byť financované musia. [48][75][76]

Ako sociálne siete generujú zisk

Sociálne siete patria medzi najvýnosnejšie biznis modely súčasnosti. Marketingové stratégie platforiem bývajú často prepracovanejšie než samotné funkcie aplikácie. Základom ich príjmov je model, ktorý speňažuje pozornosť. V princípe – čím dlhšie sa používateľ na platforme nachádza, tým viac reklám mu môže byť zobrazených. Ako uvádza Bergen, hlavným produktom nie je technológia samotná, ale používateľ a jeho pozornosť, ktorá je následne predávaná inzerentom v podobe cielenej a často prispôbenej reklamy. [48][53][61][67]

Algoritmy hrajú v tomto modeli rozhodujúcu úlohu – sú navrhnuté tak, aby maximalizovali čas strávený na platforme odporúčaním obsahu, ktorý vyvoláva silné emocionálne reakcie (napr. šok, pobavenie či rozhorčenie). Tým sa zvyšuje pravdepodobnosť, že používateľ zotrvá online dlhšie, čím sa zvyšuje počet zobrazených reklám. Aj keď sú reklamy vedome ignorované, ich opakované zobrazovanie zanecháva stopu v podvedomí a prispieva k vytvoreniu dôvery voči značke či produktu. [48][53][61][67]

YT ako jedna z najväčších platforiem čelil viacerým kontroverziám v súvislosti so svojím obchodným modelom. Jednou z najvýraznejších bola tzv. Adpocalypse. Išlo o situáciu, keď boli reklamy veľkých značiek spojené s kontroverzným obsahom,

čo viedlo k ich masovému stiahnutiu z platformy. Táto udalosť odhalila zraniteľnosť modelu, ktorý je závislý od automatizovaného spájania reklám s obsahom, a zároveň upozornila na náročnosť moderovania obrovského množstva videí, ktoré sú denne nahrávané. [48][53][61][67]

Kvôli tejto udalosti došlo k sprísneniu pravidiel monetizácie, čo sa zas negatívne ovplyvnilo množstvo youtuberov. Zároveň však začala byť kladená väčšia zodpovednosť na samotné platformy – najmä v súvislosti s tým, aký obsah odporúčajú, zdieľajú a speňajú. [48][53][61][67]

Aj keď sa môže zdať, že sociálne siete sú prístupné zdarma, v skutočnosti ide o jeden z najvýnosnejších a najvplyvnejších obchodných modelov dneška. Neustále inovácie a estetické úpravy nie sú motivované potrebami používateľov, ale snahou o čo najdlhšie udržanie ich pozornosti. Čím viac času je na platforme stráveného, tým vyšší zisk dosahuje spoločnosť, ktorá ju prevádzkuje. Monetizácia však prináša aj zodpovednosť – niektoré platformy sa jej chopili aktívne, iné len čiastočne. [48]

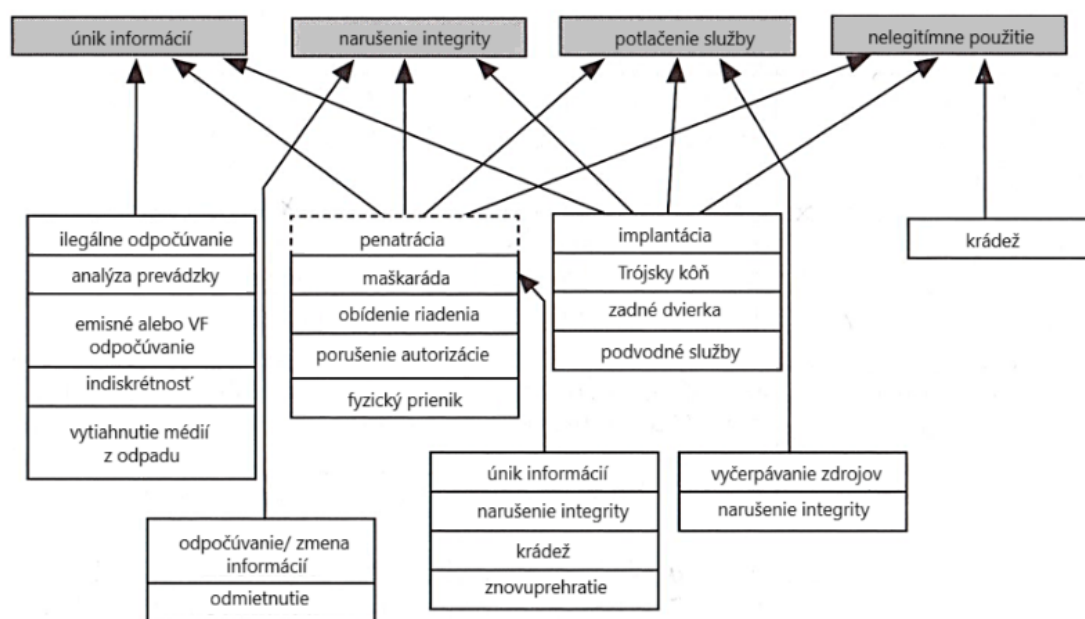
Kapitola poskytuje komplexný pohľad na fenomén sociálnych sietí a ich význam v súčasnej spoločnosti. Analyzuje zmeny v medziľudskej komunikácii, dopady sociálnych sietí na psychiku používateľov, ako aj ich úloha v spoločenskom či firemnom prostredí. Pozornosť je venovaná aj rozdeleniu sietí, ich obľúbenosti, špecifikám používateľského správania – napríklad nechcote platiť za služby alebo rizikómu zdieľaniu osobných údajov. Samostatne sú rozpracované psychologické dôsledky – vrátane závislosti, informačného preťaženia, sociálneho porovnávania, parasociálnych väzieb či efektu informačných bublín. Kapitulu uzatvára rozbor obchodného modelu platforiem, najmä spôsobov monetizácie prostredníctvom reklamy a predaja používateľských dát.

2 VYBRANÉ BEZPEČNOSTNÉ HROZBY NA SOCIÁLNYCH SIEŤACH A ANALÝZA RIZÍK

Pri užívaní Internetu každodenne, môže dôjsť k pravdepodobnej strate opatrnosti. Možno si niektorí užívatelia stále dávajú pozor, aby nezdieľali verejne fotky z dovolenky, na ktorej sa ešte nachádzajú, aby ich neokradol príležitostný zlodej. Určite ale nedávajú taký pozor na algoritmy ako zozáčiarku, kedy museli často byť z neho aj nadšení a skôr si pamätali, čo na Internete videli. Teraz si mnohí užívatelia zapnú TikTok na 5 minút, lebo čakajú na MHD (Mestská Hromadná Doprava) na zastávke. Pravdepodobnosť, že si takýto užívateľ pamätá, čo za tú chvíľu videl vo svojom smartfóne je vážne mizivá. Ale vzniknuté stopy aj tých pár minút sa s nami môžu nieť aj naďalej. [61][75][76]

Podľa autora knihy, *Kybernetická kriminalita*, Václava Jirovského existujú 4 skupiny základných hrozieb:

- a) *„Únik informácií, je stav, kedy dôjde k vyzradeniu chránenej informácie neautorizovanému subjektu.*
- b) *Narušenie integrity, predstavuje poškodenie, zmenu či vymazanie dát.*
- c) *Potlačenie služby, znamená úmyselné bránenie v prístupe k informáciám, aplikáciám či systému.*
- d) *Nelegitímne použitie je použitie informácií neautorizovaným subjektom či neoprávneným spôsobom.“ [77]*



Obrázok 2 Vzájomný vzťah jednotlivých kybernetických hrozieb podľa Jirovského

(Zdroj:[77]; preklad: [vlastný])

2.1 Manipulácia

V meatspace sa ľudom môže veľa krát stať, že budú za život zmanipulovaní a takéto zistenie vedie so sebou mnoho negatívnych emócií a pocitov. Na sociálnych sieťach sa manipulácia deje ešte jednoduchšie, lebo si jej ani nemusia byť ich užívatelia vedomí. Nie je ľahké takýto proces zistiť, lebo tvorcovia sociálnych sietí pracujú s nastavením ľudskej mysle, fungovaním mozgu a sú veľmi vzdelaní ohľadom ľudskej psychiky. Čím menej sa človek pohybuje v reálnom svete, tým viac predáva informácie o svojich návykoch, preferenciách a ako už bolo spomenuté, stáva sa viac závislým na sociálnych sieťach. Posúvanie prstom po obrazovke, čiže scrollovanie, zároveň navyšuje finančné príjmy tvorcom obsahu sociálnych sietí. [48]

Definícia

Manipulácia je zámerné ovplyvňovanie myslenia, správania alebo vnímania iných osôb s cieľom dosiahnuť vlastný prospech. Manipulátor využíva rôzne techniky, ktoré často zahŕňajú zneužívanie dôvery, emócií, naivity či iných pozitívnych vlastností obete. Tento proces môže viesť k tomu, že cieľová osoba prijíma názory, myšlienky alebo konanie, ktoré by inak dobrovoľne neakceptovala, pričom si často ani neuvedomuje, že je manipulovaná. [78][79][80][81][82]

Typy manipulácie

a) Clickbait

Po rokoch čítania dámskych magazínov každý ľudský jedinec súhlasí, že šéfredaktori tie titulné strany zbytočne dramatizujú až prehánajú, ale aj tak si ich zákazníci budú naďalej kupovať, lebo sú zvedaví či naozaj to bude tak ako hovorí titulok. Alebo minimálne zoberú výtlačok v obchode do rúk a prelistujú, aby mohli situáciu overili hneď. Dôvod kúpy, aj keď si zákazník overil, že titulok opäť zveličuje je už ovplyvnený rôznymi psychologickými faktormi ako napr. človeku môže byť nepríjemné čítať tak dlho magazínový článok, keď okolo sa mihajú ľudia. A mnoho ľudí om kvôli určitému sociálnemu statusu a správaniu záleží na tom, čo si o nich iní myslia. A toto môže byť jeden z dôvodov pre kúpu takéhoto časopisu.

Existuje argument, že zákazník nové číslo daného magazínu kúpili kvôli niečomu úplne inému, čo ho zaujalo pri jeho overovaní pravdivosti titulku. Avšak dotyčný vzal do rúk časopis z dôvodu, že ho zaujal titulok a tým sa biznis vydavateľskej spoločnosti vydaril, lebo zaujal prostredníctvom neho a vyhral nad ľudským faktorom.

Vyššie rozoberaný text hovoriaci o zaujímavom avšak nie úplne pravdivom titulku je v podstate definíciou clickbaitu. Vymyslieť pútavý často až prehnaný názov produktu, ktorý tvorca predáva hlavne za účelom, aby pokoril ľudskú slabosť – zvedavosť.

Neznamená to, že daný obsah magazínu, časopisu či novín je škodlivý, nepriateľský alebo negatívny. Pre niekoho môže byť, niekto ho môže milovať. Každému človeku sa páči niečo iné. Myšlienkou však ostáva, ak si daný výtlačok kúpi zákazník v prvom rade kvôli titulku, ide o clickbait v reálnom živote.

Tvorcovia na Internete, sociálnych sieťach, tiež zistili, že získať pozornosť publika, aj keď len na jedno kliknutie im zvýši dosahy, čísla a výnosy. Na YouTube pred pár rokmi vládla éra, kedy pomaly každý tzv. YouTuber ako sa nazývajú tvorcovia na YT, používali clickbaity na svoje videá. Ľudí tento spôsobom prezentovania svojich výtvorov však veľmi rýchlo omrzelo a YouTuberi, ktorí sa touto cestou vydali v očiach svojich fanúšikov strácali relevantnosť a pozitívne ohlasy. Niektorí sa uvedomili a zmenili svoju taktiku, iní ďalej pokúšajú trpezlivosť svojich sledovateľov.

Mnoho tvorcov však naďalej tento spôsob prezentovania uplatňuje, pretože ak spravia tento clickbait poriadne, môže im vyniesť dokonca viac peňazí ako keby sa takémuto prejavu vyhýbali. Na sociálnych sieťach sa často počítajú samotné kliknutia na video alebo článok.

Jedná sa o zhladnutia, ktoré už vynášajú peniaze tvorcom. Avšak, ak fanúšik nepozerá konkrétne video na YT viac ako 30 sekúnd, zhladnutie sa nepočíta a všetka snaha tvorcu o pútavý titulok padá, ak nedokáže sledovateľa zaujať po nasledovnú dobu 30 sekúnd.

[48][84][85]

b) Astroturfing

Astroturfing je praktika, pri ktorej sa umelo vytvára dojem spontánnej podpory alebo pozitívnej recenzie zo strany verejnosti a to s cieľom ovplyvniť verejnú mienku alebo rozhodovanie ľudí.

Táto metóda spočíva v skrytí skutočných sponzorov alebo iniciátorov zverejnených informácií. Napríklad ak ide o politickú kampaň, recenzie na produkt, alebo ideológie, aby komunikácia vyzerala, že pochádza od nezávislých občanov či spotrebiteľov. Avšak môže sa jednať o zaplatených aktérov, ktorí v skutočnosti nemusia súhlasiť s myšlienkou, ktorú šíria, ale kvôli platu sú ochotní sa zúčastniť danej stratégie (marketingového ťahu). Nemusí ísť len o amatérov, ktorí sú zaplatení, aby zakladali blogy, písali recenzie, kde sa pozitívne nakláňajú k danej téme, ale môže ísť aj o profesionálov, ktorí sa týmto spôsobom klamania živia.

[86][87][88]

Konkrétny príklad sa dá uviesť o firme Bell Canada, ktorá nabádala svojich zamestnancov, aby na ich aplikácie v iTunes a Google Play pridávali pozitívne reakcie bez udania vzťahu k spoločnosti, čo však bolo v rozpore so zákonom v súťaži v rámci, ktorej boli súčasťou. Kvôli účasti v súťaži bolo ich daňou za podvod pokuta, avšak astroturfing nie je v bežnom živote právne trestným. [88]

c) Vplyv influencerov

V dnešnej dobe slovo influencer pozná snáď každý. Znamená „ten, čo ovplyvňuje“. V jednoduchosti by sa dalo povedať, že ide o bežného človeka, ktorý nejakým spôsobom - či účasťou v reality show, chodením s niekým známym alebo si v spoločnosti sami vystavali meno svojím podnikaním. [89]

Tento bod sa zameriava na influencerov, ktorí len existujú, objavujú sa po boku iných tvorcov, ale sami tvorcami nie sú. Berú spolupráce, pridávajú fotky, videá alebo príbehy na svoje sociálne siete, ale nevenujú sa k tvorbe iného obsahu ako len prezentovaním svojho života v takej miere, že ich sledovatelia o nich veľa toho ani nevedia. Medzi takýto typ

influencerov patrí napríklad priateľka YouTubera, ktorá sa objavuje v jeho videách, ale inak nie je tvorcom iného obsahu ako len, že má účet na Instagrame a ľudia jej dajú sledovanie, pretože im príde sympatická. Stáva sa influencerkou akonáhle sa okruh jej sledovateľov zväčší natoľko, že firmy majú záujem s ňou spolupracovať a jej prácou je vlastne propagovať produkty daných firiem, s ktorými má zmluvy a je nimi vyplatená. Samozrejme, ak tieto ponuky daná osoba prijme. [73]

Vplyv influencera môže byť veľmi podceňovaný, ale je neskutočne nebezpečný hlavne ak nie je regulovaný morálnymi zásadami. Nie každý influencer má spolupráce a propaguje pozitívne produkty. Pod neškodnou propagáciou môžeme vnímať u tzv. beauty influecerky („tie, čo ovplyvňujú krásu“), ktoré propagujú rôzne značky kozmetiky. Avšak aj tu treba dávať pozor či ide o známu a overenú značku alebo o ich výrobu, na ktorej chcú, čo najviac zarobiť a môže ísť o nekvalitný produkt, čo môže ublížiť. To je najväčšie mínus influencerov vo všeobecnosti. Ich propagácia určitého produktu alebo služieb nezaručuje pozitívny výsledok.

Dobрым príkladom je situácia, keď futbalista Cristiano Ronaldo odložil počas tlačovej konferencie Coca Colu bokom a nahradil ju vodou. Akcie spoločnosti padli o vyše 3 miliardy eur.[90][91]

Vplyv, ktorý majú influenceri nie je niečo, čo by sa malo podceňovať. Sú skutočnou hrozbou, hlavne ak sa začnú medzi nimi hádky a dôjde na tvrdenia proti tvrdeniam a spoločnosť sa začne zbytočne polarizovať. [73]

Reklama cez influencerov má ešte väčšiu moc ako bežná, ktorá neustále sa objavuje v médiách. S influencermi si sledovatelia vytvárajú parasociálne vzťahy, ktoré ich dokážu manipulovať, aby si skôr zakúpili dané produkty, aj keď ich práve nepotrebujú alebo majú overené lacnejšie či kvalitnejšie produkty. Lenže, keďže to odporúča ich obľúbený influencer, tak si to zakúpia. V predchádzajúcej kapitole v sekcii Psychologické dopady sociálnych sietí sa popisovala problematika parasociálnych vzťahov podrobnejšie. [73]

d) Bots a automatizované účty

V poslednej dobe sa pod príspevkami na sociálnych sieťach hromadia rôzne komentáre s nesprávnou gramatikou, erotickou či úplne odlišnou tematikou od príspevku, pod ktorým sa nachádzajú. Ide o profily, ktoré môžu byť napojené na AI (Artificial Intelligence) a sú len vopred naprogramované ako sa majú chovať, ale nie sú reálne spravované ľudskou bytosťou.

Okrem komentárov, môžu aj reagovať *páči sa mi to* na príspevky a vytvárať/šíriť svoj obsah. Môže ísť podporu k šíreniu určitých myšlienok, podobne ako pri astroturfingu alebo len zvýšiť viditeľnosť určitých tém alebo dezinformácií. [92]

Sociálne inžinierstvo

Sociálne inžinierstvo je pojem, ktorý zahŕňa rôzne techniky manipulácie a klamstiev, cez ktoré sa snaží dostať k prístupom k účtom na sociálnych sieťach a materiálom, ktoré užívatelia v kyberpriestore udržiavajú v zdanlivo v svojom súkromí.

Keďže ľudský faktor je vždy bodom zlomu, jedná sa o najslabší článok zabezpečenia. Jednoduchšie ako snaha nabúrať sa do PC (Osobný Počítač) a prelomiť jeho zabezpečenie je pomocou rafinovanosti získať heslo a tým získať všetko potrebné pre získanie prístupu.

Thomas M. Thomas udáva vo svojej knihe *Zabezpečení počítačových sítí bez předchodcích znalostí* príklad pre sociálne inžinierstvo. V tomto scenári autor volal na IT² oddelenie nemenovanej firmy, kde mu zdvihol jeden zo zamestnancov, ktorý bol práve vyššie postavený. Autor sa predstavil ako pracovník cestovnej kancelárie a aj napriek tomu, že vedel len meno firemného zamestnanca, ktorého chce kontaktovať, pomocou dôvtipu z volaného pracovníka IT oddelenia vymámil osobné informácie firemného zamestnanca.

Táto forma prelomovania zabezpečenia je chápaná aj ako hackerský útok, aj napriek tomu, že šikovnosť a znalosť v technike práve nie je nutnosťou. Ak má hacker k dispozícii už len takto zopár dohľadateľných informácií, dokáže sa pomocou sociálneho inžinierstva dostať o ďalší level ďalej na svojej ceste.

[77][78][93]

2.2 Regulačné mechanizmy a cenzúra na sociálnych sieťach

V kontexte správy obsahu na sociálnych sieťach zohráva významnú úlohu regulačná politika platforiem. Prevádzkovatelia sociálnych sietí sú povinní dodržiavať legislatívne rámce krajín, v ktorých pôsobia, čo často vedie k úpravám alebo odstraňovaniu obsahu tak, aby neporušoval miestne zákony.

Tento proces však otvára dôležitú diskusiu o slobode prejavu, keďže algoritmická filtrácia a manuálna kontrola obsahu môžu neúmyselne viesť k potláčaniu legitímnych

² Informačné technológie

názorov a demokratickej debaty. Ako príklad býva často uvádzaný nemecký zákon NetzDG (Nemecký zákon o regulácii obsahu na internete), ktorý ukladá platformám povinnosť odstrániť nenávisťné prejavy do 24 hodín od ich nahlásenia. Ďalšie prípady sa týkajú situácií, v ktorých vlády požadujú obmedzenie alebo odstránenie obsahu vyjadrujúceho určité politické názory.

Z týchto príkladov vyplýva, že online cenzúra je do istej miery neoddeliteľnou súčasťou fungovania digitálnych platforiem. Jej dopady a účinnosť sú zároveň predmetom častej verejnej diskusie – niektoré kroky sú vnímané ako nevyhnutná ochrana spoločnosti, iné ako kontroverzné zásahy do základných práv.

[8];[66][8][67]

Na Slovensku v súčasnom čase pripravujú zákon proti šíreniu nenávisťi na sociálnych sieťach, čo môže mať dobré úmysly, ale podporuje to taktiež určitý typ cenzúry, s ktorým sa môže otvárať otázka či je určitá cenzúra nutná a vhodná. Rovnako sa aj črtá ďalšia otázka, ktorá sa zameriava na definíciu nenávisťi, pretože tento pojem sa dá ohýbať podľa potreby uplatniteľa alebo nahlašovateľa.[94] Podrobnejšie sa o cenzúre a slobode slova píše v kapitole Vybrané aspekty bezpečnosti.

2.3 Hoaxy a dezinformácie

Hoax je falošná správa alebo fáma, ktorá sa zvyčajne šíri na pobavenie, vyvolanie paniky alebo dokonca ako žart. Hoaxy majú často podobu varovania pred neexistujúcim nebezpečenstvom alebo výzvy na pomoc, napríklad zdieľaním falošných príbehov o stratených deťoch.

Dezinformácia je zámerné šírenie nepravdy alebo polopravdy s cieľom ovplyvniť verejnú mienku alebo získať výhodu. Dezinformácie môžu byť politicky motivované a používajú sa napríklad na manipuláciu voličov alebo na rozdelenie spoločnosti.

Rozdiel teda spočíva najmä v úmysle: hoax môže byť neúmyselný alebo len pre zábavu, zatiaľ čo dezinformácia má strategický cieľ.

[95][96][97]

Podkategórie:

a) Konšpiračné teórie

Konšpiračné teórie predstavujú nevysvetlené alebo zámerne skreslené javy, príbehy či udalosti, ktoré sú rôznymi skupinami ľudí interpretované odlišným spôsobom. V mnohých prípadoch sú tieto výklady vnímané ako vierohodné, pretože zodpovedajú presvedčeniam alebo emóciám príjemcu – napriek tomu, že ich pravdivosť nie je možné objektívne overiť. Dôvodom býva buď nedostatok dôkazov, úmrtie priamych aktérov, alebo skutočnosť, že autor pôvodného obsahu (napríklad knihy či filmu) si zámerne ponecháva určité informácie ako súčasť umeleckého zámeru.

V tejto súvislosti je dôležité rozlišovať medzi konšpiračnými teóriami a fanúšikovskými špekuláciami. Do tejto kategórie preto nie sú zaradované neformálne teórie vytvárané fanúšikmi rôznych celebrit, filmov, literárnych diel či záhadných miest. V kontexte tejto práce sú za konšpiračné teórie považované najmä dezinformácie a hoaxy, ktoré sú prezentované ako úplne pravdivé informácie. Tieto obsahy môžu byť potenciálne škodlivé – a to nielen pre príjemcu, ale aj pre osoby, ktorých sa týkajú.

Typickým znakom konšpiračných teórií je, že sa vyvíjajú postupne a bývajú utvárané kolektívne. Postupom času sú dopĺňané ďalšími verziami, čím sa vytvára dojem komplexného a zmyselného príbehu – napriek tomu, že ide len o nepodložené špekulácie, ktoré môžu byť mylne považované za fakty.

[98]

b) Falošné správy

Jedná sa o zavádzajúce informácie, ktoré často napodobňujú spravodajský štýl prejavu. Ich cieľ môže byť rôznorodý. Od zábavy cez zisk až po manipuláciu verejnosti. Spravidla sa šíri cez menej dôveryhodné médiá alebo zjavne nedôveryhodných jedincov, ktorý si svoju povest' poškvrnili vierou v rôzne hoaxy a dezinformácie, ktoré boli neskôr vyhodnotené ako klamlivé. [95]

Zameraním sa na cieľ falošných správ, pod zábavou by si mali užívatelia vedieť predstaviť satiru. Na každej sociálnej sieti sa už len z princípu nachádza minimálne jeden profil, ktorý zámerne šíri vymyslené až absurdné správy. Tieto profily aj nesú popisy ako satiru a každý trochu zmýšľajúci človek vidí, že ide o príspevky so zámerom pobaviť, problém však nastáva ak to objavia ľudia, ktorí tieto príspevky správne neodhadnú. [95]

Samozrejme, nie práve tieto satirické príspevky sú problematické. U nich je viac pravdepodobné, že si aj tí mene všímaví uvedomia neoficiálnosť daných médií alebo jasné klamstvá. Avšak keď ide o ciele zisku a manipulácie verejnosti, tam sa nechajú nachytať aj tí viac osvietení. Predsa len, aj do rôznych siekt, do ktorých si myslia, že sa vysoko vzdelaní ľudia nikdy nemôžu dostať, sa dostanú. A to len preto, lebo si ľudia z princípu dôvery v druhých, získané informácie neoverujú a veria tomu, čo vidia alebo hovoria ich obľúbený tvorca (parasociálny vzťah). [73][95]

c) Propaganda

Mnoho štátov a náboženských organizácií využíva sociálne siete na propagovanie svojich ideológií. Ponúkajú to v lákavých formách, ktoré človeka zaujmú a má chuť po nich siahnuť a dozvedieť sa viac, avšak s tým prichádza aj pasca, v ktorej sa môže nechcene a nevedome ocitnúť a keď to jedinec zistí, je už neskoro a cesta von už nie je taká príjemná ako bola cesta tam. [99]

Jedinou možnosťou ako sa vyhnúť uvereniu v nepravdivé informácie je neustále kontrolovanie získanej informácie. Čím viac relevantných zdrojov, tým lepšie. Nestačí sledovať len bulvár, časopisy či instagramové profily ako zdroj svojich informácií. [48][100]

Extrémistické sociálne siete

Twitter a Telegram sú sociálne siete, ktoré ak ide o zdieľaný obsah na platformách, nemajú žiadne obmedzenie. Každý názor či už extrémisticky konzervatívny alebo z úplne opačného spektra, extrémisticky liberálny, má právo byť zdieľaný, aj keď obsahuje informácie, ktoré sú v spoločnosti neprijateľné. Na týchto sociálnych sieťach nie je komplikované sa dopracovať k materiálom, ktoré môžu obsahovať znaky antisemitizmu, rasizmu či násilia.

Avšak ani anarchia na Internete neponúka správne riešenie, rovnako ako ani cenzúra. Niektoré veci by však nemali byť zdieľané za žiadnych okolností, pretože nemali byť ani nikdy spravené – napr. detská pornografia, vraždy, mučenie alebo plánovanie podobných incidentov.

[24][48][101][102]

2.4 Nebezpečné správanie užívateľov na sociálnych sieťach

V predchádzajúcom bode sa načrtlo nevhodné správanie užívateľov na sociálnych sieťach, ktoré je extrémistické či už na sociálnych sieťach alebo v meatspace. V tejto sekcii

sa ukazuje o správaní užívateľov, ktoré nie je takého veľkého kalibru, avšak jeho následky môžu byť až extrémne.

Kyberšikana

Pojem šikana nie je ľuďstvu aj napriek generačným rozdielom neznámy. Niektorí jedinci majú s týmto slovo väčšie emocionálne spojenie ako druhí, ale ľudia, presne vedľa, čo pojem šikana znamená a ako môžu byť situácie vytvorené skrze šikanu nepríjemné. Aj napriek tomu, že po Internete kolujú rôzne momenty, kedy užívateľ napáda slovne toho druhého a myslí si, že sa jedná o „zdravú“ formu šikany alebo že si ju dotýčny aj zaslúži.

Kyberšikana je pojem, ktorý je ale tiež známy na skrz generácie. Minimálne posledné desaťročie, keďže šikana v kyberpriestore je čoraz častejšia nešťastná udalosť. Ľudia rôznych generácií sa o nej dozvedajú zo správ v televízii alebo na samotných sociálnych sieťach. Pod kyberšikanou vnímame využitie prostriedkov, ktoré sú k dispozícii v kyberpriestore skrze informačné, komunikačné technológie a služby.

Formy kyberšikany sú rôzne, ale náplňou tejto práce sa nie je zamerať sa na jej znaky, formy prejavu ani na dôvody či spôsoby predchádzaniu, ale skôr upozorniť na realitu a dôsledky, ktoré môže škodlivé správanie na sociálnych sieťach spôsobiť aj keď pre mnohých môže byť branné na ľahkú váhu, keďže útočníci si často neuvedomujú skutočnú silu sociálnych sietí a ich dopady v reálnom živote.

Jan Kolouch a spol., nám vo svojom diele *Cybercrime* ponúkajú niekoľko príbehov detí, ktoré skončili tragicky na základe online zosmiešňovania, tyranizovania a ubližovania.

Šikana, ktorá z reálneho života prerastie do kyberpriestoru alebo naopak, je ešte nebezpečnejšia ako šikana len v jednom z priestorov. Problematika (kyber)šikany spočíva v nedostatočnom krytí zákonom či právnymi aspektami. Niektoré aspekty môžu byť potrestané, avšak nie komplexne ako je potrebné, pretože (kyber)šikana sama o sebe nie je trestným činom ani priestupom.

[48][77][48][93]

Kybergrooming

Podstatou kybergroomingu je získať dôveru obete a následne ju manipulovať. Celý útok prebieha cez Internet a niekedy útočník, ktorého sa dá označovať aj ako predátor, vedie komunikáciu smerom k stretnutiu, na ktorom môže dôjsť k sexuálnemu zneužitiu či fyzickému napadnutiu.

Keďže najčastejšími obeťami sú dievčatá v pubertálnom štádiu života a stále v maloletosti, ukazuje sa ako málo sa na sociálnych sieťach dbá na vek užívateľov a rovnako aj vekový rozdiel komunikujúcich či ich úmysly. Sociálne siete používajú reálni ľudia, ktorých by možno jednotliví užívatelia v realite nikdy neoslovili.

V tejto problematike však môže dôjsť podľa právneho systému aj k potrestaniu útočníkov.

[93][103]

Sexting

Ďalšou nepríjemnou situáciou, ktorú svojím správaním vytvoria užívatelia medzi sebou je sexting. Najväčším problémom danej činnosti je, že s veľkou pravdepodobnosťou vznikla úplne dobrovoľne a chcene zo strany obete, ktorá sexuálne materiály útočníkovi sprostredkovala. Skrze získané materiály môže útočník svoju obeť vydierať so zverejnením alebo rozposlaním daných fotografií či videí ak obeť nesplní jeho požiadavky. Časť útočníci sú práve bývalí partneri, cudzí a dokonca aj blízki ľudia na sociálnych sieťach, ktorým obeť dôverovala.

Sexting samotný nie je trestným činom ak ide o dospelé osoby. Avšak zverejňovanie fotiek bez súhlasu osoby áno, rovnako aj šírenie informácií o človeku, ktoré nie sú pravdivé alebo môžu spôsobiť vážnu ujmu.

Jednoduchým riešením tohto problému je daný obsah a materiál nikdy s nikým nezdieľať a svoju intimitu držať len v reálnom svete a nie v rôznych zariadeniach či v chatoch so svojimi partnermi aj napriek tomu, že daná činnosť môže byť príjemná. Následky môžu byť neadekvátne nepríjemnejšie a tým je lepšie predchádzať vôbec možným nepríjemnostiam.

[77]

Kyberstalking

Stalking je veľmi nebezpečným fenoménom, kedy je jedinec kontaktovaný ďalším užívateľom v takom nadmernom štádiu a takým spôsobom, že sa obeť bojí o svoje zdravie, život a bezpečie. Obeť o súkromie úplne prichádza, aj keď nechce, pretože kontakt od útočníka je nadmerný a v podstate o svojej obeti vie množstvo informácií, ktoré na cudzinca sú moc bohaté. Dost' často tá obeť si za vedomosť stalkera môže aj sama, keď zdieľa informácie o sebe nepremyslene. Druhá vec však je, že zdravý jedinec nebude spokojný s tým, aby o ňom neznámy človek vedel toľko informácií, zároveň však zdravý jedinec ani nebude vedieť toľko aj úplne osobných a intímnych informácií.

Často kyberstalking presahuje do stalkingu v meatspace. Toto jednanie je možné trestne stíhať za splnenia podmienok, ktoré paragraf pre nebezpečné prenasledovanie požaduje.

[77]

2.5 Únik informácií

Odkedy sa zapojili prvé počítače do siete, stali sa ľudia zraniteľnými. Medzi jednotlivými užívateľmi sa našli tí zdatnejší, ktorí dokázali prekročiť bariéry medzi svojím zariadením a zariadeniami druhých. Vtedy začalo dochádzať k prvým únikom dát. Priamoúmerne s rýchlym kradnutím dát začala rásť aj snaha o vytvorenie bezpečných systémov, v ktorých sa dá bez strachu pracovať a byť naďalej súčasťou počítačových sietí. [78]

Sociálne siete predstavujú atraktívne ciele pre útočníkov z viacerých dôvodov. Medzi jednotlivé dôvody patrí vysoký počet používateľov, veľké množstvo osobných údajov, možnosť rýchlej manipulácie verejnej mienky a nedostatočná informovanosť používateľov o bezpečnostných rizikách.

Hackerské útoky

Pokiaľ sa používatelia pohybujú na Internete, je zrejmé, že sú pomocou svojej IP³ adresy dostupný pre hackerov. Aby však mohli bez väčšieho strachu, teda v pocite bezpečia pracovať a využívať možnosti, ktoré sú im poskytované, treba sa zabezpečiť voči neželaným útočníkom, ktorí môžu zneprijemniť užívanie samotného Internetu alebo len sociálnych sietí, ak nie dokonca v meatspace, ak by užívateľom napr. ukradli údaje z bankovej karty.

³ jedinečné číselné označenie

Každý počítač alebo smartfón už má určité zabezpečenie, rovnako aj sociálna sieť, na ktorej sa pohybujú jej používatelia má určité svoje protokoly, pravidlá, ktoré zabezpečujú pocit bezpečia ak nie jeho samotné naplnenie. Avšak, nesmie sa zabúdať na ľudský faktor, ktorý celý túto ilúziu narúša. Často totiž sa stáva, že o sebe človek tvrdí, že je nepodstatným a nikto by ho nechcel „hacknúť“, pretože nejde o veľké známe meno medzi väčším objemom ľudí. Neuvedomuje si však, že môže mať určité spojenia na niekoho, kto naopak ten dôležitý je a hacker sa k tomu hlavnému cieľu môže dostať skrze toho, čo si myslí, že sa nemusí o bezpečnosť svojho zariadenia starať dostatočne, lebo je ten „nepodstatný“.

Podobné tvrdenia sú považované za „security by obscurity“. Toto to tvrdenie pokrýva predstavu, že takýto užívatelia sú v bezpečí len preto, že zatiaľ neboli „objavení“. Dá sa to prirovnať k vojakovi ukrytému v zákope. Kým ostáva neodhalený, cíti sa v bezpečí – avšak ide len o pocit ilúzie. V skutočnosti je v mimoriadne zraniteľnej pozícii a ak by ho nepriateľ objavil, stal by sa ľahkým cieľom. Rovnako aj v digitálnom priestore môže byť pocit anonymity klamlivý – neznamena to, že ich užívatelia sú v skutočnom bezpečí.

Ciele útokov hackerov sa delia na príležitostný cieľ a zámerne zvolený. Po Internete sa pohybuje mnoho hackerov, ktorý hľadajú dostatočne zraniteľnú obeť, ktorá ich k niečomu dostane. K príkladu sa dá uviesť úvaha, že by sa nejaký takýto hacker nabúral do počítača, ktorý je napojený na univerzitnú wifi (bezdrôtovú sieť), je práve prihlásený k univerzitnému účtu alebo má možnosť sa prihlásiť. Existuje možnosť, že uškodí celému systému ak bude mať v rukách tieto údaje. A práve táto obeť útoku si mohla povedať: „Veď nie som podstatná, kto by už len chcel moje údaje a informácie o mne.“ A preto sa nebojí zdieľať rôzne veci na sociálnych sieťach a vôbec si nedáva pozor na ich následné zabezpečenie.

[78]

Hackerský útok prebieha v 6-tich krokoch:

- a) *„Obhliadka a prieskum terénu*
- b) *Sledovanie*
- c) *Súpis prostredia*
- d) *Získanie prístupu*
- e) *Rozšírenie oprávnení*
- f) *Vytvorenie zadných vrátok a zahľadenie stôp“ [78]*

Zameranie tejto bakalárskej práce spočíva na sociálnu sieť, preto aj nasledujúce pasáže obsahujú informácie o možnom hackerskom útoku práve cez sociálnu sieť.

[78][78]

a) Obhliadka a prieskum terénu

O čo viac informácií o sebe, možno aj zdanlivo nevinných informácií užívateľ na sociálnych sieťach bude zdieľať, riskuje svoje bezpečie. Hlavne ak je napr. jeho heslo meno jeho domáceho miláčika, ktorého pravidelne pridáva do príbehov a príspevkov na Instagrame. Nie nadarmo sa hovorí, čo sa na Internet pridá, už to tam aj ostane. Aj keď mnohí hovoria, že si pridávajú na sociálne siete, čo sa im páči, hackerovi vytvárajú priam portfólio možností ako na danú osobu zaútočiť. Stačí aj telefonát, v ktorom sa bude hacker tváriť, akoby bol z určitej firmy, napr. pizzerie alebo realitnej kancelárie a má o svojej obeti informácie, ktoré nie sú ľahko dostupné a vplyvom vytvorenia dôvery mu obeť poskytne ďalšie, lebo si myslí, že ide skutočne o niekoho, kto sa k tým informáciám musel dostať len skrze patrenie do danej firmy. Avšak daný užívateľ na ten Facebook pred 10-timi rokmi zverejnili začiatok svojej kariéry v konkrétnej banke. To užívateľ zdieľal pozvánky na biliard, ktorý sa hráva každý piatok o 18:00 v neďalekom podniku a neskôr fotky ako sa ho aj zúčastnil. Možno si aj tak myslí, že nejde o nič prelomové. Jednoducho niekto vie, že v tom čase sa nachádzal tam a potenciálny útočník nevie, kde býva alebo či niekto doma je a teda vzniká pochybnosti o možnosti ublíženia danému užívateľov.

V prvom rade si treba uvedomiť, že tento užívateľ je už veľmi zraniteľný v tom momente, lebo ak už je objektom útoku, nemá sa ako brániť. Ak aj je technicky zdatní a za normálnych okolností, keby sa nachádzal za počítačom aj schopní sa brániť. Lenže ten hacker vie, že teraz sa zabáva vonku s priateľmi. Musela by to byť veľmi výnimočná udalosť, aby sa spomínaný užívateľ akcie nezúčastnil ak sme ju pár dní dozadu zdieľal, že sa opäť organizuje. A možno útočník vie, že keby sa jej užívateľ nezúčastnil, tak by k tomu napísal poznámku typu: „Pozývame nových ľudí, ale my sa nezúčastnime.“ A ten útočník to vie, lebo jeho obeť tento krok už spravila aj pred mesiacom. Užívateľ ani nemusí vedieť ako a hackerovi dáva do rúk všetko, čo potrebuje.

Rovnako však ostáva možnosť, že sa dostanú prv do samotného zariadenia, z ktorého následne budú napádať aplikácie (sociálne siete).

[78][78]

b) Sledovanie

V ďalšom kroku si bude hacker overovať či skutočne sú informácie na našich sociálnych sieťach pravdivé. Možno práve skontaktovaním v predstieraní, ako sa už spomínalo vyššie (sociálne inžinierstvo) alebo skrze iné profily na sociálnych sieťach. [78]

c) Súpis prostredia

Keď hacker má dostatok informácií o jednotlivých potenciálnych obetiach svojho útoku, zoskupí ich a na základe všetkého, čo vie, vyberie sú to najvhodnejšiu, v preklade, tú najzraniteľnejšiu. [78]

d) Získanie prístupu

Okrem mýtu o nedôležitosti svojich krokov na sociálnych sieťach, je ďalším mýtom aj myšlienka o jedinom ciele a to prevziať kontrolu nad daným internetovým profilom. Oveľa príjemnejšou technikou je sa neodhalit' a nenápadne sa snažiť získavať informácie z ponúkaných možností. Často totiž užívatelia majú aj vzájomne prepojené iné sociálne siete. Ak by sa hacker dostal do mailovej schránky užívateľa, mal by veľkú moc nad jeho sociálnym životom, hlavne ak tento užívateľ svoje pôsobenie na Internete uľahčil, aby mu stačilo ako jediné pripojenie práve cez e-mail a tým pádom, prelomenie jedného hesla, vedie k napadnutiu ďalších účtov. [78]

Útoky, ktoré sú tiež reálne v tejto fáze uskutočniť sa nazývajú skriptové:

a) Preťaženie pamäťového bufferu

Vyrovňavacia pamäť alebo anglicky memory buffer je časť pamäte, ktorá sa dočasne ukladá na rôznych miestach v programovom vybavení. Praktickosť spočíva v tom, že sa z nej rýchlejšie načítajú programy ako z dlhodobej. Pokiaľ nie je správne ošetrová a síce, aby nemohla presiahnuť určitý limit, hacker môže túto nezodpovednosť využiť a spôsobiť v operačnom systéme situácie, ktoré ani nevieme predpokladať. [78][104]

b) Uhádnutie hesla metódou hrubej sily

Existujú programy, ktoré sú prepojené so slovníkmi a keď ich hacker spustí, budú skúšať rôzne slová z určitého slovníka, ktorý je napojený na daný program. Slovníky môžu byť aj konkrétnejšie alebo úplne konkrétne, nie len všeobecné. [78]

c) Odpočúvanie hesla

Ak sa hacker dostal do počítačovej siete, stačí mu len vyčkať na správny okamih, kedy sú zadávané heslá pre prihlásenie sa do počítača alebo danej sociálnej siete a útočník sa k nemu vtedy s nadhľadom dostane. [78]

d) Zachytenie súboru hesiel

V systémoch sa zvykne nachádzať balíček alebo teda súbor s heslami, ktoré sa narušiteľ môže rozhodnúť skúsiť prelomiť. Je to pravdepodobne náročnejší proces ako predchádzajúce možnosti, ale ak sa rozšifrovanie podarí, môže sa dostať k veľkému množstvu cenných informácií. [78]

e) Rozšírenie oprávnení

Útok sa nachádza vo fáze, kedy je narušiteľ dostatočne hlboko v systéme, aby mohol s ním narábať takmer úplne podľa svojej vôle, akoby daný profil napr. na Facebooku, patril práve jemu. Avšak, aby skutočne mohol nad ním prevziať úplnú moc, potrebuje svoje právomoci rozšíriť.

Skrze jeden prelomený profil by sa pravdepodobne snažil získať prístup k zoznamu priateľov alebo sledovateľov, ktorí by mohli byť ďalšími cieľmi.

Rovnako však získava aj prístup k osobným údajom používateľa, ako sú e-maily, telefónne čísla alebo súkromné správy, ktoré môžu byť opäť zneužitú na ďalší útok niekde v budúcnosti.

Je aj možné spustenie škodlivého kódu cez odkazy alebo aplikácie zdieľané na profile.

Nie je to len buď alebo, je dosť pravdepodobné, že môže byť uplatnenie všetkých krokov daným jedincom.

[78]

f) Vytvorenie zadných vrátok a zahľadanie stôp

Hacker by sa mohol pokúsiť nainštalovať zadné vrátka do systému sociálnej siete, čím by si zabezpečil prístup aj po odstránení zraniteľnosti. Na zakrytie svojich stôp by hacker mohol využívať anonymné siete (napr. Tor) a techniky maskovania, aby sledovanie jeho aktivít bolo zložitejšie.

Tento proces zdôrazňuje, ako dôležité je dôsledné zabezpečenie účtov na sociálnych sieťach – od silných hesiel cez dvojfaktorovú autentifikáciu až po dôsledné kontroly systémových zraniteľností.

[78]

Cracking

Ľudská nevzdelanosť alebo skôr všeobecná znalosť spôsobuje, že hacking a cracking sa zamieňajú alebo priam prekrývajú.

V jednoduchosti sa dá povedať, že tieto pojmy zahŕňajú tie isté oblasti a činnosti avšak základný rozdiel spočíva v tom, že pod cracking patrí viacero foriem škodenia, porušovania a nelegálnej činnosti.

Hackeri sa delia na kategórie: White Hats, Black Hats a Gray Hats. Tí White nespôsobujú škody, neničia systém, ale práveže spadajú pod tvrdenie „*etický hacker*“. Black Hats je presným opakom predchádzajúcej kategórie, kedy ide väčšinou o kriminálne živly. Gray Hats sú medzníkom medzi extrémnymi zaškatul'kovanými kategóriami, pretože môžu byť aj škodlivými, ale nie moc.

Práve Black Hats nesú označenie crackeri. Rovnako pojem cracking pokrýva aj porušovanie autorských práv, obchádzanie ochranných značiek a zisťovanie prístupového hesla.

[93]

Neoprávnené zdieľanie dát

Tieto zdieľania väčšinou prebiehajú s tretími stranami, ktoré sa dejú na sieťach v rámci obchodovania kvôli sponzorovaným reklamám. Ak sa to vysvetľuje transparentne v podmienkach platforiem alebo v cookies jednotlivých stránok, ktoré samozrejme, užívatelia často nečítajú, len klikajú *súhlasím* a *ok* (súhlasím), môže dôjsť k nechcenému zdieľaniu informácií o sebe, avšak na to sa nemôže užívateľ odvolávať, keďže povolenie udelil vo forme elektronického podpisu. [100][106][107]

Problém však nastáva ak sa dané súčasti nekomunikujú transparentne a platformy dáta predávajú tretím stranám pre lepšie ovládnutie publika. [100][106][107]

Phishingové útoky

Phishing je forma kybernetického útoku využívajúca metódy sociálneho inžinierstva, pri ktorom sa útočník vydáva za dôveryhodnú osobu alebo inštitúciu (napr. banku, doručovateľa, priateľa alebo zamestnávateľa) s cieľom získať citlivé informácie, ako sú heslá, údaje o kreditných kartách alebo iné osobné dáta. Útok prebieha najčastejšie prostredníctvom e-mailov, textových správ alebo telefonátov, kde sa obeť presviedčajú, aby klikli na odkaz, zadali údaje na podvodnej stránke alebo si stiahli škodlivý súbor. Útočníci využívajú strach, naliehavosť či zvedavosť, aby presvedčili obeť konať podľa ich pokynov, pričom cieľom môže byť ktokoľvek – od bežných používateľov až po vysokopostavených zamestnancov.

V jednoduchosti ide o útoky, ktoré sú zamerané na ďalšiu prirodzenú ľudskú vlastnosť – dôveru. Opäť sa potvrdzuje ako inžinieri útočia na ľudskú podstatu.

[93][108][109]

Pharming

Pharming predstavuje jednu z najnebezpečnejších foriem kybernetických útokov zameraných na získanie citlivých údajov. Na rozdiel od klasického phishingu, ktorý sa spolieha na zaslanie podvodného e-mailu, pharming manipuluje s DNS systémom (Domain Name System) – teda s prekladom doménových mien na IP adresy. Cieľom útočníka je, aby bol používateľ automaticky presmerovaný na falošnú webovú stránku, aj keď zadal správnu adresu legítimnej služby (napríklad banky alebo sociálnej siete).

Takéto stránky sa graficky aj svojou funkčnosťou veľmi podobajú originálu, čo zvyšuje šancu, že používateľ bez podozrenia zadá svoje prihlasovacie údaje, ktoré sú následne zneužitú. Výhodou pre útočníka je, že tento typ útoku nemusí vyžadovať žiadny škodlivý softvér na zariadení obeť, pretože útok prebieha na úrovni internetovej infraštruktúry.

Pharming je považovaný za obzvlášť závažnú hrozbu, pretože sa často detekuje ťažšie než bežný phishing a postihuje celé skupiny používateľov bez ich priamej účasti.

[93]

Spear Phishing

Spear phishing je špecifická a vysoko personalizovaná forma phishingu. Na rozdiel od klasického phishingu, ktorý sa posiela hromadne anonymným príjemcom, spear phishing

cieli na konkrétnu osobu alebo organizáciu, ktorej chce poškodiť. Útočník si najprv zhromažďí informácie o obeti – napríklad z verejne dostupných zdrojov, sociálnych sietí alebo firemných webov – a následne vytvorí e-mail alebo správu, ktorá pôsobí dôveryhodne a je presne zacielená.

Najčastejšie sa útočník vydáva za známeho – napríklad kolegu, nadriadeného alebo technickú podporu – a žiada obeť o stiahnutie súboru, kliknutie na odkaz alebo odoslanie citlivých údajov. Táto metóda sa často používa v rámci útokov na firmy, inštitúcie alebo verejné osoby, kde môže mať únik údajov rozsiahle následky.

Vzhľadom na vysokú mieru dôveryhodnosti takýchto správ je spear phishing jedným z najúspešnejších typov kybernetických útokov, pričom obeť si často ani neuvedomia, že boli podvedené.

[93]

Vishing

V predchádzajúcom texte sa nachádza vysvetlenie, čo je to phishing a ako je nebezpečné, že veľmi jednoducho naň môže nepozorný užívateľ naletieť.

Ide o telefonickú verziu phishingu, kedy sa jedinec so znalosťami sociálneho inžinierstva snaží vymámiť zo svojej obeť citlivé informácie. Príklad, ktorý sa uvádzali v sociálnom inžinierstve, kde sa jedinec vydával za zamestnanca cestovnej kancelárie je dokonalým príkladom vishingom. Útočník svoju skutočnú identitu nikdy nevyužíva na tento útok, práveže sa vydáva za niekoho iného a tým sa snaží splniť svoj cieľ.

[93]

Smishing

Od phishingu a vishingu sa tento spôsob útoku líši len tým, že útok je prevádzaný cez SMS správy (krátke textové správy). Tieto SMS správy sa snažia získať z obeť peniaze skrze zavolanie na číslo, ktoré bude obeť stáť viac ako keby zavolá na bežné číslo. Rovnako sú aj nebezpečné cudzie URL odkazy (webová adresa), ktoré môžu neskôr poškodiť zariadenie alebo zneužiť citlivé údaje, ktoré budú na danej stránke žiadať. [93]

Digitálna stopa a zneužitie osobných údajov

Predchádzajúce možnosti únikov dát boli predovšetkým sprostredkované pomocou techniky alebo dáta boli zneužitú v rámci nevedomosti užívateľov a útokov mierených

na nich. Tieto úniky dát môžu byť aj práve tie možnosti, keď si útočník údaje o svojej obeti verejne dohľadá a následne ich zneužije. Ide o formu útoku, kedy sa do problematiky zapája sociálne inžinierstvo a pasívne sledovanie svojej obete či potenciálnych obetí.

Problém sociálnych sietí aj spočíva v tom, že aj keď máme pri našich príspevkoch možnosť *zmazať*, v databáze sociálnej siete to môže ostať, aj keď ona musí spĺňať rôzne právne normy ohľadom toho, aby sa tieto odstránené príspevky nedostali von. Väčší problém práveže tvoria tí ľudia, ktorí si všetko zaznamenávajú a v prípade, že niekto niekde niečo zmaže, oni to dajú do sveta von zas. A vtedy je celkom náročné dopracovať sa k spravodlivosti – k potrestaniu dotyčného a odstráneniu znovu pridaného príspevku bez povolenia jeho tvorca.

Zmluvné podmienky sú veľkým aspektom bezpečnosti, ktorý ale užívatelia často nečítajú a ani im nevenujú čiastočnú pozornosť. Rovnako ako pri cookies, užívateľ zvykne automaticky kliknúť na *prijímam* a myslí si, že mu nič nehrozí, ale keď príde na problémy a predpokladá, že platforma mu pomôže, nie je to tak jednoduché vplyvom toho, že si v zmluvných podmienkach môžu napísať takmer hocičo a ak to druhá strana odsúhlasí, je to problém jej, nie sociálnej siete.

[77][93][110]

Najznámejšie úniky informácií

Cambridge Analytica & Facebook (2018)

Cambridge Analytica (CA) bola britská poradenská spoločnosť, ktorá sa zameriavala na využívanie osobných údajov s cieľom ovplyvňovať volebné procesy. Bola založená v roku 2013 ako dcérska spoločnosť skupiny SCL Group, známej svojím pôsobením v oblasti strategickej komunikácie a psychologických operácií. V rámci svojej činnosti spoločnosť CA investovala do analýzy dát a profilovania voličov – išlo o využívanie moderných technológií na vytváranie voličských profilov a zacielenie politických kampaní na základe osobných údajov. Medzi jej prvých investorov patril Robert Mercer, ktorý do rozvoja spoločnosti vložil 15 miliónov dolárov. Názov „Cambridge Analytica“ mal byť podľa dostupných zdrojov navrhnutý Steveom Bannonom, vtedajším poradcom prezidenta Donalda Trumpa.

V roku 2018 sa spoločnosť ocitla v centre medzinárodného škandálu po tom, ako bolo odhalené, že neoprávnene získala údaje od 50 až 87 miliónov používateľov Facebooku.

Tieto dáta boli následne použité na vytváranie detailných voličských profilov, vďaka čomu bolo možné cieľiť personalizované politické posolstvá na vybrané skupiny obyvateľstva. Táto prax vyvolala rozsiahle vyšetrovania na celom svete. Bolo poukazované na to, že spoločnosť zohrávala úlohu nielen počas prezidentskej kampane Donalda Trumpa v roku 2016, ale aj pri referende o brexite, ako aj v politických kampaniach v Indii, Nigérii či na Blízkom východe.

Kontroverzie sa netýkali len spoločnosti CA, ale aj jej materskej organizácie SCL Group, ktorá mala byť podľa viacerých správ zapojená do volebných operácií na všetkých kontinentoch. Po vypuknutí škandálu sa tieto aktivity údajne pokúsili presunúť pod spoločnosť Emerdata Ltd, založenú v roku 2017. V tejto súvislosti boli zaznamenané aj podozrenia, že jeden z hlavných akcionárov SCL, Vincent Tchenguiz, sa mal podieľať na vzniku izraelskej súkromnej spravodajskej agentúry Black Cube.

Škandál okolo spoločnosti Cambridge Analytica viedol k jej zániku – v roku 2018 bolo podané oznámenie o likvidácii. Tento prípad upozornil na závažné riziká spojené so zhromažďovaním a využívaním osobných údajov v prostredí sociálnych médií. Zároveň sa stal impulzom pre globálnu diskusiu o ochrane súkromia, etických hraniciach v digitálnom marketingu a transparentnosti politickej komunikácie.

[111][112][113][114]

Sony Pictures hack (2014)

Jedným z najznámejších prípadov cieleného spear phishingu v histórii kybernetickej bezpečnosti bol útok na spoločnosť Sony Pictures Entertainment z roku 2014. Tento incident mal mimoriadne vážne dôsledky – nielen z hľadiska úniku citlivých dát, ale aj z pohľadu jeho geopolitického presahu.

Podľa analýzy publikovanej v knihe *CyberCrime* bol útok označený ako typický príklad toho, ako môže byť spear phishing využitý ako účinný nástroj na kompromitáciu celej organizácie. Zamestnancom spoločnosti boli doručované personalizované e-maily, ktoré sa vydávali za internú komunikáciu – často prichádzali údajne od kolegov či IT oddelenia. Ich cieľom bolo získanie prihlasovacích údajov a následná inštalácia škodlivého softvéru (malvéru) do firemnej siete.

Ako uvádzajú zdroje BBC a Columbia SIPA, následkom útoku došlo k úniku rozsiahleho množstva interných dát – vrátane e-mailovej komunikácie vedenia spoločnosti, doposiaľ nezverejnených filmov, obchodných zmlúv s hercami, platových údajov

či osobných informácií viac než 47 000 súčasných a bývalých zamestnancov. Útok mal aj výrazný psychologický efekt: zamestnancom boli adresované hrozby, kancelárie boli dočasne uzavreté a spoločnosť čelila silnému mediálnemu tlaku [115][116]

Podľa spoločnosti Coverlink bol tento incident označený ako učebnicový príklad zlyhania v oblasti kybernetickej ochrany. Spoločnosť Sony bola následne nútená investovať milióny dolárov do obnovy systémov a reputácie a zároveň čelila viacerým žalobám zo strany poškodených osôb [117]

Tento prípad poukazuje na to, že spear phishing nepredstavuje len technickú hrozbu, ale ide o komplexný sociálno-technologický útok, ktorý využíva kombináciu dôvery, prístupu k interným informáciám a ľudskej nepozornosti. Práve táto kombinácia umožňuje dosiahnuť významné a potenciálne deštruktívne výsledky.

[93][115][116][117][118]

LinkedIn dátový únik (2021)

V júni roku 2021 sa na hackerskom fóre objavila ponuka na predaj údajov približne 700 miliónov používateľov LinkedIn, čo predstavovalo asi 92 % vtedajšej používateľskej základne tejto platformy. Údaje zahŕňali celé mená, e-mailové adresy, telefónne čísla, informácie o zamestnaní, pohlaví a ďalšie verejne dostupné údaje z profilov používateľov.

Spoločnosť LinkedIn v oficiálnom stanovisku uviedla, že nejde o klasický prípad úniku dát v dôsledku narušenia bezpečnostných systémov, ale o tzv. scraping – proces automatizovaného zhromažďovania verejne dostupných údajov bez oprávnenia. Aj keď pri incidente nedošlo ku kompromitácii hesiel ani platobných informácií, zozbierané dáta mohli byť zneužitú na cielené phishingové útoky, krádeže identity alebo iné formy sociálneho inžinierstva.

Tento prípad poukázal na riziká spojené s verejným zdieľaním osobných údajov na profesionálnych platformách a zdôraznil význam zodpovedného nastavenia súkromia a dôsledného zabezpečenia údajov používateľov, aj v prípade, že sa jedná o informácie formálne označované ako „verejné“.

[93][119][120]

Pharming – bankové podvody v Českej republike (2015)

V roku 2015 boli na území Českej republiky zaznamenané prípady pharmingových útokov, pri ktorých bola použitá technika zameraná na presmerovanie používateľov

na falošné webové stránky bez ich vedomia. Podľa publikácie *CyberCrime* boli útoky realizované prostredníctvom modifikácie systémového súboru „hosts“ vo Windows alebo prostredníctvom zmeny DNS nastavení v domácich smerovačoch. V dôsledku týchto zásahov boli používatelia po zadaní adresy svojej banky (napr. Fio banka alebo Komerčná banka) presmerovaní na podvodné weby, ktoré verne napodobňovali vzhľad oficiálnych stránok.

V tejto súvislosti vydala Fio banka verejné upozornenie na vlnu podvodných e-mailov, ktorých cieľom bolo nájsť klientov na kliknutie na odkaz a následné prihlásenie sa do online bankovníctva. Odkazy viedli na falošné domény, ako napríklad cs-post.net, ktoré boli vizuálne prakticky totožné s originálnymi stránkami, no slúžili na zber prihlasovacích údajov a ich následné zneužitie. Klientom bolo odporúčané zadávať adresu banky ručne, kontrolovať prítomnosť bezpečnostného certifikátu a vyhýbať sa odkazom zasielaným cez e-mail alebo SMS správy.

Na túto hrozbu zareagovali viaceré bankové inštitúcie zavádzaním pokročilejších bezpečnostných opatrení, ako je dvojfaktorová autentifikácia, overovanie cez SMS alebo detekcia neštandardného správania v rámci online aplikácií. Komerčná banka bola za svoje bezpečnostné inovácie v tom istom roku ocenená spoločnosťou Finparáda ako líder v oblasti bezpečnosti vo finančnom sektore.

Pharming predstavuje významnú kybernetickú hrozbu aj v súčasnosti, najmä preto, že na rozdiel od phishingu si nevyžaduje chybu používateľa – útok môže byť úspešne vykonaný zneužitím dôvery vo vlastné zariadenie alebo prostredníctvom manipulácie so sieťovými nastaveniami. Efektívnou prevenciou zostáva pravidelná aktualizácia zariadení, využívanie spoľahlivého antivírusového softvéru a dôsledná kontrola bezpečnostných prvkov webových stránok.

[93][121][122]

Smishing kampane (CZ/SK banky, pošta)

V rokoch 2014 a 2015 bol na území Českej republiky zaznamenaný výrazný nárast phishingových a smishingových útokov, ktoré sa vydávali za oficiálnu komunikáciu Českej pošty. Útočníci rozposielali hromadné e-maily a neskôr aj SMS správy, v ktorých sa tvrdilo, že adresát nebol zastihnutý pri doručovaní zásielky, prípadne že je potrebné uhradiť clo alebo iný poplatok. Správy obsahovali odkaz na podvodnú webovú stránku, ktorá napodobňovala vzhľad oficiálneho webu Českej pošty [93]

Podľa publikácie *CyberCrime* boli pri týchto útokoch používané domény ako *cs-post.net*, *ceskaposta.net* a ďalšie imitácie. Falošné stránky boli graficky takmer totožné s originálom, pričom ich cieľom bolo prinútiť používateľa stiahnuť škodlivý súbor alebo zadať citlivé údaje – vrátane prihlasovacích údajov či údajov o platobnej karte [93]

Česká pošta opakovane zverejšovala verejné varovania na svojom webe, v ktorých zdôrazňovala, že nikdy neposiela e-maily s výzvou na zadanie údajov alebo s odkazmi na sťahovanie súborov. V mnohých prípadoch boli falošné správy písané chybnou češtinou alebo vytvárané cez automatizované prekladače, čo však nestačilo na odhalenie podvodu menej skúsenými používateľmi [93]

Tento incident predstavuje učebnicový príklad sociálneho inžinierstva a poukazuje na to, akou ľahkosťou môže byť používateľ zmanipulovaný, ak je falošný obsah prezentovaný dôveryhodným spôsobom. Podobné útoky sa pritom vyskytujú dodnes – v mierne upravenej podobe – najmä v mene doručovacích spoločností, colných orgánov alebo bánk [93]

Vyššie uvedené prípady jasne ukazujú, že kybernetické hrozby nie sú len teoretickou možnosťou, ale reálnou a opakovanou súčasťou digitálneho prostredia. Bez ohľadu na to, či ide o sofistikovaný spear phishing smerovaný na nadnárodnú korporáciu, manipulatívne pharmingové útoky na bežných občanov alebo zneužitie verejných dát z profesionálnych sietí – vždy ide o zásah do súkromia, dôvery a bezpečnosti používateľov.

Každý z týchto incidentov odhaľuje inú stránku kybernetickej zraniteľnosti:

- a) Sony Pictures pripomína, ako ľudský faktor môže spustiť masívny únik dôverných dát.
- b) Český pharming a smishing ukazujú, že dôvera vo vizuálnu podobnosť a autoritu značiek sa dá ľahko zneužiť.
- c) Únik z LinkedIn zas zdôrazňuje, že aj verejné údaje sa môžu stať cenným nástrojom pre kyberzločincov.

Spoločným menovateľom všetkých prípadov je absencia obozretnosti, nedostatočné zabezpečenie a rýchla adaptácia útočníkov na nové digitálne prostredie. Tieto prípady slúžia ako varovanie aj motivácia – pre používateľov, aby boli v digitálnom priestore opatrnejší, a pre spoločnosti, aby investovali do osvet, prevencie a moderných bezpečnostných nástrojov.

Úlohou bezpečnostných stratégií v dnešnej dobe nie je len reagovať na incidenty, ale predvídať ich a systematicky im predchádzať.

[93]

2.6 Metódy analýzy rizík

V tejto sekcii sú predstavené jednotlivé metódy pre analýzu rizík, ktoré sú využité v praktickej časti. Analýza rizík pomáha skrze výskum nahliadnuť hlbšie do vybratých rizík na skúmanie. Tento krok je veľmi dôležitý, aby bolo následne po bližšom pochopení rizík možné usúdiť ako treba riziká správne a dôsledne ošetriť.

Zvolená metóda	Typ rizík
CARVER	Technické riziká
FMEA/PNH (Analýza možných porúch a ich dôsledkov / Pravdepodobnosť, Následok a Odhaliteľnosť rizika)	Procesné/právne riziká
KARS (Kvalitatívna analýza rizík s využitím ich súvzťažnosti)	Psychologické/sociálne riziká

Tabuľka 1 Rozčlenené riziká podľa zvolenej metódy a typu rizika

(Zdroj: [vlastný])

Metóda CARVER

Metóda CARVER má svoj pôvod vo Vietname, kde bola využitá počas vojny. V súčasnosti sa aktívne využíva v armáde, napríklad americkej. Jedná sa o analytický nástroj a slúži na identifikovanie významnosti bezpečnostných rizík podľa určitých kritérií. V tejto bakalárskej práci daná metóda bude využitá na systematické vyhodnotenie v prvom rade technických rizík, s ktorými môže užívateľ sociálnych sietí prísť do kontaktu.[123][124][125][126][127]

V čase jej vzniku bola používaná na vyhodnocovanie aktív v zmysle – čo je najcennejšie a najzraniteľnejšie pre protivníka, v súčasnosti sa prispôsobila a využíva sa aj k vyhodnocovaniu rizík. **Chyba! Nenašiel sa žiaden zdroj odkazov.**[124][125][126]

Referenčná hodnota (rizík)	Kategória rizík
24-30	Kritický význam (Kategória I.)
18-23	Dôležitý význam (Kategória II.)
12-17	Bežný význam (Kategória III.)
6-11	Nízky význam (Kategória IV.)

Tabuľka 2 Kategórie metódy CARVER

(Zdroj:[123])

Číselné hodnoty sa priradia šiestim kritériám: kritickosti, prístupnosti, obnoviteľnosti, zraniteľnosti, vplyvu a rozpoznateľnosti, aby ohodnotili každé aktívum (v tomto prípade riziko). [123][124][125][126]

Označenie	Anglické znenie	Slovenské znenie
C	Critically	Kritickosť
A	Accessibility	Prístupnosť
R	Recognizability	Obnoviteľnosť
V	Vulnerability	Zraniteľnosť
E	Effect	Vplyv
R	Recognizability	Rozpoznateľnosť

Tabuľka 3 Kritéria metódy CARVER

(Úpravené z[123])

Kritickosť predstavuje jedno z kľúčových kritérií pri hodnotení rizík. V tomto kontexte sa posudzuje, aký vážny dopad by malo naplnenie konkrétneho rizikového scenára na fungovanie systému. Hodnotí sa najmä miera narušenia prevádzky, bezpečnosti alebo funkčnosti systému ako celku, prípadne jeho významnej časti. Riziko je považované za kritické v prípade, že by jeho realizácia spôsobila výrazné obmedzenie alebo úplný výpadok kľúčových procesov. Pri hodnotení kritickosti je potrebné zohľadniť prepojenosť s inými procesmi a sekundárne vplyvy, ktoré môžu vzniknúť v dôsledku reťazovej reakcie v rámci systému. [123][124][125][126]

Kritickosť	Hodnoty	Popis kritéria
Veľmi nízka	1	Riziko by spôsobilo úplne nahraditeľné škody bez významného dopadu.
Nízka	2	Riziko by malo mierny dopad, menšími náklady alebo čas na opravu.
Stredná	3	Riziko by spôsobilo dočasné obmedzenie fungovania s vyššou personálnou alebo technickou náročnosťou.
Vysoká	4	Riziko by spôsobilo vážnejší výpadok alebo narušenie kľúčovej funkcie systému.
Veľmi vysoká	5	Riziko by viedlo k úplnému zlyhaniu systému alebo nezvratným následkom.

Tabuľka 4 Kritérium kritickosti

(Úpravené z[123])

Prístupnosť vyjadruje, ako jednoducho môže dôjsť k realizácii rizika – teda do akej miery je pre útočníka alebo hrozbu možné dosiahnuť svoj cieľ. Posudzuje sa, aké ochranné opatrenia a bariéry musia byť prekonané, a či je ich obídenie technicky, organizačne alebo fyzicky náročné. Riziko sa považuje za ľahko prístupné, ak ho možno realizovať bez potreby prekonávania významných obranných prvkov. Naopak, nízka prístupnosť znamená, že existuje viacero vrstiev ochrany, ktoré realizáciu rizika výrazne sťažujú. [123][124][125][126]

Prístupnosť	Hodnoty	Popis kritéria
Veľmi nízka	1	Realizácia rizika je extrémne zložitá, vyžaduje násilie alebo prekonanie silnej ochrany.
Nízka	2	Realizácia rizika je možná, ale zložitejšia, napr. pomocou lesti.
Stredná	3	Riziko je relatívne jednoducho realizovateľné, avšak s určitým odporom.
Vysoká	4	Riziko možno uskutočniť pomerne ľahko, prekonaním bežnej ochrany.
Veľmi vysoká	5	Riziko je veľmi ľahko realizovateľné, bez prekážok alebo ochrany.

Tabuľka 5 Kritérium prístupnosti

(Úpravené z[123])

Obnoviteľnosť sa vzťahuje na schopnosť organizácie zotaviť sa po naplnení rizika. Hodnotí sa pripravenosť na obnovenie činnosti, dostupnosť náhradných riešení a čas potrebný na návrat do normálneho režimu. Riziko s nízkou obnoviteľnosťou

je charakterizované dlhodobými alebo finančne náročnými následkami, ktoré komplikujú návrat do pôvodného stavu. [123][124][125][126]

Obnoviteľnosť	Hodnoty	Popis kritéria
Veľmi nízka	1	Zotavenie systému do 1 týždňa.
Nízka	2	Obnova možná do 1 mesiaca.
Stredná	3	Obnova by trvala do 3 mesiacov.
Vysoká	4	Obnova by bola možná do 1 roka.
Veľmi vysoká	5	Obnova by trvala viac ako 1 rok.

Tabuľka 6 Kritérium obnoviteľnosti

(Úpravené z[123])

Zraniteľnosť označuje prítomnosť slabých miest v systéme, ktoré môžu byť zneužitú na realizáciu rizika. Hodnotí sa existencia technických, organizačných alebo procesných nedostatkov, ktoré môžu uľahčiť naplnenie rizikového scenára. Sleduje sa aj úroveň znalostí a zdrojov, ktoré by útočník potreboval – čím nižšia odbornosť je vyžadovaná, tým je zraniteľnosť vyššia. [123][124][125][126]

Zraniteľnosť	Hodnoty	Popis kritéria
Veľmi nízka	1	Riziko možno naplniť len s profesionálnymi znalosťami a výbavou, s minimálnym dopadom.
Nízka	2	Realizácia vyžaduje špeciálne schopnosti, dopad je výraznejší.
Stredná	3	Riziko môže naplniť priemerne znalý útočník s bežnými prostriedkami.
Vysoká	4	Riziko dokáže zneužiť aj menej skúsený útočník s improvizovaným vybavením.
Veľmi vysoká	5	Riziko je zneužiteľné prakticky bez znalostí a vybavenia, s maximálnym dopadom.

Tabuľka 7 Kritérium zraniteľnosti

(Úpravené z[123])

Vplyv predstavuje rozsah a závažnosť dôsledkov, ktoré môže naplnenie rizika spôsobiť. Môže ísť o narušenie prevádzky, ohrozenie zdravia alebo života osôb, stratu reputácie, dôvery zo strany verejnosti, prípadne o ekonomické škody. Riziko s vysokým

vplyvom je schopné zasiahnuť viacero oblastí súčasne a spôsobiť komplexné škody. [123][124][125][126]

Vplyv	Hodnoty			Popis kritéria
Veľmi nízka	1	bez následkov na zdraví a životoch	do 50 000 Kč	Žiadne ohrozenie zdravia alebo života, zanedbateľné škody.
Nízka	2	následky na zdraví do 1 osoby	do 200 000 Kč	Dopad na jednotlivcov alebo časti technológie, obmedzený rozsah.
Stredná	3	následky na zdraví do 3 osôb	do 500 000 Kč	Dopad na viaceré osoby alebo celý objekt, výpadok kritických služieb.
Vysoká	4	následky na zdraví do 20 osôb	do 1 000 000 Kč	Vážne ohrozenie zdravia väčšej skupiny, dlhodobé obmedzenie prevádzky.
Veľmi vysoká	5	úmrtie osôb	nad 1 000 000 Kč	Úmrtia, veľkoplošné alebo trvalé následky, zásadná reputačná alebo ekonomická strata.

Tabuľka 8 Kritérium vplyvu

(Úpravené z[123])

Rozpoznateľnosť vyjadruje, do akej miery je riziko včas identifikovateľné a monitorovateľné. Vysoká rozpoznateľnosť znamená, že ide o známe riziko s dostupnými varovnými signálmi, ktoré je možné predvídať a včas mu zabrániť. Nízka rozpoznateľnosť naopak znamená, že riziko sa môže prejaviť nečakane alebo bez varovania, čo zvyšuje pravdepodobnosť jeho naplnenia. [123][124][125][126]

Rozpoznateľnosť	Hodnoty	Popis kritéria
Veľmi nízka	1	Riziko je takmer neidentifikovateľné aj pri maximálnom úsilí.
Nízka	2	Identifikácia rizika si vyžaduje veľké úsilie a je málo pravdepodobná.
Stredná	3	Riziko možno identifikovať pri priemernej úrovni monitoringu.
Vysoká	4	Riziko je dobre identifikovateľné bežnými metódami.
Veľmi vysoká	5	Riziko je zjavné, opakovane sa vyskytuje a ľahko sa rozpoznáva.

Tabuľka 9 Kritérium rozpoznateľnosti

(Úpravené z[123])

Po priradení hodnôt sa jednotlivé čísla spočítajú a výsledok je referenčnou hodnotou, ku ktorej sa následne pridelí kategória rizika, ktorá určuje význam rizika.

Metóda modifikovaná FMEA/PNH

Modifikovaná metóda FMEA/PNH predstavuje kombináciu dvoch prístupov k analýze rizík – klasickej metódy FMEA (Failure Mode and Effects Analysis) a bodovej metódy PNH (Pravdepodobnosť, Následok, Hodnotenie). [128]

R = miera rizika

P = pravdepodobnosť vzniku rizika

N = závažnosť následkov

H = odhaliteľnosť

Vybraté riziko sa hodnotí na základe výberu jednotlivých kritérií z N, P a H. Vynásobením týchto hodnôt medzi sebou sa dostáva výsledok R – miera rizík, pri ktorej sa potom posudzuje prijateľnosť rizika a následne určujú opatrenia. [123]

R	Výsledná (porovnatelná) miera rizika	Prijateľnosť rizika	N - následok		
1-3	bezvýznamné riziko	prijateľné	1	Bez následkov na zdraví a životoch	Finančná strata na majetku nepresahujúca hodnotu 5000 Kč
4-10	menej významné riziko		2	Nepatrné následky na zdraví a životoch	Mierna škoda na majetku nepresahujúca 25 000 Kč
11-50	mierne riziko	podmienečne prijateľné	3	Vážnejšie následky na zdraví a životoch	Mierne škoda na majetku nepresahujúca hodnotu 125 000 Kč
51-100	významné riziko	neprijateľné	4	Vysoké následky na zdraví a životoch	Vyššia škoda na majetku nepresahujúca hodnotu 500 000 Kč
101-125	nežiaduce riziko		5	Veľmi vysoké následky na zdraví a životoch	Kritická škoda na majetku presahujúca hodnotu 500 000 Kč

Tabuľka 10 Parametre posúdenia rizík

(Zdroj:[123])

P – pravdepodobnosť vzniku rizika		Popis kritéria	
1	Náhodná, veľmi nepravdepodobná	1	Riziko odhaliteľné v dobe jeho spáchania
2	Skôr nepravdepodobná	2	Ľahko odhaliteľné riziko behom pár minút
3	Pravdepodobná, reálna hrozba	3	Odhaliteľné riziko behom pár minút
4	Veľmi nepravdepodobný vznik	4	Ťažko odhaliteľné riziko behom pár minút
5	Trvalá hrozba	5	Neodhaliteľné riziko

Tabuľka 11 Parametre posúdenia rizík

(Zdroj:[123])

Metóda Kars

Ďalšia metóda, ktorá je použitá v praktickej časti práce v rámci analýzy rizík je metóda KARS (Kvalitatívna Analýza Rizík s využitím Súvzťažnosti), ktorá predstavuje systematický postup pre identifikáciu následnú klasifikáciu a na koniec vyhodnotenie vzájomných väzieb medzi jednotlivými rizikami. Touto metódou sa umožňuje určiť,

ktoré riziká sú pre systém, ktorý je skúmaný najnebezpečnejšie a vyžadujú si z tohto dôvodu prioritné riešenie. [129]

Postup aplikácie metódy KARS:

1. Zostavenie súpisu rizík

V prvej fáze metódy KARS je zostavený súpis rizík, ktoré sa v rámci daného systému môžu vyskytnúť. Tento zoznam musí byť vypracovaný čo najdetailnejšie, aby bolo možné dosiahnuť presné a hodnotné výsledky.

Súpis môže obsahovať riziká ako napr. požiar, výbuch, únik nebezpečných látok, záplavy a pod. V našom prípade sa však riziká týkajú kyberpriestoru so zameraním na sociálne siete.

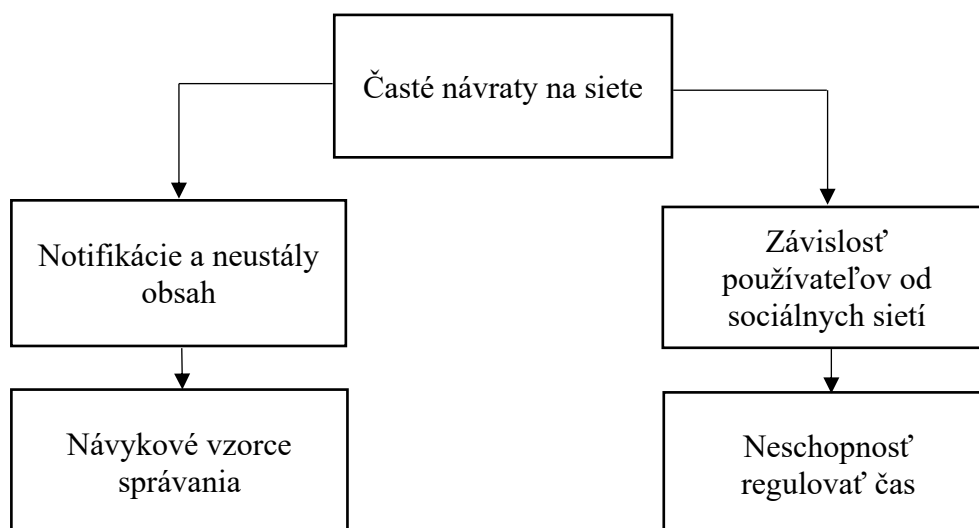
2. Vytvorenie tabuľky rizík

Z každého rizika sa vytvorí slovný popis, ktorý sa následne prevedie do grafickej formy.

Slovný popis:

Ak sa používateľ opakovane vracia na sociálnu sieť kvôli notifikáciám a neustálemu obsahu, môže si vytvoriť návykové vzorce správania, čo vedie k závislosti od siete a neschopnosti regulovať čas online.

Obrázok 3 Príklad z praktickej časti pre slovný prepis rizika závislosti na sociálnej sieti



Obrázok 4 Príklad grafického prevedenia z praktickej časti práce pre riziko závislosti na sociálnej sieti

(Zdroj:[vlastný])

Z grafického prevedenia je zostavená tabuľka rizík, kde sú jednotlivé riziká rozmiestnené do riadkov aj stĺpcov. Týmto spôsobom sa každé riziko porovnáva s ostatnými a posudzuje sa ich vzájomná súvislosť.

3. Vyplnenie matice súvzťažnosti

Do tabuľky sa následne vkladajú hodnoty súvzťažnosti medzi rizikami:

- a) Vloží sa hodnota 1, ak riziko R_i môže vyvolať riziko R_j .
- b) Vloží sa hodnota 0, ak takáto súvislosť neexistuje

Takto sa postupuje po riadkoch zľava doprava, pričom na diagonále sú hodnoty vždy 0, pretože riziko nemôže vyvolať samo seba.

4. Výpočet koeficientov aktivity a pasivity (KAR_i , KPR_i)

Po doplnení tabuľky je vykonaný výpočet koeficientu aktivity KAR_i (vyjadrujúci, koľko ďalších rizík môže toto určité riziko vyvolať) a koeficientu pasivity KPR_i (koľkými inými rizikami môže byť dané riziko vyvolané).

$$KAR_i = \frac{\Sigma R_i}{x - 1} \cdot 100 =$$

$$KPR_i = \frac{\Sigma R_i}{x - 1} \cdot 100 =$$

Tieto koeficienty sa vypočítavajú ako percentuálny podiel z celkového počtu rizík (mínus 1).

5. Grafické zobrazenie a vyhodnotenie

Na základe týchto koeficientov je zostavený graf súvzťažnosti, v ktorom sú riziká rozdelené do štyroch kvadrantov:

- I. kvadrant – primárne a sekundárne nebezpečné riziká
- II. kvadrant – sekundárne nebezpečné riziká
- III. kvadrant – primárne nebezpečné riziká
- IV. kvadrant – relatívne bezpečné riziká

Osy O_1 a O_2 sa určujú tak, aby bol I. kvadrant najvýznamnejší.

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

[129]

Využitie v praktickej časti

V praktickej časti práce bola metóda KARS využitá na analýzu rizík, ktoré sa môžu stať ak užívatelia sociálnych sietí nebudú v oblasti ich bezpečného užívania vzdelaní a nebudú svoje vedomosti využívať. Pomocou súpisu rizík a následného vyhodnotenia ich vzájomných väzieb sa identifikovali kritické riziká s najvyššími hodnotami KARi a KPRi, ktorým sa v návrhu bezpečnostných opatrení venovala prioritná pozornosť.

Tieto metódy pre praktickú časť boli zvolené z dôvodu ich rôznorodého zamerania, keďže aj dané riziká postihujú rozdielne oblasti a tým sa pokrývajú všetky skúmané oblasti rizík.

[129]

Kapitola sa venuje identifikácii a analýze najvýznamnejších bezpečnostných rizík spojených s používaním sociálnych sietí. V úvodnej časti sa analyzujú rôzne formy digitálnej manipulácie a následne sa pozornosť sústreďuje na fenomén dezinformácií, vrátane hoaxov a extrémistických platforiem, ktoré tieto obsahy šíria. Dôležité miesto zaujímajú aj riziká spojené s nebezpečným správaním používateľov, ako aj analýza únikov informácií, ku ktorým môže dôjsť v dôsledku hackerských útokov, phishingu či neoprávneného zdieľania údajov.

V druhej časti kapitoly sa detailne rozoberá metodológia hodnotenia rizík, konkrétne metódy CARVER, modifikovaná FMEA/PNH a metóda KARS. Ich princípy a praktické využitie slúžia ako nástroje na hlbšie porozumenie zraniteľnostiam digitálneho prostredia a zároveň ako základ pre vypracovanie praktickej časti práce.

3 VYBRANÉ ASPEKTY BEZPEČNOSTI

Podľa autorov Jack Goldsmith a Tim Wu knihy *Kto riadi Internet* je známe, že snaha o absolútnu voľnosť na Internete je limitovaná, pretože má rovnaké dopady ako keby vo svete nefungujú zákony. Sú veci, ktoré na sociálnych sieťach je potrebné kontrolovať a dodržiavať, inak by sa tento nástroj zmenil na zbraň. Rovnako však v tejto kapitole sa nachádzajú informácie ohľadom limitácií nariadení a ich nedostatkov. [130]

3.1 Ochrana osobných údajov na sociálnych sieťach

Ochrana osobných údajov sa v súčasnosti stáva jednou z kľúčových tém v súvislosti so sociálnymi sieťami. Platformy ako Facebook, Instagram či TikTok denne spracúvajú obrovské množstvo údajov o používateľoch – od základných identifikačných údajov, cez polohu, správanie, až po preferencie a nákupné zvyklosti. Tento rozsiahly zber dát si vyžaduje jasne definované právne rámce, ktoré majú za cieľ chrániť práva jednotlivcov a zabezpečiť transparentnosť ich spracovania. [130]

V Európskej únii je základným dokumentom nariadenie GDPR (General Data Protection Regulation), ktoré vstúpilo do platnosti v roku 2018. GDPR zaviedlo princípy ako právo na prístup k údajom, právo byť zabudnutý, či právo na opravu – čo v prípade sociálnych sietí znamená, že používateľ má nárok vedieť, aké údaje o ňom platforma spracúva, ako ich používa a má možnosť ich vymazať. [130]

Z pohľadu kyberbezpečnosti GDPR tiež kladie dôraz na minimalizáciu údajov a zodpovednosť prevádzkovateľov za zabezpečenie databáz pred únikom či zneužitím dát. Pri nedodržaní týchto povinností hrozia sociálnym sieťam vysoké pokuty – ako ukázali prípady Cambridge Analytica alebo únikov údajov miliónov používateľov Facebooku.

[111][112][113][114]

Okrem spracovania je dôležité venovať pozornosť aj uchovávaniu a zdieľaniu údajov. Podľa knihy *CyberSecurity*, technologické platformy musia jasne špecifikovať, ako dlho sú údaje uchovávané a komu môžu byť ďalej sprístupnené – či už partnerom, vývojárom, reklamným agentúram alebo štátnym orgánom. Zákon o kybernetickej bezpečnosti (181/2014 Zb.), ktorý kniha komentuje, dopĺňa tieto povinnosti o technické a organizačné opatrenia, ktoré majú zaistiť integritu, dôvernosť a dostupnosť spracúvaných údajov.

Zároveň sa otvára diskusia o globálnych štandardoch ochrany údajov, keďže väčšina sociálnych platforiem pôsobí mimo EÚ (Európskej Únie). Ich povinnosť rešpektovať

európske regulácie však zostáva, ak cieľia na občanov EÚ – čo podčiarkuje význam medzinárodnej spolupráce a harmonizácie právnych rámcov.

[8][93]

Digitálne regulácie v EÚ a vo svete

V súčasnosti rastie tlak na vytvorenie právneho rámca, ktorý by reagoval na čoraz väčší vplyv sociálnych sietí na spoločnosť a spôsob, akým sa šíria informácie. Európska únia sa snaží zabezpečiť väčšiu transparentnosť, ochranu základných práv a predchádzať zneužívaniu týchto platforiem prostredníctvom nových pravidiel.

Jedným z kľúčových opatrení je Digital Services Act (DSA), ktorý vstúpil do platnosti v roku 2024. Zavádza pravidlá pre veľké online platformy, najmä v súvislosti s odstraňovaním nelegálneho obsahu, transparentnosťou algoritmov a efektívnejším moderovaním obsahu. Používateľ má po novom právo vedieť, ako funguje odporúčací algoritmus, a môže si zvoliť aj jeho verziu bez profilovania.

V oblasti umelej inteligencie bol predstavený návrh tzv. AI Act, ktorý sa zameriava na reguláciu vývoja a využívania AI technológií v EÚ. Tento dokument sa dotýka aj fungovania sociálnych sietí – napríklad v oblastiach automatizovaného rozhodovania, moderácie príspevkov alebo odporúčacích systémov. Hlavným cieľom je, aby boli tieto systémy transparentné, férové a zodpovedné.

Veľkú pozornosť si vyžaduje aj boj proti dezinformáciám. Sociálne siete čelia požiadavke, aby zasahovali proti manipulatívneho obsahu. Ako príklad možno uviesť nemecký zákon NetzDG, ktorý prikazuje odstrániť nenávisťný obsah do 24 hodín od nahlásenia.

Otázka však zostáva, ako nájsť rovnováhu medzi ochranou používateľov a zachovaním slobody prejavu. Ako upozorňuje Castells, regulácia by nemala prerásť do cenzúry, ale mala by byť primeraná, transparentná a mala by ponechať používateľom možnosť odvolania.

[8][93][110]

	Oblasť	GDPR	DSA	AI Act
1	Cieľ regulácie	Ochrana osobných údajov	Bezpečné digitálne prostredie	Bezpečné využívanie umelej inteligencie
2	Zameranie	Zber, spracovanie a uchovávanie dát	Odstraňovanie nelegálneho obsahu, algoritmy	Regulácia systémov AI (vrátane algoritmov na sieťach)
3	Typ regulácie	Nariadenie EÚ (od 2018)	Nariadenie EÚ (účinné od 2024)	Pripravované nariadenie EÚ
4	Dotknuté platformy	Všetky subjekty, ktoré spracúvajú údaje občanov EÚ	Veľké online platformy a trhy	Subjekty vyvíjajúce a nasadzujúce AI v EÚ
5	Práva používateľov	Právo na prístup, opravu, výmaz (t. z. „byť vymazaný“)	Právo na informácie o algoritmoch, možnosť zvoliť si ich alternatívu	Ochrana pred neobjektívnym rozhodovaním
6	Povinnosť platforiem	Transparentnosť, minimalizácia dát, bezpečnosť údajov	Rýchle odstraňovanie obsahu, vysvetlenie odporúčaní	Transparentnosť, auditovateľnosť, zákaz niektorých AI

Tabuľka 12 Zhrnutie GDPR, DSA a AI Act

(Zdroj: [vlastný])

Cenzúra vs. sloboda prejavu

Internet je miesto, kde si ľudia často myslia alebo pociťujú presne to, čo si pod slobodou predstavujú – môžu si robiť, čo chcú, bez následkov. Avšak nie je to ani zďaleka tak. V prípade, že by chceli patriť pod štátnu sféru, musia očakávať podrobnú kontrolu svojich profilov a všetkých interakcií, ktorých na nich v minulosti viedli až niekoľko rokov dozadu.

Ďalší míľnik omylu môže spočívať v predpoklade, že je užívateľom sociálnych sietí na sieťach a Internete samotnom všetko dostupné len to musí viesť nájsť alebo dostať povolenie skrze legálnu platbu alebo taktiež legálne cez iného užívateľa (povolenie k sledovaniu obsahu daného jedinca na sociálnych sieťach). Avšak už v počiatkoch Internetu, keď veľmi známa firma Yahoo zažívala rozkvet ešte, keď súčasný Google neexistoval, ľudia narazili na nutnosť zákonov/pravidiel aj vo virtuálnej sfére. Dovtedy totiž, kyberspace pravidlá nemal a rôzne spoločnosti, aj užívatelia si v podstate mohli robiť, čo chceli. Nebol v tom čase ešte ani na toľko rozvinutý, aby každá domácnosť vlastnila PC alebo internet. Avšak, keď to začalo narážať do meatspace, ukázalo sa, že sloboda, po ktorej ľudstvo neustále túži asi nedokáže existovať v podobe, ktorú by dokázali ako spoločnosť akceptovať. Jedná sa o udalosť, kedy sa skrze vyhľadávač Yahoo francúzsky aktivista proti neonacizmu, menom Mark Knobel dostal na ich webe na aukčný server,

kde sa predávali materiály týkajúce sa koncentračných táborov. Rozhodol sa súdiť Yahoo, keďže bolo v rozpore s francúzskymi zákonmi, aby daný obsah bol zdieľaný, šírený a vôbec bolo možné kúpiť niečo také. Yahoo odmietlo obsah stiahnuť. Boli predsa americkou firmou, ktorú nemohli obmedzovať zákony vo Francúzsku. To by znamenalo, že by sa museli prispôbovať všetkým zákonom, ktoré vo svete sú, aby vyhoveľi každej krajine. Pravdepodobne by potom museli prestať existovať. Yahoo sa snažilo dokázať, že nemá dosah nad tým, aby obmedzilo obsah pre Francúzov, pretože nevie presne určiť ich geografickú polohu. Avšak, v Štokholme mala spomínaná firma servery, aby bol web v Európe prístupnejší vo vyššej rýchlosti. Práve tieto servery boli jedným z bodov k súdnej výhre Marka Knobela. Totižto boli dôkazom schopnosti identifikovať polohu užívateľov. Na základe súdnej prehry a ďalších komplikácií nakoniec Yahoo povolilo a produkty z aukčného webu odstránilo. Táto situácia je len kvapkou ukážky toho ako je Internet ovládaný a my si pri tom môžeme myslieť aké je to slobodné miesto. [130]

Cenzúra podľa zákonov danej krajiny je niečo, čo sa z občianskeho hľadiska môže zdať nevinné, keďže daní občania nemajú k obsahu prístup ani normálne v meatspace, avšak ak ide o cenzúru na sociálnych sieťach, je to o niečom inom. [130]

Opakované nahlasovanie obsahu pre násilie, sexuálne alebo inak nevhodné príspevky či profily vedie k odstráneniu daných príspevkov alebo celých profilov. Prípadne k strate kontroly nad užívateľským profilom. Táto strata kontroly sa nazýva blokovanie. Užívateľ stráca prístup k profilu dočasne alebo úplne (môže končiť až odstránením). [131]

Často ale podmienky, ktoré každé sociálne siete majú vytvorené ohľadom tejto situácie, sú veľmi nejasné alebo subjektívne natoľko, že ak ste pre platformu nevyhovujúcim užívateľom, môže vám odoprieť prístup alebo odstrániť profil bez udania pádného dôvodu.

Zatiaľ čo spoločnosť Meta, oproti minulosti, kedy sa nesnažili nevhodný obsah žiadnym spôsobom cenzúrovať, len miestami, kladie na skrývanie a kontrolu oveľa väčší dôraz. Avšak, nie je to práve dokonalé. Rôzni ľudia už prišli na spôsoby ako obohrať systém a napriek pravidlám, bez problémov zverejniť nevhodný obsah. Zároveň sa zvykne stať, že niektorým profilom je daný obsah aj keď nie je kontroverzný zamietnutí, ale iným ten istý typ je povolení. S rovnakým problémom zápasí aj platforma pre tvorcov videí, YT. Nieкого potrestajú tvrdo za niečo, čo ani nespravil, ale oni si myslia, že áno, niekomu zas toho veľa prechádza. Oni problém s nevhodným obsahom riešia oveľa prísnejšie ako iné platformy. Zatiaľ čo na iných miestach sa môžu objavovať vulgarizmy bez problémov, YT netoleruje žiadne, rovnako aj určité špecifické slová musia tvorcovia cenzúrovať zvukmi

alebo nahradzovať inými výrazmi. Dobrým príkladom je slovo „samovražda“, ktorú youtuberi nahradzujú výrazom „sebanežitie“. [67][132][133][67]

X, platforma na spôsob Facebooku, ale rozšírená viac v Amerike ako v Európe, pred tým ako ju kúpil Elon Musk sa volala Twitter a tiež tam vládla určitá cenzúra voči prejavom násilia, sexuálnemu obsahu alebo nenávisti. Po jeho kúpe, Musk odblokoval profily známym osobnostiam, ktoré boli obvinené z rôznych týchto prečinov voči ľudskosti a v podstate zaviedol takmer absolútnu slobodu. [10][101][102]

Telegram si však nesie najdlhšiu históriu slobodného prejavu vo svojej existencii. Je to prevažne chatovacia služba, ale používajú ju aj známe osobnosti na šírenie svojich myšlienok, presvedčení či ideológií. Ukážka jeho vernosti k súkromiu a bezpečiu sa ukázala už v jeho počiatku, kedy jej majiteľ pôvodom z Ruska odmietol odovzdať svojej rodnej zemi informácie o jej užívateľoch a následne musel utiecť do Nemecka. [10][101][102]

Obe platformy už boli spomenuté v podkapitole o extrémistických sociálnych sieťach.

Cenzúra násilia a nenávisti je v spoločnosti medzi ľuďmi vo veľkej miere akceptovaná. Kontroverznou sa až stáva tzv. prísna cenzúra, ktorá vládne v krajinách ako sú Rusko, Čína a Severná Kórea. V Rusku a Číne je to o to viac nebezpečné, lebo sa krajiny tvária ako demokratické, aspoň pre svojich občanov, zatiaľ čo pre svet ide o zjavnú ukážku diktatúry. [134][135][136]

Digitálny priestor sa stal nielen miestom pre voľnú výmenu názorov, ale aj bojiskom pre ochranu súkromia, právne zodpovednosti platforiem a stabilitu pre smer verejnosti. Ochrana osobných údajov prostredníctvom GDPR, nové povinnosti platforiem podľa DSA a nadchádzajúce regulácie v oblasti umelej inteligencie ukazujú snahu legislatívy držať krok s rýchlym technologickým vývojom. [8][93][110]

Zároveň sa však čoraz viac ukazuje, že zásahy do fungovania sociálnych sietí – hoci motivované ochranou používateľov – môžu naraziť na hranice slobody prejavu. Otázka, kde končí ochrana pred škodlivým obsahom a kde začína cenzúra, sa tak stáva kľúčovou výzvou pre budúcnosť digitálnej regulácie. Je preto nevyhnutné, aby sa právne rámce nielen technicky prispôbovali realite, ale aj zachovávali rovnováhu medzi bezpečnosťou a základnými právami občanov.

Kapitola sa zaoberá kľúčovými otázkami súvisiacimi s bezpečnosťou v online prostredí, predovšetkým na sociálnych sieťach. V úvode je pozornosť venovaná ochrane osobných údajov, kde je rozpracovaná implementácia nariadenia GDPR a jeho vplyv na digitálne platformy. Zdôrazňujú sa práva používateľov, povinnosti prevádzkovateľov a uvádzajú sa konkrétne prípady, na ktorých je ilustrovaný význam zodpovedného nakladania s dátami.

Zároveň sú analyzované súčasné formy digitálnej regulácie v rámci EÚ aj mimo nej, pričom sú predstavené nové legislatívne nástroje zamerané na posilnenie transparentnosti a bezpečnosti online priestoru. Ďalšou rozoberanou témou je problematika cenzúry a slobody prejavu – sú zhodnotené konkrétne zásahy do online obsahu a porovnávané prístupy jednotlivých platforiem. Upozorňuje sa na etickú dilemu medzi ochranou používateľov a zachovaním slobody slova, ako aj na rozdiely medzi demokratickými a autoritárskymi modelmi digitálnej regulácie.

Kapitola tak pokrýva právne, technologické a spoločenské aspekty bezpečnosti, pričom je kladený dôraz na potrebu hľadania rovnováhy medzi účinnou reguláciou a ochranou základných práv v digitálnom priestore.

4 MYLNÉ PREDSTAVY AKO PREKÁŽKA KYBERBEZPEČNOSTI

Táto kapitola sa zameriava na jeden z faktorov, ktorý síce nie je technický ani legislatívny, no výrazne ovplyvňuje úroveň kyberbezpečnosti – a tým sú mylné predstavy samotných užívateľov. Kým predchádzajúce časti práce sa venovali konkrétnym typom rizík a ich následným dopadom, tu sa pozornosť presúva na to, ako tieto riziká vnímajú ľudia a prečo ich často podceňujú. Práve tieto skreslené predstavy spôsobujú, že mnohé hrozby zostávajú nepovšimnuté alebo sú neriešené. Kapitola tak otvára tému psychologických a spoločenských bariér, ktoré bránia prevencii a robia z používateľského správania jeden z najzraniteľnejších bodov online priestoru.

V praxi sa totiž často ľudia stretávajú s tým, že užívatelia jednotlivé riziká, ktoré boli v predchádzajúcich kapitolách rozoberané, ignorujú alebo ich nepovažujú za dôležité. Tým pádom sa im ani nesnažia predchádzať. Objavujú sa rôzne mylné predstavy, ktoré bránia preventívnemu správaniu. Napríklad častý je postoj, že pokiaľ niečo nie je vidieť, neexistuje to. Toto nastavenie ohľadom „neviditeľnosti“ daných rizík vedie k pasivite – ak niekto osobne nezažil problém, môže mať pocit, že sa ho to netýka.

Rovnako sa stále dá stretávať s ilúziou anonymity a súkromia, hoci každá online aktivita zanecháva digitálnu stopu, ktorú môže ktokoľvek aj s menšou znalosťou o zraniteľnosti platforiem, zneužiť. Ďalšou častou chybou je viera, že sociálne siete sú zadarmo a „bez následkov“. V skutočnosti sa za siete platí, len inak, akoby jej užívatelia predpokladali. Platia svojimi údajmi, pozornosťou alebo správaním, ktoré sa stáva súčasťou obchodného modelu platformy.

Tieto platformy často využívajú sofistikované algoritmy, ktoré síce pôsobia neutrálne, ale v skutočnosti cielene pracujú s užívateľovými emóciami. Vyvolávajú silné reakcie, polarizujú názory a neustále svojich užívateľov stimulujú – čím zvyšujú pravdepodobnosť závislosti, preťaženia, pocitu menejcennosti alebo nerealistických porovnávaní.

Nie je pravda, že digitálna manipulácia sa týka len mladších, výrazne starších alebo menej skúsených používateľov. Algoritmy sú navrhnuté tak, aby zasiahli každého – bez ohľadu na vek, vzdelanie alebo technické zručnosti. Riziková je aj prílišná dôvera v umelú inteligenciu, ktorá má svoje limity a nedokáže nahradiť zodpovedné ľudské rozhodovanie.

Záverom tejto kapitoly sa nesie myšlienka, že technológie ľuďstvu síce ponúkajú množstvo výhod, ale samy o sebe nie sú zárukou pozitívneho vplyvu. Ak chýba kritické myslenie, uvedomenie si rizík a ochota meniť svoje digitálne správanie, môže sa aj ten najpokročilejší nástroj obrátiť proti ľuďstvu. Preto je dôležité venovať pozornosť nielen právnym a technickým riešeniam, ale aj psychologickým a spoločenským súvislostiam, ktoré často riziká ešte viac prehľbujú. Riziká, ktoré zo začiatku ovplyvňujú len jednotlivca sa však môžu rýchlo rozšíriť aj na širšiu skupinu užívateľov.

V teoretickej časti v prvej kapitole s názvom Sociálne siete sa čitatelia zoznámili s pojmom sociálne siete, ako ovplyvnili ľudstvo v zmene spôsobe komunikácie, jej rýchlosti, efektivity a vplyve na psychické zdravie. Ďalej bola priblížená typológia sietí, zoznámenie sa s rizikovým správaním užívateľov a podrobnejšie rozobratie psychologických dopadov sociálnych sietí na ich užívateľov. Posledným bodom bolo zoznámenie sa s fungovaním obchodného modelu, na ktorom fungujú sociálne siete.

V kapitole Bezpečnostné hrozby na sociálnych sieťach a analýza rizík sa čitateľ zoznamuje s manipuláciou a jej rôznych foriem, medzi ktoré patrí aj sociálne inžinierstvo. Rozoberá sa problematika nepravdivých informácií, prevažne hoaxov a dezinformácií a následne sa vo väčšej miere zameriava na únik informácií, ktorý je veľkým bodom zlomu na sociálnych sieťach. Kapitulu uzatvára zoznámenie sa s metódami, ktoré sú neskôr použité v praktickej časti pre analýzu vybraných rizík.

V tretej kapitole s názvom Vybrané aspekty bezpečnosti sa bližšie rozoberá otázka cenzúry, ktorá bola načrtnutá v predchádzajúcej kapitole. Rovnako sa kladie dôraz na ochranu osobných údajov a predstavujú sa bezpečnostné opatrenia, ktoré EÚ uplatňuje pre sociálne siete.

Teoretickú časť uzatvára kapitola Mylné predstavy ako prekážka digitálnej bezpečnosti. V kapitole sa predstavujú konkrétne mylné predstavy, ktorým ľudia veria a z toho dôvodu často podceňujú riziká a nebezpečenstvá, ktoré na sieťach hrozia.

II PRAKTICKÁ ČÁST

5 ANALÝZA VYBRANÝCH RIZÍK NA SOCIÁLNÝCH SÍŤÁCH

Sociálne siete sa stali neoddeliteľnou súčasťou každodenného života jednotlivcov aj väčších spoločností. Ich časté užívanie však prináša rôzne riziká, ktoré môžu ohroziť bezpečnosť údajov, súkromie užívateľov alebo dokonca, bezpečie firiem. Kapitola sa zameriava na identifikáciu a rozbor jednotlivých vybraných rizík, ktoré sú spojené s užívaním sociálnych sietí. Cieľom je poukázať na najčastejšie riziká a predostrieť možné opatrenia, ktoré pomôžu buď zmierniť, alebo ich až eliminovať.

Zoznam vybraných rizík na sociálnych siet'ach spomínaných v teoretickej časti:

- a) Phishing
- b) Pharming
- c) Únik údajov
- d) Zneužitie zraniteľnosti
- e) Slabá autentifikácia
- f) Porušenie GDPR
- g) Nesprávne zdieľanie údajov
- h) Nejasné podmienky predplatného
- i) Závislosť používateľov od siete
- j) Sociálne porovnávanie a psychická nepohoda
- k) Dezinformačné a informačné bubliny
- l) Dopamínová slučka a kompulzívne správanie
- m) Fomo a tlak na neustálu online prítomnosť
- n) Parasociálne vzťahy s influencerami
- o) Prienik účtov

Metóda CARVER je v práci použitá:

- a) Phishing
- b) Pharming (z pohľadu útočníka)
- c) Únik údajov

- d) Zneužitie zraniteľnosti
- e) Prienik účtov

Modifikovaná metóda FMEA/PNH je použitá na:

- a) Porušenie GDPR
- b) Nesprávne zdieľanie údajov
- c) Nejasné podmienky predplatného
- d) Pharming (z pohľadu systému)
- e) Slabá autentifikácie

Metóda KARS je použitá na:

- a) Závislosť používateľov od siete
- b) Fomo a tlak na neustálu online prítomnosť
- c) Dopamínová slučka a kompulzívne správanie
- d) Parasociálne vzťahy s influencerami
- e) Sociálne porovnávanie a psychická nepohoda
- f) Dezinformačné a informačné bubliny

5.1 Metóda CARVER

a) Phishing

Faktor	Hodnota	Popis
Kritickosť	5	Získanie prihlasovacích údajov môže viesť k strate prístupu a citlivých dát
Prístupnosť	5	Phishingové e-maily sú ľahko rozosielateľné, často bez odhalenia
Obnoviteľnosť	4	Po odhalení phishingu je ťažké zabrániť zneužitiu údajov
Zraniteľnosť	5	Používatelia sú často náchylní kliknúť na podvodný obsah bez overenia
Vplyv	5	Útok môže spôsobiť ekonomické a reputačné škody
Rozpoznateľnosť	4	Podvodné správy bývajú často nerozoznateľné od skutočných

Tabuľka 13 Spracovanie metódy CARVER pre phishing

(Zdroj: [vlastný])

Vyhodnotenie metódy CARVER pre phishing

Číslo 28 sa stalo referenčnou hodnotou a poukazuje na kritický význam rizika. Vysokú hodnotu si nesie hlavne v oblastiach kritickosti, prístupnosti a dopadu.

Záver: Z týchto zistení vyplýva, že ide o jeden z najzávažnejších typov sociálneho inžinierstva s potenciálom narušiť nielen jednotlivcov, ale aj celé organizácie. Prevencia by mala zahŕňať edukáciu používateľov, technické filtre a systém včasného varovania.

b) Pharming

Faktor	Hodnota	Popis
Kritickosť	5	Získané prihlasovacie údaje môžu útočníkovi sprístupniť účty a bankové financie
Prístupnosť	4	Presmerovanie na falošnú stránku môže prebehnúť bez vedomia používateľa
Obnoviteľnosť	5	Po zadaní údajov nie je možné získať ich späť – sú kompromitované
Zraniteľnosť	4	Slabé zabezpečenie DNS alebo nedostatok HTTPS ⁴ zvyšuje riziko
Vplyv	5	Finančné straty a strata dôvery sú bežným dôsledkom
Rozpoznateľnosť	4	Používateľ si často neuvedomí, že navštívil falošný web

Tabuľka 14 Spracovanie metódy CARVER pre pharming

(Zdroj: [vlastný])

Vyhodnotenie metódy CARVER pre pharming

Číslo 27 sa stalo referenčnou hodnotou a poukazuje na kritický význam rizika. Vysokú hodnotu si nesie hlavne v oblastiach kritickosti, obnoviteľnosti a dopadu.

Záver: Z týchto zistení vyplýva, že ide o útok s vysokou prioritou, ktorý by mal byť riešený kombináciou technických opatrení a osvetou.

⁴ Zabezpečený protokol pre prenos údajov na internete

c) Únik údajov

Faktor	Hodnota	Popis
Kritickosť	5	Užívateľ stráca svoje súkromie, bezpečie, financie alebo aj reputáciu.
Prístupnosť	4	Prístup často cez zraniteľný systém, slabé zabezpečenie
Obnoviteľnosť	5	Po úniku je veľmi ťažké alebo nemožné údaje dostať späť
Zraniteľnosť	4	Systémy často nie sú dostatočne chránené, slabá kontrola prístupov
Vplyv	5	Dôsledky môžu byť právne, reputačné aj ekonomické
Rozpoznateľnosť	4	Únik údajov môže zostať dlho neodhalený – nie je hneď viditeľný.

Tabuľka 15 Spracovanie metódy CARVER pre únik údajov

(Zdroj:[vlastný])

Vyhodnotenie metódy CARVER pre únik údajov

Číslo 27 sa stalo referenčnou hodnotou a poukazuje na kritický význam rizika. Vysokú hodnotu si nesie hlavne v oblastiach kritickosti, obnoviteľnosti a dopadu.

Záver: Z týchto zistení vyplýva, že ide o jeden z najkritickejších incidentov, keďže dôsledky sú trvalé. Krokom k väčšiemu bezpečiu je dôsledná kontrola prístupov, šifrovanie údajov a detekčné mechanizmy.

d) Zneužitie zraniteľnosti

Faktor	Hodnota	Popis
Kritickosť	5	Získanie kontroly nad systémom alebo dátami môže ochromiť organizáciu
Prístupnosť	4	Verejne známe chyby sú ľahko prístupné útočníkom cez internet
Obnoviteľnosť	4	Obnova po útoku môže byť náročná a časovo zdĺhavá
Zraniteľnosť	5	Chýbajúce aktualizácie a záplaty predstavujú veľké riziko
Vplyv	5	Útok môže spôsobiť odstávku služieb a únik dát
Rozpoznateľnosť	3	Útoky môžu ostať nepozorované, ak chýbajú monitorovacie nástroje

Tabuľka 16 Spracovanie metódy CARVER pre zneužitie zraniteľnosti

(Zdroj: [vlastný])

Vyhodnotenie metódy CARVER pre zneužitie zraniteľnosti

Číslo 26 sa stalo referenčnou hodnotou a poukazuje na kritický význam rizika. Vysokú hodnotu si nesie hlavne v oblastiach kritickosti, zraniteľnosti a dopadu.

Záver: Z týchto zistení vyplýva, že vysokou prioritou by malo byť technické riešenie zraniteľnosti. Jedným z odporúčaní pre predchádzaniu takémuto typu útoku je audit softvérov a penetračné testy.

e) Prienik účtov

Faktor	Hodnota	Popis
Kritickosť	5	Útočník môže získať prístup k osobným alebo firemným účtom
Prístupnosť	4	Slabé heslá alebo opakované heslá uľahčujú prístup
Obnoviteľnosť	5	Obnova účtu môže byť časovo náročná alebo nemožná bez overenia identity
Zraniteľnosť	4	Mnohé účty nemajú aktivované dvojfaktorové overenie
Vplyv	5	Prienik môže spôsobiť reputačné škody, finančné straty a šírenie malvéru
Rozpoznateľnosť	5	Neoprávnený prístup môže byť odhalený až po čase

Tabuľka 17 Spracovanie metódy CARVER pre prienik účtov

(Zdroj: [vlastný])

Vyhodnotenie metódy CARVER pre prienik účtov

Číslo 28 sa stalo referenčnou hodnotou a poukazuje na kritický význam rizika. Vysokú hodnotu si nesie hlavne v oblastiach kritickosti, zraniteľnosti a dopadu.

Záver: Z týchto zistení vyplýva, že získanie prístupu k účtom môže viesť k rýchlemu zneužitiu osobných alebo pracovných údajov. Bezpečnostné odporúčania sú zaviesť dvojfaktorové overenie, pravidelné menenie hesiel a analyzovať pokusy o prienik.

Záver metódy CARVER

Metóda CARVER preukázala svoju vhodnosť na hodnotenie bezpečnostných incidentov v digitálnom prostredí. Výsledky môžu slúžiť ako pre návrh konkrétnych bezpečnostných opatrení k zabráneniu zbytočných útokov, ktoré sa skrze známe riziká a ich zhodnotenie dá predísť.

Možno konštatovať, že daná metóda pomohla systematicky vyhodnotiť, ktoré riziká si vyžadujú najvyššiu prioritu v rámci ochrany používateľov sociálnych sietí, a poskytla kvalitný podklad pre ďalšiu analytickú aj praktickú prácu.

Riziko	C	A	R	V	E	R	Referenčná hodnota
Phishing	5	5	4	5	5	4	28
Pharming	5	4	5	4	5	4	27
Únik údajov	5	4	5	4	5	4	27
Zneužitie zraniteľnosti	5	4	4	5	5	3	26
Prienik účtov	5	4	5	4	5	5	28

Tabuľka 18 Závrer metódy CARVER

(Zdroj: [vlastný])

Riziko	Možná příčina	Dôsledok	Závažnosť následkov (N)	Pravdepodobnosť vzniku rizika (P)	Odhaliteľnosť rizika (H)
Porušenie GDPR	Nedostatočné zabezpečenie údajov, chýbajúca kontrola súhlasov	Pokuta od ÚOOÚ ⁵ , strata dôvery používateľov	5	3	3
Nesprávne zdieľanie údajov	Neúmyselné sprístupnenie informácií verejnosti alebo nesprávnym osobám	Únik údajov, reputačné škody	4	4	4
Nejasné podmienky predplatného	Automatická obnova, neprehľadná zmluva	Nechcené platby, nespokojnosť používateľov	3	4	3
Pharming (systémová chyba)	Slabá DNSSEC ⁶ ochrana, chýbajúce certifikáty	Presmerovanie na falošný web, odcudzenie údajov	5	3	4
Slabá autentifikácia	Jednoduché heslá, chyba 2FA ⁷ (dvojfaktorové overenie)	Neautorizovaný prístup, zneužitie identity.	5	4	4

Tabuľka 19 Rozobratie jednotlivých rizík pomocou metódy FMEA/PNH

(Zdroj: [vlastný])

⁵ Úrad na ochranu osobných údajov⁶ Domain Name System Security Extensions (Bezpečné rozšírenie DNS)

Riziko	Miera rizika	Prijateľnosť rizika
Porušenie GDPR	45	Podmienečne prijateľné
Nesprávne zdieľanie údajov	64	Neprijateľné
Nejasné podmienky predplatného	36	Podmienečne prijateľné
Pharming (systémová chyba)	60	Neprijateľné
Slabá autentifikácia	80	Neprijateľné

Tabuľka 20 Vyhodnotenie rizík metódy FMEA/PNH

(Zdroj: [vlastný])

Záver modifikovanej metódy FMEA/PNH

Modifikovaná metóda FMEA/PNH bola použitá na analýzu rizík, ktoré vyplývajú najmä z procesných, systémových nedostatkov a chýb, ktoré spôsobí ľudský faktor pri používaní sociálnych sietí.

Z výslednej prijateľnosti rizika, ktorá je podmienená mierou rizika sa dá ľahko usúdiť, že dané riziká sú veľkým problémom pre bezpečnosť a ani jedno z daných rizík sa nedá brať na ľahkú váhu. 3 z 5-tich uvedených rizík boli vyhodnotené ako neprijateľné a teda vyžadujú okamžitý zákrok k vytvoreniu opatrení. Najväčšie riziko predstavuje slabá autentifikácia. Pharming a nesprávne zdieľanie údajov tiež predstavujú na základe využitej metódy neprijateľné riziko.

Výsledky metódy FMEA/PNH môžu byť podkladom pre plánovanie kontrolných mechanizmov a revíziu vnútorných procesov na zníženie zraniteľnosti.

Riziko	N	P	H	Miera rizika	Prijateľnosť rizika
Porušenie GDPR	5	3	3	45	Podmienečne prijateľné
Nesprávne zdieľanie údajov	4	4	4	64	Neprijateľné
Nejasné podmienky predplatného	3	4	3	36	Podmienečne prijateľné
Pharming (systémová chyba)	5	3	4	60	Neprijateľné
Slabá autentifikácia	5	4	4	80	Neprijateľné

Tabuľka 21 Záver modifikovanej metódy FMEA/PNH

(Zdroj: [vlastný])

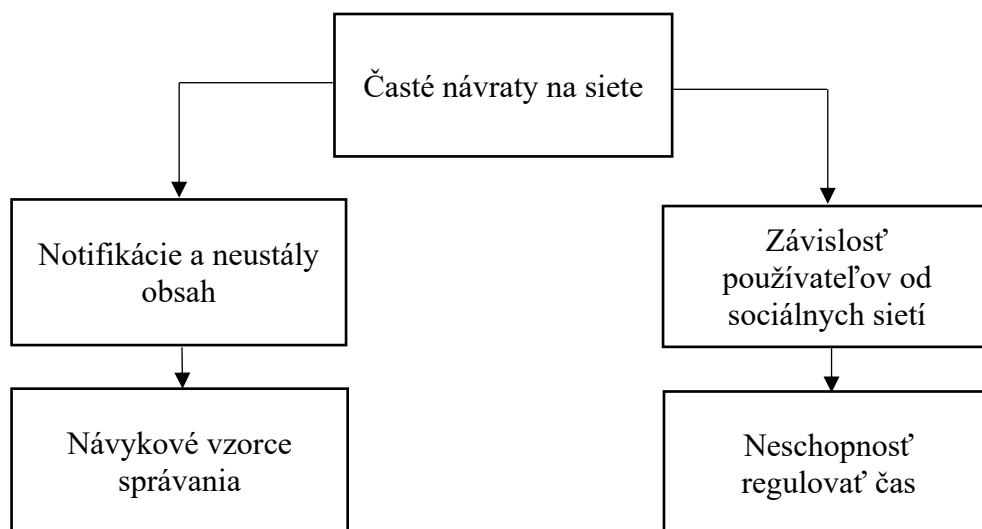
Metóda KARS

a) Závislosť používateľov od siete

Slovný popis:

Ak sa používateľ opakovane vracia na sociálnu sieť kvôli notifikáciám a neustálemu obsahu, môže si vytvoriť návykové vzorce správania, čo vedie k závislosti od siete a neschopnosti regulovať čas online.

Grafická forma:



Obrázok 5 Grafická forma pre závislosť používateľov od siete

(Zdroj: [vlastný])

Riziko		1	2	3	4	5	Súčet
1	Časté návraty na sieť	0	0	1	1	1	3
2	Notifikácie a neustály obsah	1	0	1	1	1	4
3	Návykové vzorce správania	1	1	0	1	1	4
4	Závislosť používateľov od sociálnych sietí	1	1	1	0	1	4
5	Neschopnosť regulovať čas	1	1	1	1	0	4
Súčet		4	3	4	4	4	

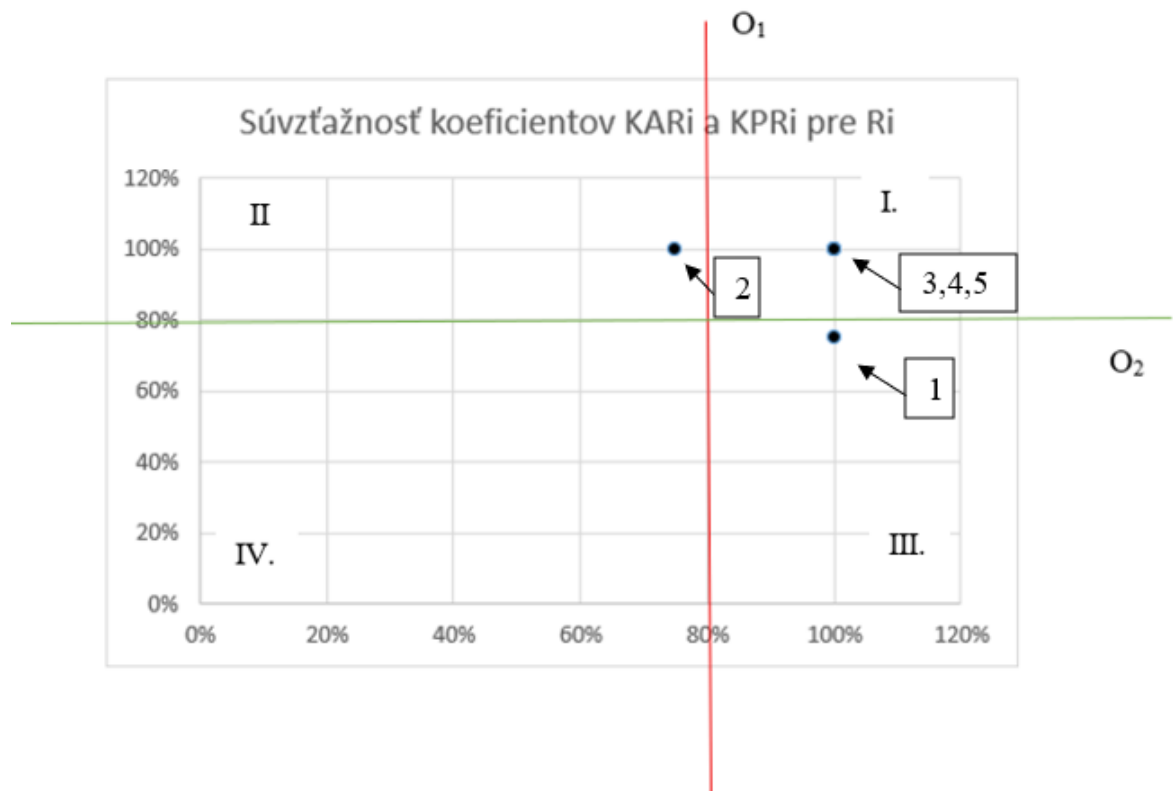
Tabuľka 22 Metóda Kars aplikovaná pre riziká závislosti používateľov od siete

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR_i [%]	75%	100%	100%	100%	100%
KPR_i [%]	100%	75%	100%	100%	100%

Tabuľka 23 Percentuálne vyhodnotenie rizík závislosti používateľov od siete

(Zdroj: [vlastný])



Graf 4 Súvzťažnosť koeficientov KARi a PRi pre Ri závislosti používateľov na sieti

(Zdroj: [vlastný])

	Oblasť	Riziko	Charakteristika	Záver
1	I – primárne a sekundárne nebezpečné riziká	3 (návykové vzorce správania), 4 (závislosť používateľov od sociálnych sietí), 5 (neschopnosť regulovať čas)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a sú ovplyvňované	Najkritickejšie riziká, prioritne riešiť
2	II – sekundárne riziká	2 (notifikácie a neustály obsah)	Vysoké KPR, nízke KAR – silne ovplyvňované, málo ovplyvňujú	Citlivé na vplyvy, sledovať a riešiť príčinné riziká
3	III – primárne riziká	1 (závislosť používateľov na sieti)	Vysoké KAR, nízke KPR – ovplyvňujú, ale nie sú výrazne ovplyvňované	Spúšťač rizík, preventívne zasiahnuť

Tabuľka 24 Vyhodnotenie výsledkov metódy KARS pre závislosť používateľov na sieti

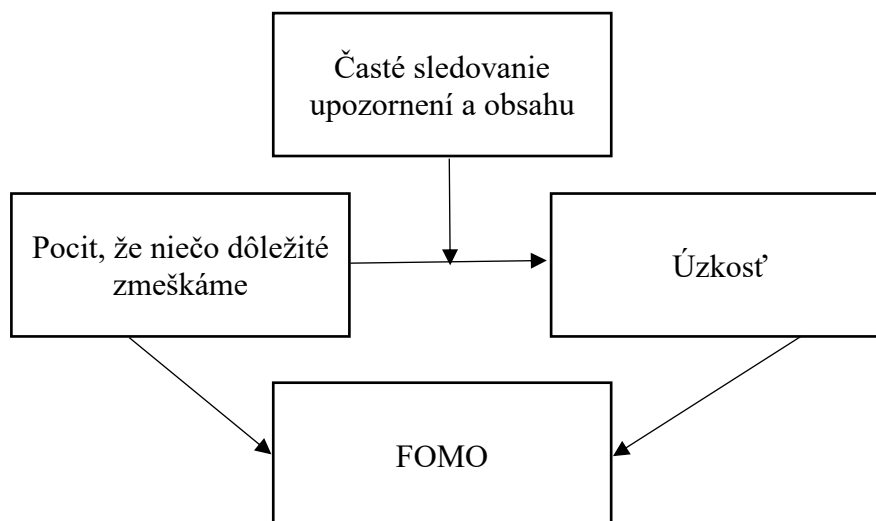
(Zdroj: [vlastný])

b) FOMO a tlak na neustálu online prítomnosť

Slovný popis:

Ak používateľ vníma, že ostatní neustále niečo zažívajú alebo zdieľajú, vzniká obava z premeškania. Táto úzkosť vedie k neustálemu kontrolovaniu aplikácií, čo spôsobuje stres a zhoršuje koncentráciu.

Grafická forma:



Obrázok 6 Grafická forma FOMO a tlak na neustálu online prítomnosť

(Zdroj: [vlastný])

Riziko		1	2	3	4	Súčet
1	Časté sledovanie upozornení a obsahu	0	1	1	1	3
2	Pocit, že niečo dôležité zmeškáme	1	0	1	1	3
3	FOMO	1	1	0	1	3
4	Úzkosť	1	1	1	0	3
Súčet		3	3	3	3	

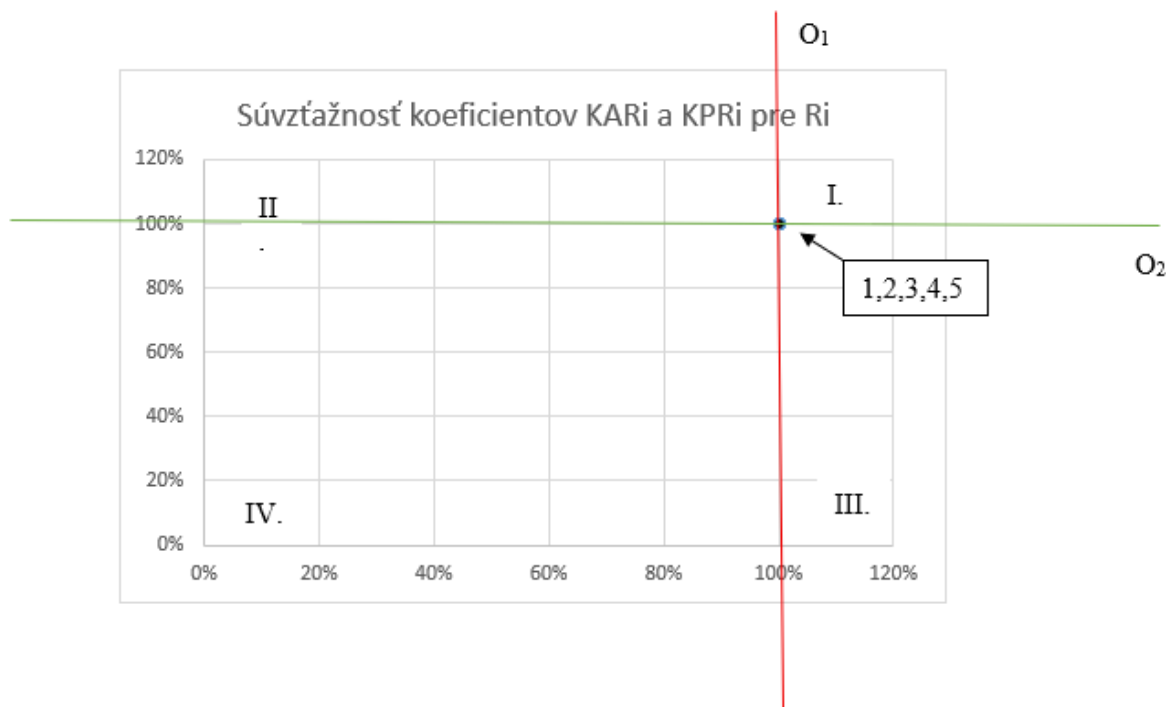
Tabuľka 25 Metóda Kars aplikovaná pre riziká FOMO a tlak na neustálu online prítomnosť

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR_i [%]	100%	100%	100%	100%	100%
KPR_i [%]	100%	100%	100%	100%	100%

Tabuľka 26 Percentuálne vyhodnotenie rizík FOMO a tlak na neustálu online prítomnosť

(Zdroj: [vlastný])



Graf 5 Súvzťahnosť koeficientov KARi a PRi pre Ri FOMO a tlak na neustálu online prítomnosť

(Zdroj: [vlastný])

Oblasť	Riziko	Charakteristika	Záver
I – primárne a sekundárne nebezpečné riziká	1-5 (všetky hodnotené riziká v danej kategórii)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a zároveň sú nimi silno ovplyvňované	Najkritickejšie riziká, vyžadujú najvyššiu prioritu, monitorovať a riadiť

Tabuľka 27 Vyhodnotenie výsledkov metódy KARS pre FOMO a tlak na neustálu online prítomnosť

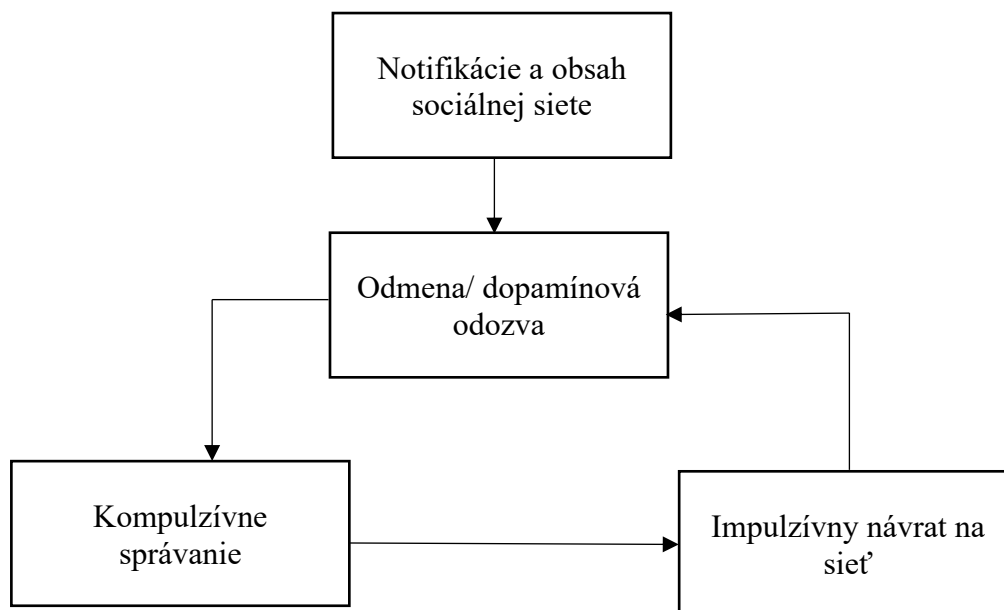
(Zdroj: [vlastný])

c) Dopamínová slučka a kompulzívne správanie

Slovný popis:

Ak algoritmus opakovane odmeňuje používateľa za scrollovanie, zdieľanie a reakcie, vzniká cyklus odmeňovania dopamínom. Ten podporuje nutkavé správanie a vedie k zníženiu sebaregulácie.

Grafická forma:



Obrázok 7 Grafická forma dopamínovej slučky a kompulzívneho správania

(Zdroj: [vlastný])

Riziko		1	2	3	4	Súčet
1	Notifikácie a obsah sociálnej siete	0	1	1	1	3
2	Odmena/dopamínová odozva	1	0	1	1	3
3	Kompulzívne správanie	1	1	0	1	3
4	Impulzívny návrat na sieť	1	1	1	0	3
Súčet		3	3	3	3	

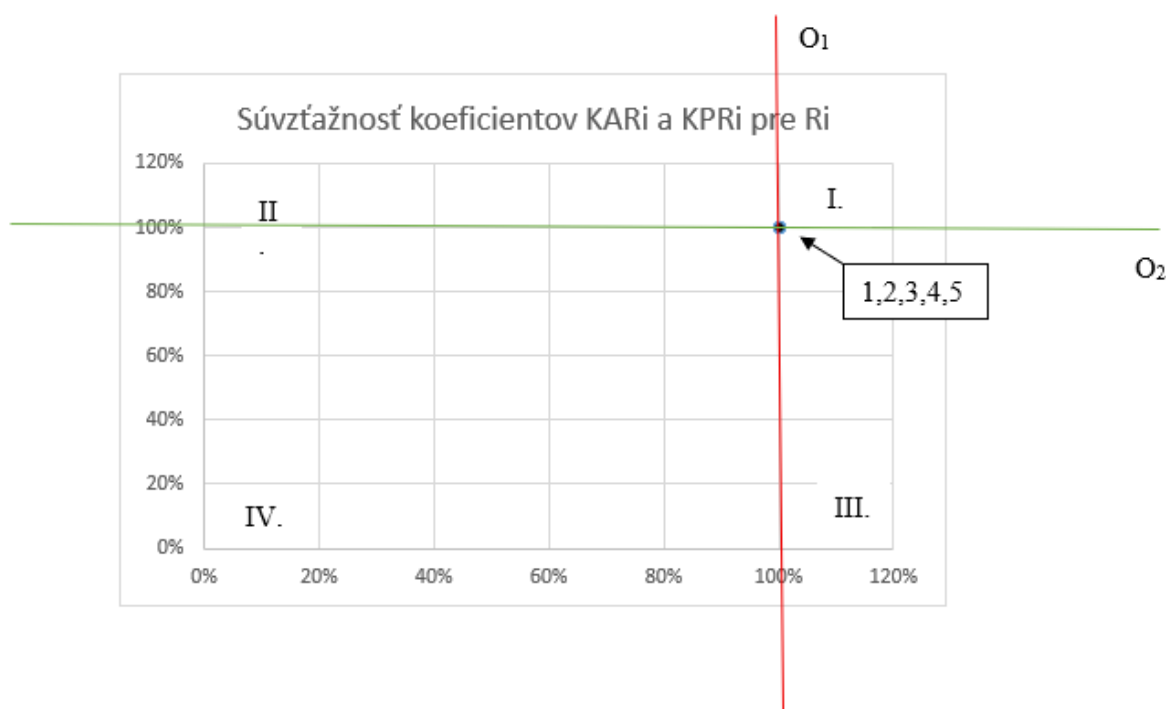
Tabuľka 28 Metóda Kars aplikovaná pre riziká dopamínovej slučky a kompulzívneho správania

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR_i [%]	100%	100%	100%	100%	100%
KPR_i [%]	100%	100%	100%	100%	100%

Tabuľka 29 Percentuálne vyhodnotenie rizík dopamínovej slučky a kompulzívneho správania

(Zdroj: [vlastný])



Graf 6 Súvzťažnosť koeficientov KAR_i a KPR_i pre R_i dopamínovej slučky a kompulzívneho správania

(Zdroj: [vlastný])

Oblasť	Riziko	Charakteristika	Záver
I – primárne a sekundárne nebezpečné riziká	1-5 (všetky hodnotené riziká v danej kategórii)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a zároveň sú nimi silno ovplyvňované	Najkritickejšie riziká, vyžadujú najvyššiu prioritu, monitorovať a riadiť

Tabuľka 30 Vyhodnotenie výsledkov metódy KARS pre dopamínovú slučku a kompulzívne správanie

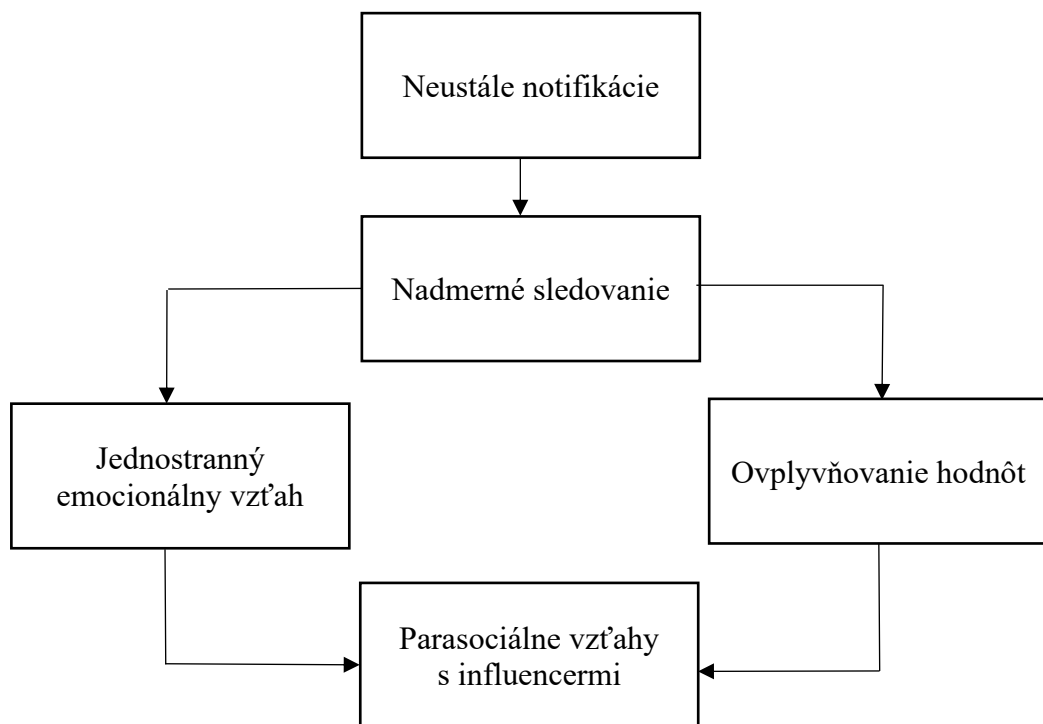
(Zdroj: [vlastný])

d) Parasociálne vzťahy s influencerami

Slovný popis:

Ak používateľ nadväzuje jednostranný emocionálny vzťah s influencerom, môže to viesť k závislosti od jeho obsahu, skreslenej realite a ovplyvneniu vlastných hodnôt alebo rozhodnutí.

Grafická forma:



Obrázok 8 Grafická forma parasociálnych vzťahov s influencerami

(Zdroj: [vlastný])

Riziko		1	2	3	4	5	Súčet
1	Neustále notifikácia	0	1	1	1	1	4
2	Nadmerné sledovanie	1	0	1	1	1	4
3	Jednostranný emocionálny vzťah	0	1	0	1	1	3
4	Ovplyvňovanie hodnôt	0	1	1	0	1	3
5	Parasociálne vzťahy s influencerami	0	1	1	1	0	3
Súčet		1	4	4	4	4	

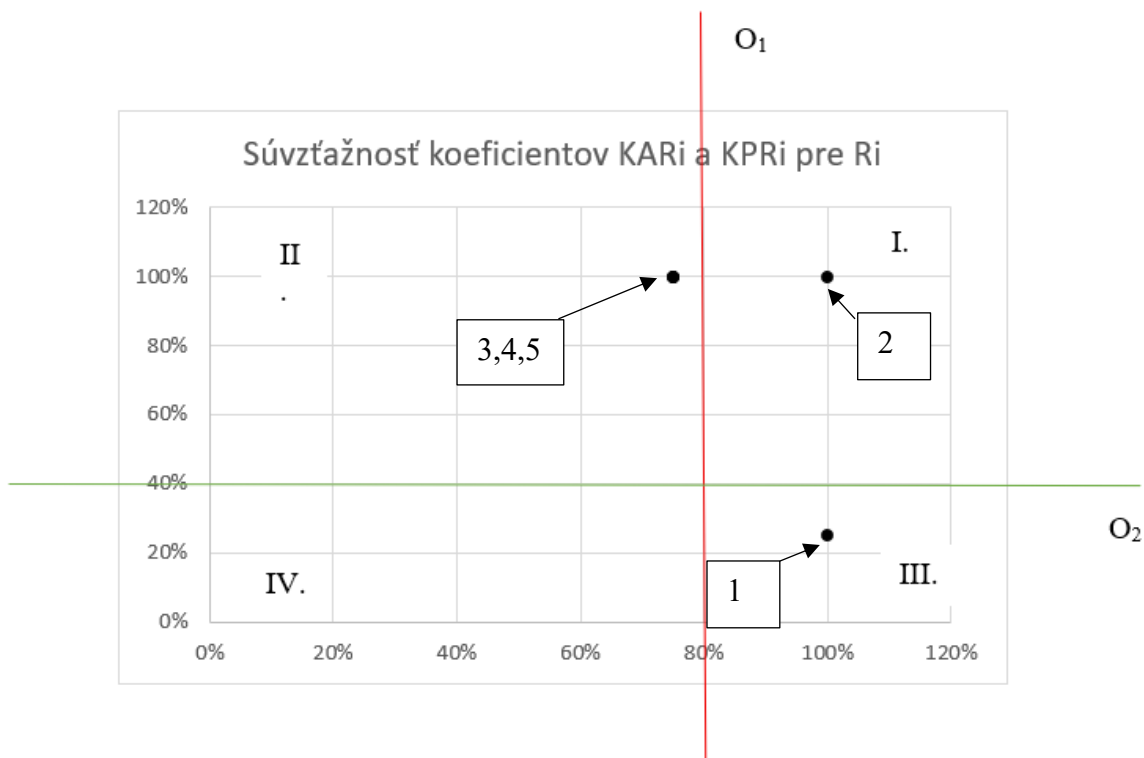
Tabuľka 31 Metóda Kars aplikovaná pre riziká parasociálnych vzťahov s influencerami

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR _i [%]	100%	100%	75%	75%	75%
KPR _i [%]	25%	100%	100%	100%	100%

Tabuľka 32 Percentuálne vyhodnotenie rizík parasociálnych vzťahov s influencerami

(Zdroj: [vlastný])



Graf 7 Súvzťažnosť koeficientov KARi a PRi pre Ri parasociálnych vzťahov s influencerami

(Zdroj: [vlastný])

Oblasť	Riziko	Charakteristika	Záver
I – primárne a sekundárne riziká	2(nadmerné sledovanie)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a sú ovplyvňované	Najkritickejšie riziko, prioritne riešiť a monitorovať
II – sekundárne riziká	3 (jednostranný emocionálny vzťah), 4 (ovplyvňovanie hodnôt), 5 (parasociálne vzťahy s influencerami)	Vysoké KPR, nízke KAR – silne ovplyvňované, málo ovplyvňujú	Citlivé na vplyvy, sledovať a riešiť príčinné riziká
III – primárne riziká	1 (neustále notifikácie)	Vysoké KAR, nízke KPR – ovplyvňujú, ale nie sú výrazne ovplyvňované	Spúšťač rizík, preventívne zasiahnuť

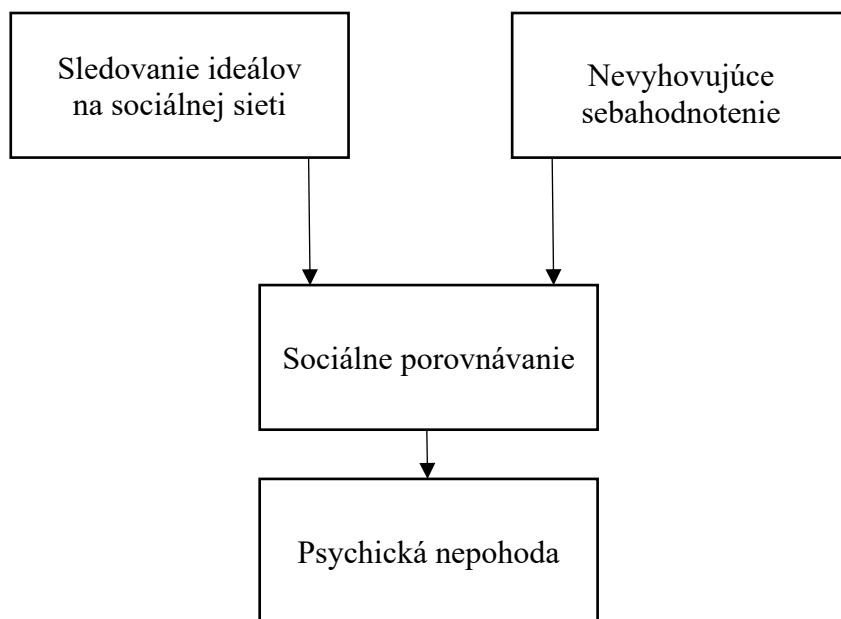
Tabuľka 33 Vyhodnotenie metódy KARS pre parasociálne vzťahy s influencerami

(Zdroj: [vlastný])

e) Sociálne porovnávanie a psychická nepohoda

Slovný popis:

Ak sa používateľ často porovnáva s ideálne vykresleným obsahom iných, môže to spôsobiť pokles sebadôvery, vznik pocitu menejcennosti a dlhodobú psychickú nepohodu.

Grafická forma:

Obrázok 9 Grafická forma sociálneho porovnávania a psychickej nepohody

(Zdroj: [vlastný])

Riziko		1	2	3	4	Súčet
1	Sledovanie ideálov na sociálnej sieti	0	1	1	1	3
2	Nevyhovujúce sebahodnotenie	1	0	1	1	3
3	Sociálne porovnávanie	1	1	0	1	3
4	Psychická nepohoda	1	1	1	0	3
Súčet		3	3	3	3	

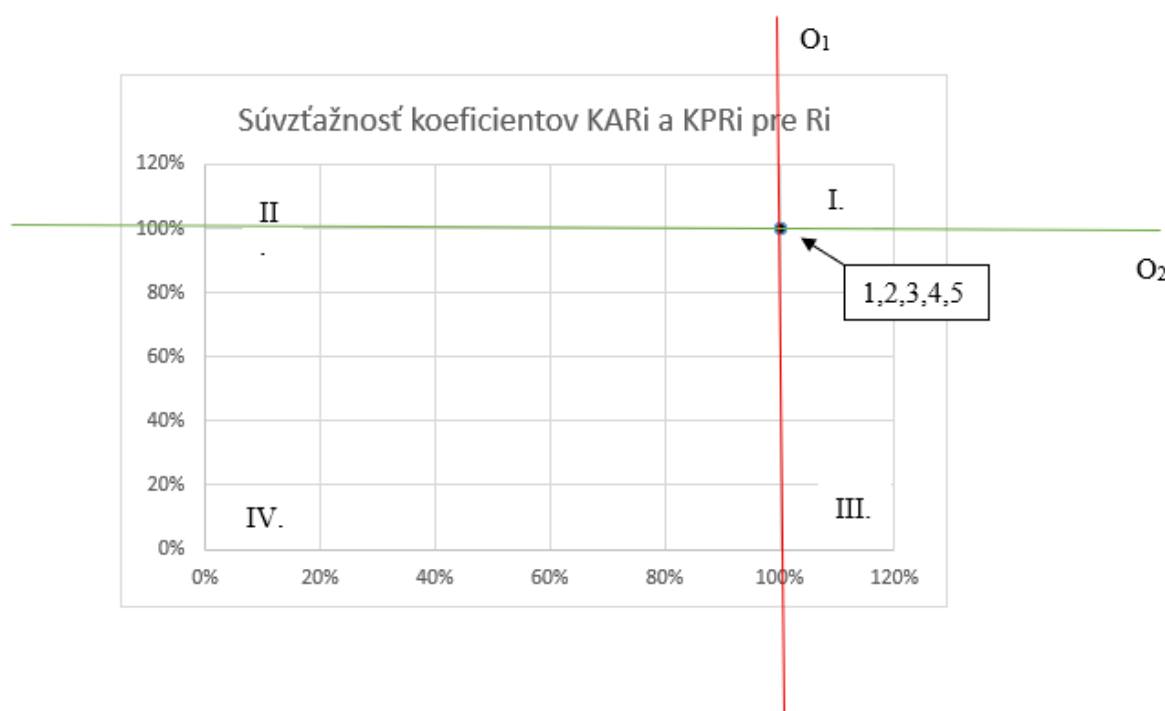
Tabuľka 34 Metóda Kars aplikovaná pre riziká sociálneho porovnávania a psychickej nepohody

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR_i [%]	100%	100%	100%	100%	100%
KPR_i [%]	100%	100%	100%	100%	100%

Tabuľka 35 Percentuálne vyhodnotenie rizík sociálneho porovnávania a psychickej nepohody

(Zdroj: [vlastný])



Graf 8 Súvzťahnosť koeficientov KAR_i a KPR_i pre R_i sociálneho porovnávania a psychickej nepohody

(Zdroj: [vlastný])

	Oblasť	Riziko	Charakteristika	Záver
1	I – primárne a sekundárne nebezpečné riziká	1-5 (všetky hodnotené riziká v danej kategórii)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a zároveň sú nimi silno ovplyvňované	Najkritickejšie riziká, vyžadujú najvyššiu prioritu, monitorovať a riadiť

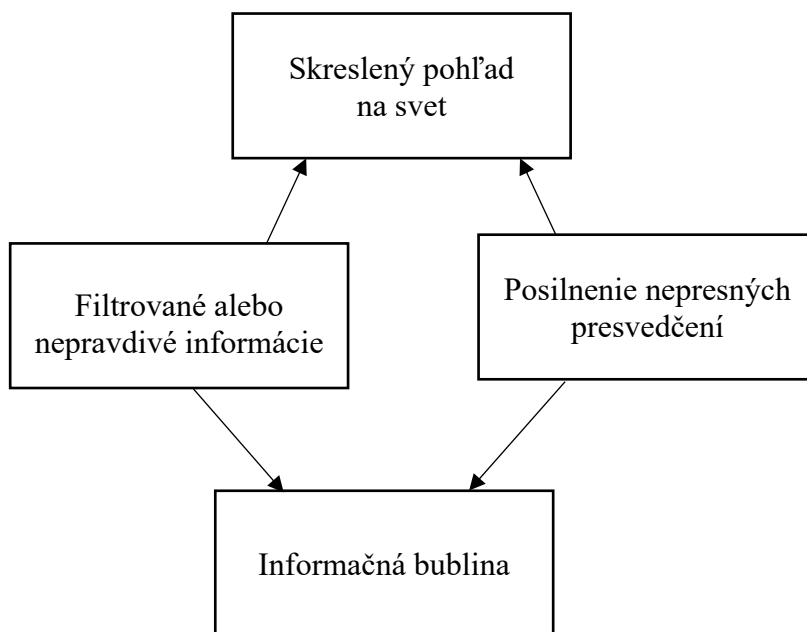
Tabuľka 36 Vyhodnotenie výsledkov metódy KARS pre sociálne porovnanie a psychickú nepohodu

(Zdroj: [vlastný])

f) Dezinformačné a informačné bubliny

Slovný popis:

Ak algoritmus dlhodobo ponúka len obsah potvrdzujúci názory používateľa, vzniká informačná bublina. Tá znižuje schopnosť kriticky myslieť, podporuje polarizáciu a prijímanie nepravdivých informácií.

Grafická forma:

Obrázok 10 Grafická forma dezinformačnej a informačnej bubliny

(Zdroj: [vlastný])

Riziko		1	2	3	4	Súčet
1	Skreslený pohľad na svet	0	1	1	1	3
2	Filtrované alebo nepravdivé informácie	1	0	1	1	3
3	Posilnenie nepresných presvedčení	1	1	0	1	3
4	Informačná bublina	1	1	1	0	3
Súčet		3	3	3	3	

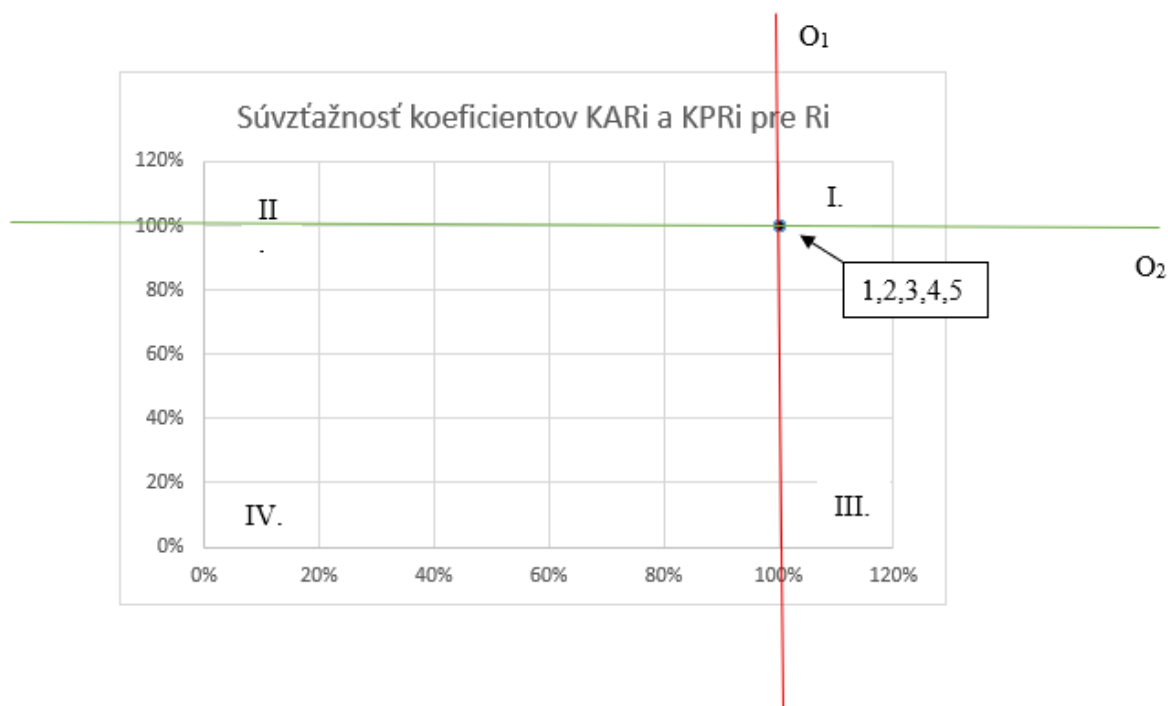
Tabuľka 37 Metóda Kars aplikovaná pre riziká dezinformačnej a informačnej bubliny

(Zdroj: [vlastný])

Riziko R_i	1	2	3	4	5
KAR_i [%]	100%	100%	100%	100%	100%
KPR_i [%]	100%	100%	100%	100%	100%

Tabuľka 38 Percentuálne vyhodnotenie rizík dezinformačnej a informačnej bubliny

(Zdroj: [vlastný])



Graf 9 Súvzťahnosť koeficientov KARi a KPRi pre Ri dezinformačnej a informačnej bubliny

(Zdroj: [vlastný])

	Oblasť	Riziko	Charakteristika	Záver
1	I – primárne a sekundárne nebezpečné riziká	1-5 (všetky hodnotené riziká v danej kategórii)	Vysoká hodnota KAR aj KPR – ovplyvňujú iné riziká a zároveň sú nimi silno ovplyvňované	Najkritickejšie riziká, vyžadujú najvyššiu prioritu, monitorovať a riadiť

Tabuľka 39 Vyhodnotenie výsledkov metódy KARS pre dezinformačné a informačné bubliny

(Zdroj: [vlastný])

Kapitola číslo 5 sa zaoberala uplatnením spomínaných metód v teoretickej časti v praxi. Analyzovala vybrané riziká pomocou metód CARVER, modifikovanou verziou FMEA/PNH a KARS. Pri čom každá bola použitá na riziká podľa jej vhodnosti.

6 SYNTÉZA VYBRANÝCH RIZÍK NA SOCIÁLNÝCH SÍŤACH A NÁVOD K BEZPEČNÉMU SPRÁVANÍ SA

V predchádzajúcej kapitole jednotlivé riziká prešli spracovaním vhodne vybraných metód. V tejto kapitole sa k jednotlivým rizikám priradujú opatrenia, ktoré sú rozdelené v štyroch kategóriach. A síce – technické, organizačné, psychologicko-edukačné opatrenia a právne a regulačné odporúčania.

Navrhnuté technické opatrenie	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Zavedenie časovačov a upozornení na nadmerné používanie aplikácií či samotných zariadení	Závislosť používateľov od siete, FOMO a tlak na neustálu online prítomnosť, dopamínová slučka a kompulzívne správanie,	Užívateľ bude informovaný koľko času trávi v aplikácii/ na zariadení a bude skôr motivovaný skrátený čas dodržiavať.
Obmedzenie nežiaducich a „vyskakovacích“ notifikácií	FOMO a tlak na neustálu online prítomnosť, parasociálne vzťahy s influencerami, dopamínová slučka a kompulzívne správanie	Užívateľ nebude pod tlakom alebo nebude pociťovať toľké nutkanie ihneď zistiť viac, riešiť alebo sa zaťažovať nepodstatnými dátami.
Silné heslá a správca hesiel ako základ	Slabá autentifikácia, prienik účtov	Užívateľov účet bude viac chránený.
Filtrovanie a označovanie dezinformačného obsahu pomocou AI nástrojov	Dezinformačné a informačné bubliny, sociálne porovnávanie	Užívateľ skôr bude vedieť, že sa nejedná o obsah, ktorý chce sledovať a zároveň sieť usúdi, že to nie je obsah, ktorý by sa mal rozširovať.
Viacfaktorová autentifikácia	Únik údajov, prienik účtov, slabá autentifikácia	Do konta užívateľa bude nutné vedieť viac informácií ako len heslo, e-mail či užívateľské meno
Bezpečnostné logy a monitoring podozrivého správania	Zneužitie zraniteľnosti, únik údajov	Ak by sa niekto pokúsil viackrát neúspešne prihlásiť do konta, tak užívateľ bude informovaný. Rovnako aj keby išlo z úplne inej časti sveta.

Tabuľka 40 Navrhnuté technické opatrenia časť 1

(Zdroj: [vlastný])

Navrhnuté technické opatrenie	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Dôraz na aktuálnosť systému, antivírusu a smerovača na zariadení	Pharming	Ak je systém aktuálny, je silnejší a tým pádom odolnejší voči vonkajším vplyvom.
Zavedenie ochranných filtrov na e-mailových serveroch	Phishing, únik údajov	Ak bude správa infikovaná vírusom alebo neoverenou URL adresou, nebude možné správu zaslať.
Automatické odhlásenie používateľa po určitej neaktivite.	Prienik účtov	Pre niektorých nepraktické, ale bezpečné v prípade, keby nad zariadením prevzal kontrolu niekto iný.
Vedieť, kde má systém slabiny	Zneužitie zraniteľnosti	Aby sa v prípade potreby užívateľ mohol v tom smere zabezpečiť svojimi možnosťami.
Používanie DNSSEC a bezpečných protokolov, ktoré zabránia manipulácii s pripojením.	Pharming+	DNSSEC zabezpečuje DNS.
Pravidelné zálohovanie svojich informácií	Únik údajov	Ak by došlo k úniku, aspoň by nedošlo k ich strate.
Šifrovanie dát nielen pri prenose	Únik údajov	Dôležité je mať zašifrované dáta aj v pokoji, napr. na disku.

Tabuľka 41 Navrhnuté technické opatrenia časť 2

(Zdroj: [vlastný])

Navrhnuté organizačné opatrenie	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Zavedenie anonymných porád alebo konzultácií s odborníkmi	Psychická nepohoda, parasociálne vzťahy s influencerami, sociálne porovnávanie a psychická nepohoda, závislosť používateľov od siete	Ako existujú bezplatné kontakty, keď ide o duševné zdravie, pomoc v núdzi, tak by fungovali aj takto
Aktívne podieľanie sa škôl na prevencii digitálnej únavy	Závislosť používateľov od siete, dopamínová slučka kompulzívne správanie, FOMO a tlak na neustálu online prítomnosť	Vysvetľovanie deťom a mladých, že tráviť čas scrollovaním, nie je skutočný oddych.

Tabuľka 42 Navrhnuté organizačné opatrenia časť 1

(Zdroj: [vlastný])

Navrhnuté organizačné opatrenie	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Obmedziť prístup zamestnancom podľa potreby	Prienik účtov, slabá autentifikácia, únik údajov	Nie každý zamestnanec potrebuje mať prístup ku všetkým dátam. V prípade napadnutia veľmi užitočné.
Zaviest' plán v prípade úniku údajov	Únik údajov, porušenie GDPR	Nech nejde len o teóriu, ktorá sa nikdy nenaplní, ale skutočne uplatnenie v praxi.
Pravidelné bezpečnostné audity a vyhodnocovanie rizík	Zneužitie zraniteľnosti, prienik účtov, únik údajov	Pravidelné kontroly bezpečia systému a na základe toho súdiť pravdepodobnosť rizík.
Interné smernice o jasnej komunikácii podmienok a súhlasu pri spracúvaní údajov.	Nejasné podmienky predplatného, zdieľanie údajov, porušenie GDPR	Nie množstvo zbytočných info, ale jasne a v krátkosti vysvetliť.
Zavedenie transparentnej politiky refundácie a zrušenia predplatného.	Nejasné podmienky predplatného	Jasne vysvetliť fungovanie každého predplatného v úvode ešte pred pridaním sa.
Revízia prístupových práv v prípade odchodu zamestnanca alebo zmeny pozície.	Slabá autentifikácia, prienik účtov, únik údajov	Nech nie je množstvo neaktívnych účtov v systéme užívateľov firmy.
Zásady digitálnej rovnováhy ako súčasť noriem v spoločnosti	Závislosť používateľov od siete, dopamínová slučka a kompulzívne správanie, FOMO, a tlak na neustálu online prítomnosť sociálne porovnávanie a psychická nepohoda	Tak ako v spoločnosti vládne istý druh etiky, dalo by sa zaviesť niečo podobné.
Interné školenie a simulované phishingové kampane vo firmách či školách	Phishing, slabá autentifikácia, únik údajov, prienik účtov	Zažiť si útoky v praxi a tým ich skôr rozlíšiť a držať sa v strehu.

Tabuľka 43 Navrhnuté organizačné opatrenia časť 2

(Zdroj: [vlastný])

Navrhnuté psychologicko-edukačné opatrenia	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Podpora zdravého vnímania vlastnej identity v online prostredí	Podpora zdravého vnímania vlastnej identity v online prostredí	Pomocou rôznych projektov, článkov a ukážkou ako skresľujú sociálne siete vnímanie
Edukácia o jednotlivých rizikách a ich následkoch	Všeobecné opatrenia pre všetky riziká	Poučení ľudí sa skôr ochránia.
Edukácia o dôležitosti kritického myslenia, digitálnej hygieny a využívaní jednotlivých opatrení	Dezinformačné a informačné bubliny	Menšia pravdepodobnosť uvereniu nepravdivým informáciám.
Kláť dôraz na opatrnosť pri používaní sociálnych sietí	Všeobecné opatrenia pre všetky riziká	Siete nie sú zóna zaručeného bezpečia.
Zvyšovanie povedomia o podvodoch cez e-maily či SMS	Pharming, phishing	Ľudia zvyknú byť viac obozretní, aj podvedome, keď o niečom častejšie počujú.
Ukazovanie typických znakov podvodných správ	Pharming, phishing	Lepšie užívatelia odhalia podvod.
Workshopy o základných bezpečnostných kontrolách, ktoré vie spraviť aj bežný užívateľ	Pharming	Poučení ľudí sa skôr ochránia.
Edukovať o informácií, že byť online neznamená byť bez rizika	Všeobecné opatrenia pre všetky riziká	Forma je voľná.
Online kurzy a interaktívne návody zamerané na rozpoznanie dezinformácií.	Dezinformačné a informačné bubliny	Nepotrebuje komentár.
Zrozumiteľné vysvetlenie, že neprečítané zmluvné podmienky môžu skryť háčik.	Nejasné podmienky predplatného	Neklikat' OK ak to nie je prečítané všetko.
Vysvetľovanie fungovania algoritmov a toho, ako vplývajú na rozhodnutia používateľa.	Všeobecné opatrenie pre všetky riziká spracovávané metódou KARS	Nepotrebuje komentár.
Edukácia o tom, čo sú parasociálne vzťahy a ako ovplyvňujú sebavnímanie.	Parasociálne vzťahy s influencerami	Môže to pomôcť užívateľom sa z tejto formy závislosti aj vyslobodiť.

Tabuľka 44 Navrhnuté psychologicko-edukačné opatrenia časť 1

(Zdroj: [vlastný])

Navrhnuté psychologicko-edukačné opatrenia	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Vzdelávať ľudí, ale bez pocitu viny	Dopamínová slučka a kompulzívne správanie	Slušne, vecne bez ponížovania neinformovaných
Otvorene hovoriť o prípadoch únikov údajov	Všeobecné opatrenie pre všetky riziká spracovávané metódami CARVER a FMEA/PNH	Ak sa budú utajovať, ľudia budú podceňovať vážnosť.
Učiť správne reagovať pri podozrení	Všeobecné opatrenia pre všetky riziká	Ako si svoje podozrenie potvrdiť, či ako následne postupovať.

Tabuľka 45 Navrhnuté psychologicko-edukačné opatrenia časť 2

(Zdroj: [vlastný])

Navrhnuté právne a regulačné odporúčania	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Povinnosť označovania reklamného obsahu influencerov	Parasociálne vzťahy s influencermi, sociálne porovnávanie a psychická nepohoda, nejasné podmienky v predplatnom	Užívateľ skôr rozlíši či ide o manipuláciu alebo má influencer skutočne pozitívne skúsenosti s danými produktami.
Zákonné právo na digitálny oddych	Závislosť používateľov od siete, dopamínová slučka a kompulzívne správanie, FOMO a tlak na neustálu online prítomnosť, sociálne porovnávanie a psychická nepohoda	Nenútiť svojich zamestnancov či študentov, aby museli pre svoju prácu využívať sieť 24/7.
Podpora legislatívnych nástrojov na zodpovednosť prevádzkovateľov	Únik údajov, zneužitie zraniteľnosti, prienik účtov, slabá autentifikácia, phishing	Nepotrebuje komentár.
Rešpektovanie zásad GDPR pri zbere, uchovávaní a zdieľaní dát	Porušenie GDPR, nesprávne zdieľanie údajov, únik údajov, prienik účtov	Dodržiavať, čo je nariadené, nesnažiť sa to obísť.
Pravidlá, ktoré zaviazajú platformy k vyššej transparentnosti pri odporúčanom obsahu (napr. zobrazovanie dôvodu odporúčania).	Dezinformačné a informačné bubliny, parasociálne vzťahy s influencermi, sociálne porovnávanie a psychická nepohoda	Aby sa algoritmy tak neprispôbovali užívateľovi a tým nevznikala závislosť.

Tabuľka 46 Navrhnuté právne a regulačné odporúčania

(Zdroj: [vlastný])

Navrhnuté právne a regulačné odporúčania	Riziká voči, ktorým pôsobí	Stručné vysvetlenie opatrenia
Zákonná povinnosť prevádzkovateľov platformy nahlasovať vážne úniky dát.	Únik údajov, porušenie GDPR	Nezatajovať pred klientami úniky
Povinné štandardy pre ochranu údajov v aplikáciách už pri návrhu	Phishing, pharming, únik údajov, zneužitie zraniteľnosti, slabá autentifikácia	Nepotrebuje komentár.
Zmluvná ochrana dát pri spolupráci s tretími stranami	Únik údajov, porušenie GDPR, nesprávne zdieľanie údajov	Aby nedošlo k úniku alebo zneužitiu citlivých informácií.

Tabuľka 47 Navrhnuté právne a regulačné odporúčania

(Zdroj: [vlastný])

V poslednej kapitole praktickej časti boli navrhnuté bezpečnostné opatrenia a odporúčenia zo 4 kategórií – technické, organizačné, psychologicko-edukačné opatrenia a právne a regulačné odporúčania – aby riešili riziká, ktoré boli v kapitole pred tým analyzované.

Výsledky metód, ktoré spracovali jednotlivé riziká v praktickej časti, môžu pôsobiť pre laikov, akoby neexistovalo riešenie, ktoré by neznamenal úplné odstránenie sociálnych sietí zo svojho života. Keďže jednotlivé riziká boli vo veľkej miere v kritických hodnotách. Avšak, dôkazom pre možnosť užívania sociálnych sietí aj napriek týmto výsledkom boli navrhnuté následne odporúčené bezpečnostné opatrenia a odporúčania pre jednotlivé ich zamerania v druhej časti praktickej časti. Výsledkom však ostáva, že aj napriek nedostatočnému zabezpečeniu sietí, webových stránok, webov a samotných zariadení, tej najzraniteľnejší bod je ľudský faktor.

Pri využívaní daných opatrení riziká automaticky nezmiznú, ale pravdepodobnosť ich vzniku sa môže znížiť z veľkej miery. Je však potrebné klásť veľký dôraz na edukáciu a rozširovanie povedomia o týchto rizikách a bezpečnostných opatrení, ktorými sa ich spôsobeniu dá zabrániť a predchádzať.

ZÁVER

Cieľom tejto bakalárskej práce bolo identifikovať, analyzovať a vyhodnotiť riziká spojené so sociálnymi sieťami z pohľadu bezpečnosti v kyberpriestore a zároveň poukázať na ich psychologické, technické a právne súvislosti. V úvode bola vysvetlená podstata sociálnych sietí a ich miesto v modernej komunikácii s dôrazom na spôsob, akým ovplyvňujú správanie jednotlivých používateľov a menia tým dynamiku spoločenských vzťahov.

Teoretická časť práce poskytla prehľad najčastejších bezpečnostných rizík v kyberpriestore ako sú phishing, pharming, úniky údajov, manipulácia, šírenie dezinformácií, psychická záťaž či závislosť od sociálnych sietí. Dôležitou súčasťou bola aj právna reflexia ochrany osobných údajov a aktuálnych digitálnych regulácií v rámci EÚ. Zároveň bola otvorená diskusia o hraniciach cenzúry a slobody prejavu v digitálnom priestore.

V praktickej časti boli tieto riziká systematicky analyzované za pomoci troch metodík: CARVER (zaoberala sa technickými rizikami), FMEA/PNH (zaoberala sa procesnými a právnymi rizikami) a KARS (zaoberala sa psychologickými a behaviorálnymi rizikami). Výsledky ukázali, že najkritickejšími rizikami nie sú iba technické útoky, ale najmä dlhodobo prehliadané psychologické a spoločenské faktory, ako sú manipulácia pomocou algoritmov, závislosť, dezinformácie a strata súkromia.

Záverom možno konštatovať, že ochrana používateľov sociálnych sietí si vyžaduje komplexný a multidisciplinárny prístup, ktorý zohľadňuje technologické, legislatívne aj psychologické rozmery digitálnej bezpečnosti. Okrem toho práca poukázala na dôležitosť kritického myslenia a zodpovedného správania na internete. Sociálne siete môžu byť cenným nástrojom, ak sú používané s rozvahou a pochopením ich výhod a rizík.

Výsledky práce môžu slúžiť v prvom rade ako podklad pre osvetu, preventívne opatrenia, ale aj ďalší výskum v oblasti zodpovedného digitálneho správania.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] *Sociálne siete*. [online]. [cit. 2025-01-03]. Dostupné z: https://encyklopediapoznania.sk/clanok/2723/socialna-siet?utm_
- [2] *Sociálne siete*. [online]. [cit. 2025-01-03]. Dostupné z: https://visibility.sk/blog/slovník/socialne-siete/?utm_
- [3] *Sociálne siete*. [online]. [cit. 2025-01-03]. Dostupné z: <https://academic.oup.com/jcmc/article/24/3/126/5420730?login=false>.
- [4] *Sociálne siete VS sociálne média* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.sciencedirect.com/science/article/abs/pii/S0007681311000061>
- [5] *Sociálne siete VS sociálne média* [online]. [cit. 2025-05-24]. Dostupné z: <https://academic.oup.com/jcmc/article/13/1/210/4583062?login=false>
- [6] *Sociálne siete VS Sociálne média* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.monaqlensing.sk/socialne-media-vs-socialne-siete/>
- [7] HARARI, Yuval Noah. *Sapiens*. Zuzana JÁNSKA (prekladateľka). Izrael: Aktuell, 2018. ISBN 9788089873067.
- [8] CASTELLS, Manuel. *The Rise of the Network Society*. 2. vydanie. Wiley-Blackwell, 2009. ISBN 9781405196864.
- [9] *Štatistika* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.statista.com/topics/3723/social-media-and-politics-in-the-united-states/#topicOverview>
- [10] *Rýchlosť a okamžitosť komunikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://sk.rekursosdeautoayuda.com/%C4%8Co-s%C3%BA-soci%C3%A1lne-siete-a-na-%C4%8Do-sl%C3%BA%C5%BEia%3F/?>
- [11] *Rýchlosť a okamžitosť komunikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.zones.sk/studentske-prace/slohove-prace/34863-vyhody-a-nevyhody-socialnych-sieti-uvaha/>
- [12] *Premena medziľudskej komunikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.union.sk/socialne-siete-vplyvajuna-psychicke-zdravie/?>
- [13] *Premena medziľudskej komunikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://glosar.aspekt.sk/default.aspx?smi=1&vid=75&>

- [14] *Vplyv na psychiku a sociálne väzby* [online]. [cit. 2025-01-03]. Dostupné z: <https://vidadu.com/article/sme-naprogramovani-ako-socialne-siete-menia-nasu-komunikaciju-a-identitu-1?>
- [15] *Vplyv na psychiku a sociálne väzby* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.brainmarket.sk/blog/fomo--strach-z-premeskania-v-digitalnom-veku/>
- [16] *Role sociálnych sietí vo verejnom priestore* [online]. [cit. 2025-01-03]. Dostupné z: <https://idea-list.sk/socialne-siete-identita-a-cirkev/>
- [17] *Role sociálnych sietí vo verejnom priestore* [online]. [cit. 2025-01-03]. Dostupné z: <https://slovenskypacient.sk/vplyv-socialnych-medii-na-psychicke-zdravie-co-s-vami-robia-socialne-siete/>
- [18] *Komunikácia vo firemnom prostredí* [online]. [cit. 2025-01-03]. Dostupné z: https://www.prohuman.sk/files/Szanyiova_Bianka-pouzivanie-socialnych-medii-na-osobny-rozvoj_0.pdf?
- [19] *Komunikácia vo firemnom prostredí* [online]. [cit. 2025-01-03]. Dostupné z: <https://medialnavychova.sk/socialne-siete-a-dusevne-zdravie/>
- [20] *Firemné siete* [online]. [cit. 2025-01-03]. Dostupné z: <https://skalindam.sk/socialne-siete-a-ich-moznosti-vyuzitia-z-hladiska-marketingu/>
- [21] *Multimediálne siete* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.monetico.sk/vyvoj-socialnych-sieti-a-ich-vyznam-v-dnesnej-dobe/>
- [22] *Siete pre zdieľanie fotografií a obrázkov* [online]. [cit. 2025-01-03]. Dostupné z: <https://topden.sk/socialne-siete-zoznam-ktore-platformy-dominuju/>
- [23] *Blogovacie siete* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.rozhladna.sk/siete/co-je-mikroblogovanie/>
- [24] *Rýchlosť šírenia falošných správ* [online]. [cit. 2025-05-07]. Dostupné z: <https://strategie.hnonline.sk/news/media/1707982-falosne-spravy-sa-na-twitteri-siria-rychlejsie-nez-pravdive>
- [25] *Chatovacie aplikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.mojandroid.sk/aplikacie-s-end-to-end-sifrovanim/>

- [26] *Chatovacie aplikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://visibility.sk/blog/najlepsie-a-najbezpecnejsie-chatovacie-aplikacie/>
- [27] *Chatovacie aplikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://blog.lebara.co.uk/sk/30-najlepsich-komunikacnych-aplikacii/>
- [28] *Chatovacie aplikácie* [online]. [cit. 2025-01-03]. Dostupné z: <https://blog.lebara.co.uk/sk/30-najlepsich-komunikacnych-aplikacii/>
- [29] *Graf využívania sociálnych sietí na Slovensku* [online]. In: . [cit. 2025-02-26]. Dostupné z: <https://www.go4insight.com/post/ko%C4%Beko-slov%C3%A1kov-je-na-soci%C3%A1lnych-sie%C5%A5ach-v-roku-2024>
- [30] *Platenie streamovacích platforiem* [online]. [cit. 2025-05-24]. Dostupné z: <https://blog.gohighlevel.com/the-subscription-business-model-unlocking-new-recurring-revenue-streams/>
- [31] *Platenie za streamovacie platformy* [online]. [cit. 2025-05-24]. Dostupné z: <https://trustcloud.tech/blog/subscription-abuse-threat-future-streaming-platforms/>
- [32] *Streamovacie platformy VS TV* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.rewind.sk/tv-vs-streamovacie-sluzby-medzi-slovakmi-pozerame-uz-len/>
- [33] *Platenie streamovacích platforiem* [online]. [cit. 2025-05-24]. Dostupné z: <https://hbr.org/2001/07/net-content-from-free-to-fee>
- [34] *Streamovacie platformy VS TV* [online]. [cit. 2025-05-24]. Dostupné z: <https://medialne.trend.sk/televizia/koniec-televiznej-nadvlady-streamovacie-sluzby-prvykrat-investuju-obsahu-viac-ako-televizie>
- [35] *Streamovacie služby* [online]. [cit. 2025-03-15]. Dostupné z: <https://strategie.hnonline.sk/news/marketing/96035718-prieskum-vyuzivanie-streamovacich-sluzieb-na-slovensku-cislom-jeden-je-netflix>
- [36] *TV vs streamovacie platformy z roku 2022* [online]. In: . [cit. 2025-03-15]. Dostupné z: <https://www.mediaklik.sk/televizia/clanok/655948-prieskum-kolko-slovakov-sleduje-netflix-hbo-max-ci-voyo-a-kolko-hodin-tyzdenne/>
- [37] *Ako Instagram zarába peniaze* [online]. [cit. 2025-05-24]. Dostupné z: <https://hbr.org/2001/07/net-content-from-free-to-fee>

- [38] *Ako Instagram zarába peniaze* [online]. [cit. 2025-05-24]. Dostupné z: https://creators.instagram.com/earn-money?locale=en_US
- [39] *Problematika predplatného a zrušenia predplatného* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.ftc.gov/news-events/news/press-releases/2024/10/federal-trade-commission-announces-final-click-cancel-rule-making-it-easier-consumers-end-recurring>
- [40] *Problematika predplatného a zrušenia predplatného* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.theguardian.com/money/2024/mar/08/spending-accidental-subscriptions-doubled-in-year-uk-citizens-advice>
- [41] *Problematika predplatného a zrušenia predplatného* [online]. [cit. 2025-05-24]. Dostupné z: <https://wearecitizensadvice.org.uk/subscription-traps-enough-is-enough-e475bd221c1f>
- [42] *Problematika digitálneho vlastníctva* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.theguardian.com/media/article/2024/may/14/my-whole-library-is-wiped-out-what-it-means-to-own-movies-and-tv-in-the-age-of-streaming-services>
- [43] *Problematika digitálneho vlastníctva* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.vanderbilt.edu/jetlaw/2025/03/10/gone-but-not-forgotten/>
- [44] *Problematika digitálneho vlastníctva* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.mofo.com/resources/insights/250318-a-new-california-digital-content-law-establishes>
- [45] *Nebezpečie platby cez Internet* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.orange.sk/clovek/detail/ochrana-osobnych-udajov-na-internete-naucte-sa-odhalit-phishing>
- [46] *Nebezpečie platby cez Internet* [online]. [cit. 2025-05-24]. Dostupné z: <https://wenetonline.sk/podvodne-praktiky-na-internete-ako-sa-chronit/>
- [47] *Nebezpečie platby cez Internet* [online]. [cit. 2025-05-24]. Dostupné z: <https://zive.aktuality.sk/clanok/qEXREub/slovaci-sa-boja-platieb-cez-internet-proti-kyberzlodejom-ale-existuje-spolahliva-ochrana/>
- [48] Orłowski-Yang, Jeff. *The Social Dilemma* [Dokumentárny dramatický film]. Online stream, Netflix, 9.septembra 2020

- [49] *Problém súkromných a verejných profilov* [online]. [cit. 2025-05-24].
Dostupné z: <https://www.aura.com/learn/social-media-privacy-risks>
- [50] *Problematika legislatívy* [online]. [cit. 2025-05-24]. Dostupné z:
https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF_2019/ZBORNÍK_sekcia_2_Trestne_pravo_FINAL_FINAL.pdf
- [51] *Vykradnutie počas dovolenky* [online]. [cit. 2025-05-24]. Dostupné z:
<https://stg.istream.sk/v-ziline-uradovali-zlodeji-pocas-jednej-noci-vykradli-dve-rodiny/2/>
- [52] *Priemer trávenia na smartfóne* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.startitup.sk/alarmujuce-cisla-prieskum-odhalil-kolko-hodin-travia-mladi-ludia-na-telefone-denne-vysledky-zarazaju/>
- [53] *Práca algoritmu* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.reputationsciences.com/how-does-algorithm-work-on-social-media-platforms/>
- [54] *Dopamín* [online]. [cit. 2025-02-26]. Dostupné z:
<https://www.kompava.sk/ako-sa-tvori-dopamin-aka-je-jeho-funkcia-a-ako-sa-prejavuje-nedostatok#2ks5polmf0vg>
- [55] *Dopamín* [online]. [cit. 2025-02-26]. Dostupné z:
https://rayzzzer.sk/dopamin-a-jeho-vplyv-na-mentalne-zdrav/#Dopamin_a_moderny_zivotny_styl
- [56] *Dopamín* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.neurinu.sk/socialne-siete-zavislost/>
- [57] *Dopamín* [online]. [cit. 2025-05-24]. Dostupné z: <https://emefka.sk/na-14-dni-som-vypla-socialne-siete-a-moj-mozog-sa-mi-podakoval-toto-zazijes-ak-to-skusis-aj-ty/>
- [58] *FOMO* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.union.sk/syndrom-fomo-alebo-strach-z-premeskania/>
- [59] *Preťaženie informáciami* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.preprints.org/manuscript/202503.0641/v1>

- [60] *Preťaženie informáciami* [online]. [cit. 2025-05-24]. Dostupné z: https://www.reddit.com/r/digitalminimalism/comments/1jpni19/how_to_deal_with_social_media_anxiety_and/
- [61] *Algoritmus* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.898marketing.com/2025/04/21/impact-of-social-media-over-time/>
- [62] *Percentá preťaženia* [online]. [cit. 2025-01-03]. Dostupné z: <https://www.mediaklik.sk/media/clanok/661623-z-mnozstva-streamovacich-sluzieb-sme-frustrovani-nieco-zaujima-na-sledovanie-musime-hladat-pridlho/>
- [63] *Chatova aplikácia pre viac aplikácií* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.beeper.com/>
- [64] *Catfishing* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.eset.com/cz/catfishing/>
- [65] *Instagram efekt* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.solangezindzi.com/blog/instagram-isn-t-real-life>
- [66] CAROLL, Henry a Pavel KRISTIÁN (prekladateľ). *Čtěte, pokud chcete dobýt Instagram*. Zoner Press, 2017. ISBN 978-80-7413-368-8.
- [67] BERGEN, Mark. *Like, Comment, Subscribe*. Penguin Books, 2022. ISBN 9780241468302.
- [68] *COVID-19 dezinformácie* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.disinfo.eu/publications/covid-19-vaccine-misinformation-and-facebook%3A-the-challenge-of-moderating-anti-vaxx-and-vaccine-hesitant-stances/>
- [69] *COVID-19 dezinformácie* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.disinfo.eu/publications/covid-19-vaccine-misinformation-and-facebook%3A-the-challenge-of-moderating-anti-vaxx-and-vaccine-hesitant-stances/>
- [70] *Dezinformácie Kapitól p* [online]. [cit. 2025-05-24]. Dostupné z: <https://www.politico.com/news/2022/01/13/jan-6-subpoena-tech-527079>

- [71] *Globálne elity* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.isdglobal.org/wp-content/uploads/2022/09/New-World-Order-ISD-External-August2022-.pdf>
- [72] *Globálne elity* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.bbc.com/news/blogs-trending-57532368>
- [73] *Parasociálne vzťahy* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.sciencedirect.com/science/article/abs/pii/S2352250X22000082>
- [74] *Emma Chamberlain* [online]. [cit. 2025-05-24]. Dostupné z:
<https://medium.com/%40brookelilley3/para-social-relationships-emma-chamberlain-3e05befae4a9>
- [75] *Skracovanie pozornosti užívateľov* [online]. [cit. 2025-05-24]. Dostupné z:
<https://arxiv.org/abs/2302.03714>
- [76] *Skracovanie pozornosti užívateľov* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.bostondigital.com/insights/shrinking-attention-span-what-it-means-marketers>
- [77] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
- [78] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Dávid Krásenský. (prekladateľ)Cisco Systems, 2005. ISBN 8025104176.
- [79] *Manipulácia* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.ipaslovakia.sk/clanok/manipulacia-a-komplex-menejcennosti-alebo-cesta-k-posilnovaniu-sebadovery?>
- [80] *Manipulácia* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.ksebe.sk/ksebe-alphabet/manipulacia?>
- [81] *Manipulácia* [online]. [cit. 2025-01-03]. Dostupné z:
https://sk.wikipedia.org/wiki/Manipul%C3%A1cia_%28psychol%C3%B3gia%29?
- [82] *Manipulácia* [online]. [cit. 2025-01-03]. Dostupné z:
<https://eduworld.sk/cd/jaroslava-konickova/3272/podla-akeho-spravania-spoznate-manipulatora>

- [83] *Umenie manipulácie* [online]. [cit. 2025-01-03]. Dostupné z:
<https://ociso.ucla.edu/cybersecurity/2024-awareness-month/social-engineering>
- [84] *Clickbait* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.ecwid.com/sk/blog/youtube-views-count.html?q=%2Fsk%2Fblog%2Fyoutube-views-count.html>
- [85] *Clickbait* [online]. [cit. 2025-01-03]. Dostupné z:
<https://visibility.sk/blog/slovník/clickbait/>
- [86] *Astroturfing* [online]. [cit. 2025-01-03]. Dostupné z:
<https://visibility.sk/blog/slovník/astroturfing/>
- [87] *Astroturfing* [online]. [cit. 2025-01-03]. Dostupné z:
<https://blog.sme.sk/vladimirbacisin/media/ako-funguje-astroturfing-nastroj-na-generovanie-umelej-podpory-politikov>
- [88] *Astroturfing* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.astroturfing.cz/v-kanade-resi-astroturfing-obdoba-naseho-uradu-pro-hospodarskou-soutez-pokuty-jdou-do-milionu-dolaru/>
- [89] *Influencer* [online]. [cit. 2025-05-24]. Dostupné z:
<https://visibility.sk/blog/slovník/influencer/>
- [90] *Coca cola a Ronaldo* [online]. [cit. 2025-01-03]. Dostupné z:
<https://standard.sk/86348/ronaldo-odložil-coca-colu-a-vyzval-na-pitie-vody-hodnota-spolocnosti-okamžite-klesla-o-tri-miliardy-eur/>
- [91] *Coca cola a Ronaldo* [online]. [cit. 2025-01-03]. Dostupné z:
<https://sita.sk/christiano-ronaldo-dal-prednost-vode-pred-coca-colou-sposobil-im-tym-citелny-prepad-akcii-video/>
- [92] *Bots* [online]. [cit. 2025-05-24]. Dostupné z:
<https://osintteam.blog/detecting-social-media-astroturfing-and-bots-with-osint-techniques-ad69754b5aa4>
- [93] KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

- [94] *Zákon proti nenávisti* [online]. [cit. 2025-05-24]. Dostupné z:
<https://www.minv.sk/?tlacove-spravy-2&sprava=pripravujeme-zakon-proti-sireniu-nenavisti-na-internete-inspirovany-nemeckom-a-rakuskom>
- [95] *Informačné operácie* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.nbu.gov.sk/dezinformacie-a-informacne-operacie/>
- [96] *Dezinformácia* [online]. [cit. 2025-01-03]. Dostupné z:
<https://sk.wikipedia.org/wiki/Dezinform%C3%A1cia?>
- [97] *Dezinformácia VS Hoax* [online]. [cit. 2025-01-03]. Dostupné z:
<https://elv.ai/sk/blog/aky-je-rozdiel-medzi-dezinformaciou-misinformaciou-a-hoaxom/>
- [98] *Konšpiračné teórie* [online]. [cit. 2025-01-03]. Dostupné z:
https://sk.wikipedia.org/wiki/Kon%C5%A1pira%C4%8Dn%C3%A1_te%C3%B3ria?
- [99] *Propaganda* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.ff.umb.sk/mkmet/pseudovedecka-historia-a-konspiracne-teorie-propaganda-a-dejepis.html?>
- [100] *Overovanie informácií* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.eac.sk/ako-rozpoznat-hoaxy-propagandu-a-dezinformacie/>
- [101] *Problematika Telegramu* [online]. [cit. 2025-05-25]. Dostupné z:
<https://arxiv.org/abs/2504.19594>
- [102] *Problematika Telegramu* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.cbsnews.com/news/elon-musk-antisemitism-on-x-twitter-jewish-leaders/>
- [103] *Kybergrooming* [online]. [cit. 2025-04-06]. Dostupné z:
<https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>
- [104] *Vyrovnávacia pamäť* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.techtarget.com/searchstorage/definition/cache>

- [105] *Overovanie informácií* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.techbox.sk/je-vobec-mozne-pohybovat-sa-bezpecne-na-socialnych-sietach?>
- [106] *Neoprávnené zdieľanie dát* [online]. [cit. 2025-01-03]. Dostupné z:
<https://vosveteit.zoznam.sk/tieto-socialne-siete-zdielaju-nase-data-s-tretimi-stranami-najviac-pricom-nie-je-jasne-kam-idu-hovori-studia/>
- [107] *Neoprávnené zdieľanie dát* [online]. [cit. 2025-01-03]. Dostupné z:
<https://vosveteit.zoznam.sk/europsky-sudny-dvor-vysetruje-facebook-nemoze-pouzivat-udaje-o-pouzivateloach-neobmedzene-neuveris-kde-ta-este-sleduje/>
- [108] *Phishing* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.flexi.sk/clanok/co-to-je-phishing>
- [109] *Phishing* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.eset.com/sk/phishing/>
- [110] *Zneužitie osobných údajov* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.securion.sk/zneuzitie-osobnych-udajov/>
- [111] *CA* [online]. [cit. 2025-01-03]. Dostupné z:
<https://ct24.ceskatelevize.cz/clanek/ekonomika/cambridge-analytica-konci-po-skandalu-se-zneuzitim-dat-facebooku-prisla-o-zakazniky-81080>
- [112] *CA* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- [113] *CA* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.novinky.cz/clanek/internet-a-pc-dohra-za-cambridge-analytica-meta-zaplati-725-milionu-dolaru-za-urovnani-soudniho-sporu-40418273>
- [114] *CA* [online]. [cit. 2025-01-03]. Dostupné z:
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- [115] *Sony Pictures* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf>

- [116] *Sony Pictures* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.bbc.com/news/technology-30189029>
- [117] *Sony Pictures útok* [online]. [cit. 2025-05-25]. Dostupné z:
<https://coverlink.com/case-study/sony-pictures-entertainment-hack/>
- [118] *Sony Pictures* [online]. [cit. 2025-05-25]. Dostupné z:
<https://coverlink.com/case-study/sony-pictures-entertainment-hack/>
- [119] *LinkedIn únik* [online]. [cit. 2025-05-25]. Dostupné z:
<https://threatpost.com/data-700m-linkedin-users-cyber-underground/167362/>
- [120] *LinkedIn únik* [online]. [cit. 2025-05-25]. Dostupné z:
<https://doteckomanie.cz/2021/06/linkedin-celi-dalsimu-uniku-dat-az-92-uzivatelskych-uctu-vcetne-jejich-osobnich-dat-bylo-zneuzito/>
- [121] *Podvodné e-maily* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.fio.cz/spolecnost-fio/media/aktuality/166641-upozorneni-na-podvodne-e-maily>
- [122] *Útoky na banky* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.penize.cz/ucty-karty/309925-k-zajisteni-bezpeci-penez-nasazuji-banky-moderni-technologie-finparada-za-to-ocenila-kb>
- [123] Analýza rizík. In: Bezpečnostní politika Univerzity Tomáše Bati ve Zlíně. Zlín: Univerzita Tomáše Bati v Zlíně, c2020 [cit. 2025-04-09].
- [124] *Metóda CARVER* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.growjob.com/clanky-personal/metoda-carver/>
- [125] *Metóda CARVER* [online]. [cit. 2025-05-25]. Dostupné z:
<https://blog.fentress.com/blog/the-importance-of-the-carver-method-in-security-assessments>
- [126] *Metóda CARVER* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.circadianrisk.com/resources/blog/what-is-carver-and-when-should-you-use-it>
- [127] *Metóda CARVER* [online]. [cit. 2025-05-25]. Dostupné z:
<https://www.fda.gov/food/food-defense-initiatives/carver-shock-primer>

- [128] FMEA [online]. [cit. 2025-05-26]. Dostupné z:
<https://relyence.com/2018/08/28/overview-fmea-types/>
- [129] KARS. In:T-SOFT. Praha: T-SOFT, c2006 [cit. 2025-04-09].
- [130] GOLDSMITH, Jack L. a WU, Tim. *Kdo řídí Internet?: iluze o světě bez hranic*. Praha: Dokořán, 2008. ISBN 978-80-257-0044-0.
- [131] Instagram súkromie [online]. [cit. 2025-05-25]. Dostupné z:
<https://privacypcenter.instagram.com/policy>
- [132] KOČÍ, Tadeáš [@Tadeas]. *KDYŽ SE VZTAH SNŮ PROMĚNÍ V NOČNÍ MŮRU.. // Hrozný Příběh Gabby Petito a Brian Laundrie*. Online, video. 3.5.2025
Dostupné z: YouTube, <https://youtu.be/9urs210U3jo?si=JorVDW7ZsmLwXRcx>
[cit. 2025-05-25].
- [133] *Mazanie profilov na sieťach* [online]. [cit. 2025-05-25]. Dostupné z:
<https://apnews.com/article/mexico-abortion-tech-whatsapp-censorship-meta-instagram-ef425bc0e77fcd279be09559c35b1663>
- [134] *Rusko* [online]. [cit. 2025-05-25]. Dostupné z:
<https://vat.pravda.sk/komunikacia/clanok/529557-spehuje-slovensko-svojich-obcanov-v-medzinarodnom-porovnaní-skoncilo-stvrte/>
- [135] *Čína* [online]. [cit. 2025-05-25]. Dostupné z:
<https://hnonline.sk/svet/861434-cina-neschvaluje-hanobenie-vodcov-blokuje-tucka-kima-tretieho>
- [136] *Severná Kórea* [online]. [cit. 2025-05-25]. Dostupné z:
<https://dromedar.zoznam.sk/cl/1000017/2589025/KLDR-oslavuje-75-rokov--Domacich-trapi-hladomor--cenzura-aj-povinna-vojenska-sluzba>

ZOZNAM OBRÁZKOV

Obrázok 1 Štruktúra globálnych investícií do obsahu	23
Obrázok 2 Vzájomný vzťah jednotlivých kybernetických hrozieb podľa Jirovského.....	39
Obrázok 3 Príklad z praktickej časti pre slovný prepis rizika závislosti na sociálnej sieti.	69
Obrázok 4 Príklad grafického prevedenia z praktickej časti práce pre riziko závislosti na sociálnej sieti.....	69
Obrázok 5 Grafická forma pre závislosť používateľov od siete	91
Obrázok 6 Grafická forma FOMO a tlak na neustálu online prítomnosť	95
Obrázok 7 Grafická forma dopamínovej slučky a kompulzívneho správania	97
Obrázok 8 Grafická forma parasociálnych vzťahov s influencerami	99
Obrázok 9 Grafická forma sociálneho porovnávania a psychickej nepohody	102
Obrázok 10 Grafická forma dezinformačnej a informačnej bubliny	104

ZOZNAM TABULIEK

Tabuľka 1 Rozčlenené riziká podľa zvolenej metódy a typu rizika	62
Tabuľka 2 Kategórie metódy CARVER.....	63
Tabuľka 3 Kritéria metódy CARVER	63
Tabuľka 4 Kritérium kritickosti.....	64
Tabuľka 5 Kritérium prístupnosti	64
Tabuľka 6 Kritérium obnoviteľnosti.....	65
Tabuľka 7 Kritérium zraniteľnosti.....	65
Tabuľka 8 Kritérium vplyvu	66
Tabuľka 9 Kritérium rozpoznateľnosti	67
Tabuľka 10 Parametre posúdenia rizík	68
Tabuľka 11 Parametre posúdenia rizík	68
Tabuľka 12 Zhrnutie GDPR, DSA a AI Act.....	74
Tabuľka 13 Spracovanie metódy CARVER pre phishing.....	83
Tabuľka 14 Spracovanie metódy CARVER pre pharming	84
Tabuľka 15 Spracovanie metódy CARVER pre únik údajov.....	85
Tabuľka 16 Spracovanie metódy CARVER pre zneužitie zraniteľnosti	86
Tabuľka 17 Spracovanie metódy CARVER pre prienik účtov	87
Tabuľka 18 Závrer metódy CARVER.....	88
Tabuľka 19 Rozobratie jednotlivých rizík pomocou metódy FMEA/PNH.....	89
Tabuľka 20 Vyhodnotenie rizík metódy FMEA/PNH.....	90
Tabuľka 21 Záver modifikovanej metódy FMEA/PNH	91
Tabuľka 22 Metóda Kars aplikovaná pre riziká závislosti používateľov od siete.....	92
Tabuľka 23 Percentuálne vyhodnotenie rizík závislosti používateľov od siete	92
Tabuľka 24 Vyhodnotenie výsledkov metódy KARS pre závislosť používateľov na sieti	94
Tabuľka 25 Metóda Kars aplikovaná pre riziká FOMO a tlak na neustálu online prítomnosť	95
Tabuľka 26 Percentuálne vyhodnotenie rizík FOMO a tlak na neustálu online prítomnosť	95
Tabuľka 27 Vyhodnotenie výsledkov metódy KARS pre FOMO a tlak na neustálu online prítomnosť	96
Tabuľka 28 Metóda Kars aplikovaná pre riziká dopamínovej slučky a kompulzívneho správania	97
Tabuľka 29 Percentuálne vyhodnotenie rizík dopamínovej slučky a kompulzívneho správania	98

Tabuľka 30 Vyhodnotenie výsledkov metódy KARS pre dopamínovú slučku a kompulzívne správanie	98
Tabuľka 31 Metóda Kars aplikovaná pre riziká parasociálnych vzťahov s influencerami .	100
Tabuľka 32 Percentuálne vyhodnotenie rizík parasociálnych vzťahov s influencerami	100
Tabuľka 33 Vyhodnotenie metódy KARS pre parasociálne vzťahy s influencerami	101
Tabuľka 34 Metóda Kars aplikovaná pre riziká sociálneho porovnávania a psychickej nepohody.....	102
Tabuľka 35 Percentuálne vyhodnotenie rizík sociálneho porovnávania a psychickej nepohody.....	103
Tabuľka 36 Vyhodnotenie výsledkov metódy KARS pre sociálne porovnanie a psychickú nepohodu.....	103
Tabuľka 37 Metóda Kars aplikovaná pre riziká dezinformačnej a informačnej bubliny ..	105
Tabuľka 38 Percentuálne vyhodnotenie rizík dezinformačnej a informačnej bubliny	105
Tabuľka 39 Vyhodnotenie výsledkov metódy KARS pre dezinformačné a informačné bubliny	106
Tabuľka 40 Navrhnuté technické opatrenia časť 1	107
Tabuľka 41 Navrhnuté technické opatrenia časť 2	108
Tabuľka 42 Navrhnuté organizačné opatrenia časť 1	108
Tabuľka 43 Navrhnuté organizačné opatrenia časť 2	109
Tabuľka 44 Navrhnuté psychologicko-edukačné opatrenia časť 1	110
Tabuľka 45 Navrhnuté psychologicko-edukačné opatrenia časť 2.....	111
Tabuľka 46 Navrhnuté právne a regulačné odporúčania	112

ZOZNAM GRAFOV

Graf 1 Využívanie sociálnych sietí na Slovensku	21
Graf 2 Využívanie sociálnych sietí na Slovensku	22
Graf 3 Sledovanie streamovacích platforiem a dopad na sledovanie TV (2022)	24
Graf 4 Súvzt'aznosť koeficientov KARi a PRi pre Ri závislosti používateľov na sieti.....	93
Graf 5 Súvzt'aznosť koeficientov KARi a PRi pre Ri FOMO a tlak na neustálu online prítomnosť	96
Graf 6 Súvzt'aznosť koeficientov KARi a PRi pre Ri dopamínovej slučky a kompulzívneho správania	98
Graf 7 Súvzt'aznosť koeficientov KARi a PRi pre Ri parasociálnych vzťahov s influencerami	101
Graf 8 Súvzt'aznosť koeficientov KARi a PRi pre Ri sociálneho porovnávania a psychickej nepohody.....	103
Graf 9 Súvzt'aznosť koeficientov KARi a PRi pre Ri dezinformačnej a informačnej bubliny	106

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AI	Artificial Intelligence (Umelá inteligencia)
CA	Cambrige Analytica
CARVER	Critically, Accessibility, Recognizability, Vulnerability, Effect, Recognizability (kritickosť, prístupnosť, obnoviteľnosť, zraniteľnosť, vplyv, rozpoznateľnosť)
CD	Kompaktný disk
COVID-19	Choroba spôsobená koronavírusom SARS-CoV-2
DNS	Domain Name System (Systém názvov domén)
DNSSEC	Domain Name System Security Extensions (Bezpečné rozšírenie DNS)
DVD	Digitálny videodisk
EÚ	Európska únia
FMEA	Failure Mode and Effects Analysis (Analýza možných porúch a ich dôsledkov)
FOMO	Fear Of Missing Out (strach z premeškania niečoho dôležitého)
IP	Jedinečné číselné označenie
IT	Information Technology (Informačné technológie)
HTTPS	Hypertext Transfer Protocol Secure (Zabezpečený protokol pre prenos údajov na internete)
K_{Amin}	minimálna hodnota koeficientu aktivity
K_{Amax}	maximálna hodnota koeficientu aktivity
KAR_i	koeficient aktivity
K_{Pmin}	minimálna hodnota koeficientu aktivity
K_{Pmax}	maximálna hodnota koeficientu aktivity
KPR_i	koeficient pasivity
MHD	Mestská hromadná doprava
Napr.	Napríklad

NetzDG	Nemecký zákon o regulácii obsahu na internete (z nemeckého Netzwerkdurchsetzungsgesetz)
O ₁ a O ₂	osi
OK	Okay (súhlasím)
PC	Osobný Počítač
PNH	Pravdepodobnosť, Následok a Odhaliteľnosť rizika
Q&A	Questions&Answers (Otázky a odpovede)
R	miera Rizika
R _i	pravdepodobnosť Rizika i
R _j	pravdepodobnosť Rizika j
SCL	Strategic Communication Laboratories (bývalá britská spoločnosť)
SMS	Short Message Service (Krátka textová správa)
tzv.	takzvané/tazvaný/takzvaná
URL	Uniform Resource Locator (Webová adresa)
ÚOOÚ	Úrad na Ochranu Osobných Údajov
Wifi	Wireless Fidelity (bezdrôtová sieť)
x	celkový súčet uvažovaných rizík
YT	Youtube
2FA	Two-Factor Authentication (Dvojfaktorové overenie)
Σ	Súčet

ZOZNAM PRÍLOH

Príloha P I: Výpočty k praktickej časti práce

PRÍLOHA P I: VÝPOČTY K PRAKTICKEJ ČASTI PRÁCE

Príloha obsahuje výpočty k metódam CARVER, modifikovanej metódy FMEA/PNH a KARS.

Výpočty pre metódu CARVER

- a) Phishing

Výpočet pre zistenie referenčnej hodnoty určujúcej kategóriu aktíva: $5+5+4+5+5+4 = 28$.

- b) Pharming

Výpočet pre zistenie referenčnej hodnoty určujúcej kategóriu aktíva: $5+4+5+4+5+4 = 27$.

- c) Únik údajov

Výpočet pre zistenie referenčnej hodnoty určujúcej kategóriu aktíva: $5+4+5+4+5+4 = 27$.

- d) Zneužitie zraniteľnosti

Výpočet pre zistenie referenčnej hodnoty určujúcej kategóriu aktíva: $5+4+4+5+5+3 = 26$.

- e) Prienik účtov

Výpočet pre zistenie referenčnej hodnoty určujúcej kategóriu aktíva: $5+4+5+4+5+5 = 28$.

Výpočty pre metódu FMEA/PNH

R = N.P.H

- a) Porušenie GDPR

$$R = 5.3.3 = 45$$

- b) Nesprávne zdieľanie údajov

$$R = 4^3 = 64$$

- c) Nejasné podmienky predplatného

$$R = 3^2.4 = 36$$

- d) Pharming (systémová chyba)

$$R = 5.3.4 = 60$$

- e) Slabá autentifikácia

$$R = 5.4^2 = 80$$

Výpočty pre metódu Kars

a) Závislosť používateľov od sociálnej siete

1 Časté návraty na sieť

$$KAR_i = \frac{3}{5-1} \cdot 100 = 75\%$$

$$KPR_i = \frac{4}{5-1} \cdot 100$$

2 Notifikácie a neustály obsah

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{5-1} * 100 = 75\%$$

3 Návykové vzorce správania

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{5-1} * 100 = 100\%$$

4 Závislosť používateľov od sociálnych sietí

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{5-1} * 100 = 100\%$$

5 Neschopnosť regulovať čas

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{5-1} * 100 = 100\%$$

$$K_{Amin} = 75\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-75)}{100} \times 80 = 80 \%$$

$$K_{pmin} = 75\%$$

$$K_{Amax} = 100\%$$

$$O_2 = K_{pmax} - \frac{(K_{pmax} - K_{pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100 - 75)}{100} \times 80 = 80\%$$

b) FOMO a tlak na neustálu online prítomnosť

1 Časté sledovanie upozornení a obsahu

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} = 100\%$$

2 Pocit, že niečo dôležité zmeškáme

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

3 FOMO

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{4-1} * 100 = 100\%$$

4 Úzkosť

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

$$K_{Amin} = 100\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-100)}{100} \times 80 = 100$$

$$K_{Pmin} = 100\%$$

$$K_{Pmax} = 100\%$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100 - 100)}{100} \times 80 = 100$$

c) Dopamínová slučka a kompulzívne správanie

1 Notifikácie a obsah sociálnej siete

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} = 100\%$$

2 Odmena/dopamínová odozva

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

3 Kompulzívne správanie

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{4-1} * 100 = 100\%$$

4 Impulzívne návraty na sieť

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

$$K_{Amin} = 100\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-100)}{100} \times 80 = 100$$

$$K_{Pmin} = 100\%$$

$$K_{Pmax} = 100\%$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100 - 100)}{100} \times 80 = 100$$

d) Parasociálne vzťahy s influencermi

1 Neustále notifikácie

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{1}{5-1} = 25\%$$

2 Nadmerné sledovanie

$$KAR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

3 Jednostranný emocionálny vzťah

$$KAR_i = \frac{3}{5-1} \cdot 100 = 75\%$$

$$KPR_i = \frac{4}{5-1} \cdot 100 = 100\%$$

4 Ovplyvňovanie hodnôt

$$KAR_i = \frac{3}{5-1} \cdot 100 = 75\%$$

$$KPR_i = \frac{4}{5-1} * 100 = 100\%$$

5 Parasociálne vzťahy s influencerami

$$KAR_i = \frac{3}{5-1} \cdot 100 = 75\%$$

$$KPR_i = \frac{3}{5-1} * 100 = 100\%$$

$$K_{Amin} = 75\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-75)}{100} \times 80 = 80$$

$$K_{Pmin} = 25\%$$

$$K_{Pmax} = 100\%$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100 - 25)}{100} \times 80 = 40$$

e) Sociálne porovnávanie a psychická nepohoda

1 Sledovanie ideálov na sociálnej sieti

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} = 100\%$$

2 Nevyhovujúce sebahodnotenie

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

3 Sociálne porovnávanie

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{4-1} * 100 = 100\%$$

4 Psychická nepohoda

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

$$K_{Amin} = 100\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-100)}{100} \times 80 = 100$$

$$K_{Pmin} = 25\%$$

$$K_{Pmax} = 100\%$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100 - 100)}{100} \times 80 = 100$$

f) Dezinformačné a informačné bubliny

1 Skreslený pohľad na svet

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} = 100\%$$

2 Filtrované alebo nepravdivé informácie

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

3 Posilnenie nepresných presvedčení

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{4}{4-1} * 100 = 100\%$$

4 Informačná bublina

$$KAR_i = \frac{3}{4-1} \cdot 100 = 100\%$$

$$KPR_i = \frac{3}{4-1} * 100 = 100\%$$

$$K_{Amin} = 100\%$$

$$K_{Amax} = 100\%$$

$$O_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} \times 80 =$$

$$O_1 = 100 - \frac{(100-100)}{100} \times 80 = 100$$

$$K_{Pmin} = 100\%$$

$$K_{Pmax} = 100\%$$

$$O_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} \times 80 =$$

$$O_2 = 100 - \frac{(100-100)}{100} \times 80 = 100$$

