

КИБЕРПОВЕДЕНИЕ И ДИГИТАЛНИ ЗАПЛАХИ: ПСИХОЛОГИЧЕСКИ И ТЕХНОЛОГИЧНИ АСПЕКТИ НА УЯЗВИМОСТТА В СОЦИАЛНИТЕ МРЕЖИ

Дечо Стоянов

Университет по библиотекознание и информационни технологии

Резюме: Социалните мрежи са неизменна част от съвременния живот и предлагат нови възможности за комуникация и обмен на информация, но също така крият сериозни рискове за потребителите. С развитието на изкуствения интелект заплахите стават по-комплексни – технологии като гласово клониране и фалшиви чатботове повишават уязвимостта и затрудняват киберсигурността. Алгоритмите и психологическите механизми в платформите правят хората по-уязвими за манипулация чрез фишинг, кражба на самоличност и кибертормоз. Прекомерното използване и липсата на дигитална грамотност засилват риска. Новите технологии, като *deepfakes*, затрудняват разграничаването между истина и измама. Препоръчват се образователни програми за повишаване на дигиталната грамотност, развитие на критично мислене и технически решения за разпознаване на фалшиви профили. Изграждането на сигурна и устойчива онлайн среда изисква съвместни действия от държави, технологични компании и потребители, както и прозрачни регулации и инвестиции в сигурността.

Ключови думи: киберпсихология; социални мрежи; изкуствен интелект; дийпфейкове; дигитални заплахи

ВЪВЕДЕНИЕ

Социалните мрежи са неразделна част от ежедневието на около две трети от световното население, създавайки паралелна реалност, която съществува успоредно с физическия свят. Тези дигитални платформи предоставят възможност на потребителите да конструират своя онлайн образ по начин, който често се различава коренно от реалната им идентичност. Чрез внимателно разработени психологически механизми социалните мрежи позволяват на индивидите да влияят на поведението и възприятията на другите, насочвайки вниманието им и дори манипулирайки техните решения. Въпреки безспорните ползи, свързани с глобалната свързаност и обмена на информация, тези платформи създават и сериозни рискове, които застрашават психичното и физическото здраве на потребителите.

През 2023 г. бързото развитие на технологиите, особено в сферата на изкуствения интелект (ИИ), води до появата на нови и по-сложни форми на дигитални заплахи. Сред тях са гласовото клониране и използването на фалшиви чатботове, които превръщат социалните мрежи в още по-опасна среда. Тези инструменти не само надграждат традиционните методи на манипулация, но и ги усилват, като добавят технологичен елемент, способен да имитира човеш-

кото поведение с висока точност. В резултат на това потребителите стават все по-уязвими за измами, дезинформация и психологическо въздействие.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Методологията на изследването се базира на интегриран подход, който съчетава количествени и качествени методи за анализ на съвременните дигитални заплахи и киберповедение. В центъра на вниманието е влиянието на психологически и технологични фактори върху уязвимостта на потребителите в социалните мрежи.

Използвани са и контент-анализи на медийни публикации и политики, а обработката на статистическите данни се извършва със специализиран софтуер. Сред основните акценти е сравнението между традиционните и нововъзникващи рискове, свързани с изкуствения интелект. Междудисциплинарният подход осигурява надеждна основа за изводи и препоръки, от значение както за потребители, така и за специалисти.

РЕЗУЛТАТИ

В съвременния дигитален свят социалните мрежи заемат ключово място в живота на хората и влияят на начина, по който възприемаме себе си, другите и света. Те вече не са просто инструменти за комуникация и обмен на информация, а среда, в която хората изграждат и представят дигитални версии на себе си, които често се разминават с реалната им идентичност. Изграждането на такъв образ в социалните мрежи създава паралелен „виртуален Аз“, често идеализиран, който лесно може да е по-уверен или успешен от реалния човек. Това явление, подкрепено от технологичните механизми на платформите, насърчава създаването на алтернативни дигитални образи, което има последици за личното самовъзприятие и социалното взаимодействие.

Потребителите имат контрол върху това какви части от живота си да споделят, какви филтри да използват и как да комуникират с общността. В резултат се появява изкривена картина на реалността, като дигиталната идентичност често не отразява автентичността на личността. Тази „перфектна версия“ на себе си се поддържа в отговор на социалните очаквания и нуждата от одобрение чрез харесвания и коментари.

Този натиск създава вътрешни конфликти у хората – разминаването между реалния и онлайн образ води до усещане за неавтентичност, съмнение в себе си и емоционално напрежение. Множество изследвания отбелязват връзка между постоянния стремеж за „перфектност“ в социалните мрежи и проблеми със самооценката, тревожност, както и депресивни състояния, особено при младите (Mary Chayko 2017).

Сравнението с другите потребители допълнително изостря проблема – социалните мрежи дават илюзия за достъп до живота на околните, но реално показват само подбрани, най-добри моменти. Това води до нереалистични стандарти за успех, щастие и социален статус. Потребителите се сравняват с

идеализирани образи, изпитват неудовлетвореност и придобиват ниско самочувствие.

Освен върху себеоценката социалните мрежи влияят и върху междуличностните отношения. Макар да улесняват нови контакти и комуникация, те повърхностно заменят дълбоките човешки връзки. Много хора влагат повече усилия в дигиталното си присъствие, отколкото във взаимоотношенията си в реалния живот, което предразполага към социална изолация и усещане за самота.

Комуникацията онлайн е ограничена – липсват невербални сигнали, като интонация, мимика и жестове, което често води до недоразумения и конфликти. Освен това анонимността във виртуалната среда може да доведе до по-агресивно или неетично поведение и намалено усещане за отговорност.

Разминаването между реалната и виртуалната идентичност има и дълбоки психологически последици. От една страна, социалните мрежи позволяват експериментиране с роли и създават възможност за временно „бягство“ от проблеми, но ако дигиталният образ започне да доминира над реалния, има риск от отчуждение от себе си. Самооценката се обвързва с онлайн метрики – последователи, харесвания и коментари, които могат да предизвикат криза на идентичността.

Поддържането на алтернативен дигитален образ отнема време, енергия и създава натиск върху потребителя постоянно да бъде интересен, актуален и харесван. Вместо върху вътрешното си развитие хората често се фокусират върху външни признаци за успех, което може да доведе до зависимост от социалните мрежи.

Психологията изследва тези ефекти, като подчертава как социалното одобрение (харесвания, коментари) активира мозъчни механизми, сходни с пристрастяването. Поведенческата зависимост се засилва чрез механизми за „непрекъсната награда“, моделирани по теорията за оперантното кондициониране на B.F. Skinner. Бързото и редовно получаване на одобрение ангажира вниманието на хората и ги кара да прекарват все повече време онлайн.

Тази зависимост поражда феномен като FOMO (страх от изпускане на нещо важно), особено сред младежите, които ежедневно изграждат все по-голяма част от своята идентичност онлайн. Систематичните изследвания доказват връзка между прекомерното използване на социални мрежи и повишения риск от тревожност, депресия, социална изолация и понижена самооценка. Особено негативен е ефектът от нереалистичните стандарти за красота, успех и щастие, които водят до трайна вътрешна неудовлетвореност.

Социалните мрежи влияят не само на психиката, но и на процесите на вземане на решения и убежденията. Алгоритмите персонализират поднесеното съдържание, създавайки информационни „балони“, в които се показват само съвпадащи с предпочитанията мнения. Това ограничава достъпа до различни гледни точки, задълбочава когнитивните изкривявания и нерядко води до радикализация.

Тези механизми може да бъдат използвани от самите платформи, но и от трети страни – политици, рекламисти, дори чужди правителства, с цел да манипулират мнението и поведението на определени групи. Чрез събиране и анализ на лични данни профилите на хората се използват за насочване на целево съдържание и влияние върху решенията им, често без съзнателното им съгласие (Bada, Nurse 2019).

Последиците от тази цифрова манипулация са изключително сериозни – от разпространение на дезинформация до дестабилизиране на демократични процеси. Социалните мрежи вече не са просто комуникационни канали, а мощен инструмент за психологическо и обществено въздействие.

Друго сериозно предизвикателство са дигиталните злоупотреби – кражба на лични данни чрез фишинг, разпространение на злонамерен софтуер или измамни кампании с „наградни игри“. Catfishing (измами с фалшиви самоличности) също е все по-разпространено явление, носещо сериозни финансови и емоционални щети на жертвите. Фалшиви профили, deepfake видеа и автоматизирани чатботи, създавани с изкуствен интелект, затрудняват разпознаването на автентичността в онлайн средата.

Дигиталните атаки засягат не само отделните потребители, но и институции и бизнеси. Автоматизацията позволява мащабно създаване на фалшиви акаунти, координирани атаки и манипулации по време на политически, здравни или икономически кризи.

Защитата от тези заплахи вече не може да бъде само технологична. Необходимо е интегриран подход, който включва образование за повишаване на дигиталната грамотност, ефективни екипи за модерирание и напреднали системи за разпознаване на фалшиво съдържание. Киберсигурността е от ключово значение за развитието на изкуствения интелект, който улеснява създаването и разпространението на манипулативна информация (Jobin, Ienca, Vayena 2019).

В заключение, научният анализ на поведението в социалните мрежи показва, че те са неразделна част от психосоциалната реалност и че водят до значителни промени в идентичността, емоциите и сигурността на хората. Единственото устойчиво решение е комбинация от психологически, социални и технически мерки, насочени към изграждане на по-здрава, етична и устойчива дигитална среда. Само чрез критична осъзнатост, ефективно законодателно регулиране и образовани граждани може да се ограничат рисковете и негативите на модерното дигитално общуване.

ИЗВОДИ/ДИСКУСИЯ

Изследването разкрива, че уязвимостта на потребителите в социалните мрежи е резултат от сложното взаимодействие между психологически и технологични фактори. Модерните дигитални заплахи вече не се ограничават до класически кибератаки, а включват хибридни методи, които комбинират манипуляционни техники с изкуствен интелект. Едностранните технически решения не са достатъчни – ключова е ролята на образованието и развитието на дигитална

грамотност, включително критично мислене и разпознаване на манипулации.

Социалните платформи и технологичните компании трябва да прилагат прозрачни механизми за мониторинг и да използват ИИ за предотвратяване на измами и дийпфейкове. Съвместната работа между различни сектори е жизненоважна за ограничаване на манипулациите и кражбите на самоличност. Не на последно място, трябва да се отчита и въздействието на дигиталните заплахи върху психичното здраве на потребителите. Ефективната защита изисква интегриран подход, който комбинира технологии, образование и психологическа подкрепа.

ЗАКЛЮЧЕНИЕ

В условията на бърза дигитализация разбирането на рисковете, свързани със социалните мрежи, е от ключово значение. Изследването разкрива как взаимодействието между психологическите особености на потребителите и технологичните инструменти поражда нови уязвимости и заплахи, особено с навлизането на генеративния изкуствен интелект. Поведението онлайн се оформя както от личностови черти, така и от алгоритмите на платформите. Заплахи като гласово клониране и фалшиви чатботове показват слабостта на традиционните защитни механизми и подкопават доверието в дигиталната среда.

Изводите подчертават, че за ефективна защита са необходими не само технологии, но и цялостна стратегия за повишаване на дигиталната грамотност, критично мислене и отговорно онлайн поведение. Сътрудничеството между академичните среди, индустрията и институциите е от ключово значение за разработване на адаптивни, етични решения. Информираността, образованието и прозрачността остават основни фактори за изграждане на сигурна и устойчива дигитална среда за бъдещите поколения.

REFERENCES

- LAKSHMANAN, Ravie, 2025. *Top 5 AI-Powered Social Engineering Attacks*. Available from: <https://thehackernews.com/2025/01/top-5-ai-powered-social-engineering.html>.
- AKHTAR, Mohammad Majid; MASOOD, Rahat; IKRAM, Muhammad; KANHERE, Salil S., 2023. *False Information, Bots and Malicious Campaigns: Demystifying Elements of Social Media Manipulations*. Available from: <https://arxiv.org/abs/2308.12497v1>.
- BADA, Maria; NURSE, Jason R. C., 2019. *The Social and Psychological Impact of Cyber-Attacks*. Available from: <https://arxiv.org/pdf/1909.13256>.
- WANG, Chenyue; KROON, Anne C.; BOERMAN, Sophie C.; MÖLLER, Judith; DE VREESE, Claes H., 2024. *The artificial intelligence divide: Who is the most vulnerable?* Available from: <https://journals.sagepub.com/doi/full/10.1177/14614448241232345>.
- ALBLADI, Samar Muslah; WEIR, George R. S., 2020. *Predicting individuals' vulnerability to social engineering in social networks*. Available from: <https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00047-5>.

SCHMITT, Marc; FLECHAIS, Ivan, 2024. *Digital deception: generative artificial intelligence in social engineering and phishing*. Available from: <https://link.springer.com/article/10.1007/s10462-024-10973-2>.

MARCELLINO, William; BEAUCHAMP-MUSTAFAGA, Nathan; KERRIGAN, Amanda; CHAO, Lev Navarre; SMITH, Jackson, 2023. *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0*. Available from: <https://www.rand.org/pubs/perspectives/PEA2679-1.html>.

CHAYKO, Mary, 2017. *Superconnected: The Internet, Digital Media and Techno-Social Life*. Available from: <https://markdangerchen.net/courses/236/chayko%20superconnected%20ch2and3.pdf>.

WALL, David S., 2007. *Cybercrime: The transformation of crime in the information age*.

IENCA, Marcello, 2023. *On Artificial Intelligence and Manipulation*. Available from: https://link.springer.com/article/10.1007/s11245-023-09940-3?utm_source.

SINGH, Gurwinder; KAUR, Ramanpreet; BHARTI, Khushboo, 2025. *Security Concerns of Generative AI on Social Media*. Available from:

https://www.researchgate.net/publication/388538274_Security_Concerns_of_Generative_AI_on_Social_Media.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy, 2019. *The global landscape of AI ethics guidelines*. Available from:

https://www.researchgate.net/publication/335579286_The_global_landscape_of_AI_ethics_guidelines.

CYBERBEHAVIOR AND DIGITAL THREATS: PSYCHOLOGICAL AND TECHNOLOGICAL ASPECTS OF VULNERABILITY IN SOCIAL NETWORKS

Abstract: *The report demonstrates that social networks are an important part of the lives of 2/3 of the population, but they also pose risks to mental and physical health. In 2023, advancements in artificial intelligence (AI) lead to new digital threats, including manipulations through voice cloning and fake chatbots. The study shows that cyberbehavior is diverse and includes threats such as phishing and identity theft. The report emphasizes the need to educate users to recognize these threats and highlights the importance of collaborative efforts to build a safe online environment.*

Keywords: *cyberpsychology; social networks; artificial intelligence; deepfakes; digital threats*

Master Engineer Decho Stoyanov, PhD Candidate

Scientific Advisor: Assoc. Prof. Nikolay Mitev, PhD
University of Library Studies and Information Technologies
Sofia, Bulgaria

E-mail: 9123492-2@unibit.bg