УДК 004.056

Б. О. Фененко

TIKTOK ЯК ІНФОРМАЦІЙНА НЕБЕЗПЕКА

Вінницький національний технічний університет

Анотація

У роботі досліджено механізми використання платформи TikTok як інструменту гібридної війни проти України. Проаналізовано ризики, пов'язані з юрисдикцією серверів КНР, та специфіку поширення дезінформації через алгоритмічні стрічки. Особливу увагу приділено методам протидії ІПСО та важливості кібергігієни для захисту національного інформаційного простору.

Ключові слова: TikTok, кібербезпека, захист персональних даних, дезінформація, ІПСО, алгоритмічний вплив, кібергігієна, національна безпека.

Abstract

This study examines the mechanisms by which the TikTok platform is used as a tool of hybrid warfare against Ukraine. It analyzes the risks associated with the jurisdiction of servers in the People's Republic of China and the specifics of disinformation dissemination through algorithmic feeds. Particular attention is paid to methods of countering information and psychological operations and the importance of cyber hygiene for protecting the national information space.

Keywords: TikTok, cybersecurity, personal data protection, disinformation, IPSO, algorithmic influence, cyber hygiene, national security.

ВСТУП

У сучасному цифровому світі інформація стала стратегічним активом і водночас інструментом впливу. Соціальні мережі, зокрема TikTok, є потужними каналами для поширення даних, які можуть використовуватися для маніпулювання свідомістю [1]. Це призводить до виникнення інформаційно-психологічних операцій (ІПСО), подібних до тих, що застосовуються в рамках гібридної війни. Актуальність теми зумовлена необхідністю захисту особистої та національної безпеки в умовах глобальних кіберзагроз [2, 3].

ОСНОВНА ЧАСТИНА

З точки зору теоретичних основ кібербезпеки, TikTok демонструє системне ігнорування принципу мінімальних привілеїв. Технічні аудити безпеки застосунку свідчать про збір надлишкового обсягу метаданих, що включають унікальні ідентифікатори пристроїв, точні координати геолокації, історію пошукових запитів та навіть доступ до вмісту буфера обміну пристрою [4]. Такий рівень доступу дозволяє формувати надзвичайно точні цифрові профілі користувачів. Ці масиви Big Data стають ідеальним підґрунтям для проведення атак із використанням методів соціальної інженерії та високотаргетованого фішингу, де зловмисник володіє вичерпною інформацією про звички та вподобання жертви [5]. Впровадження базової кібергігієни, такої як обмеження дозволів застосунку, є лише частковим заходом, оскільки архітектура платформи спочатку орієнтована на максимальне виведення та приховане отримання даних користувачів [6].

Однією з головних загроз є фізичне розташування серверної інфраструктури та юридична підпорядкованість материнської компанії ByteDance законодавству КНР. Відповідно до китайських законів про розвідку, приватні компанії зобов'язані співпрацювати з державними органами, надаючи доступ до будь-яких даних за запитом. Це створює прямий канал для несанкціонованого отримання розвідувальної інформації про громадян інших країн, що стало підґрунтям для ухвалення в США закону «*Protecting Americans from Foreign Adversary Controlled Applications Act*» [7]. Західні ініціативи щодо локалізації даних, зокрема європейський проєкт «Project Clover», мають на меті створення безпечних ізольованих сегментів для даних, проте експерти з кіберполітики зазначають, що логічний

доступ до алгоритмів та бази даних з боку розробників у КНР залишається «сірою зоною», яку неможливо повністю контролювати лише технічними засобами [8, 9]. Додаткові дослідження підтверджують, що навіть за умови фізичного зберігання інформації за межами Китаю, архітектурна залежність застосунку від центральних систем у КНР зберігає ризики несанкціонованого втручання [10, 11].

Найбільш небезпечним проявом діяльності платформи в Україні є її інструменталізація російськими спецслужбами для ведення інформаційно-психологічних операцій. Алгоритмічна стрічка TikTok побудована за принципом максимального утримання уваги, що сприяє швидкому поширенню часто маніпулятивного контенту. Під час повномасштабного вторгнення рф було зафіксовано численні кампанії, спрямовані на дискредитацію військово-політичного керівництва України та поширення панічних настроїв серед цивільного населення [12].

Російські пропагандисти використовують платформу для трансляції коротких, емоційно насичених відео, що підривають довіру до мобілізаційних процесів та західних партнерів України [13]. Особливу небезпеку становлять технології генеративного штучного інтелекту: використання діпфейків, де за допомогою підроблених відео відомі особи «закликають до капітуляції» або «розкривають таємні змови», спрямоване на руйнування когнітивної стійкості суспільства [14]. Такі операції базуються на використанні «інформаційних бульбашок», де користувач отримує лише той контент, що підтверджує його існуючі страхи чи упередження, що робить маніпуляцію максимально ефективною та прихованою [15].

ВИСНОВКИ

TikTok є не просто розважальним сервісом, а складним інструментом впливу, що поєднує в собі ризики технічного шпигунства та засоби масового психологічного маніпулювання. Для України, яка перебуває у стані активної фази гібридної війни, ці загрози мають екзистенційний характер. Забезпечення інформаційної стійкості вимагає комплексного підходу: від законодавчих обмежень на рівні держави до системної просвітницької роботи з населенням. Розвиток критичного мислення та суворе дотримання правил кібергігієни у поєднанні з державним моніторингом цифрових загроз є єдиним шляхом до нейтралізації небезпек, які несе TikTok у сучасному кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Psychological Warfare [Electronic resource] // RAND Corporation. – 2026. – Mode of access: https://www.rand.org/topics/psychological-warfare.html.
2) Protection Against Negative Information-Psychological Influences in Conditions of Hybrid War [Electronic resource] // ResearchGate. – 2025. – Mode of access: https://www.researchgate.net.
3) NATO Strategic Communications Centre of Excellence. TikTok and National Security Challenges [Electronic resource]. – 2024. – Mode of access: https://stratcomcoe.org.
4) SANS Institute. Personal Cyber Hygiene in the Age of Social Media. – 2024. – 45 p.
5) Infosecurity Magazine. TikTok Engaging in Excessive Data Collection [Electronic resource]. – 2025. – Mode of access: https://www.infosecurity-magazine.com.
6) OECD. Digital Security Risk Management for Citizens. – 2023. – 38 p.
7) Lawfare. Lessons Learned From the TikTok Saga [Electronic resource]. – 2025. – Mode of access: https://www.lawfaremedia.org.
8) U.S. Congress. Protecting Americans from Foreign Adversary Controlled Applications Act. – 2024. – 118th Congress.
9) Privacy Laws & Business. TikTok moves to enhance data security: Project Clover. – 2025. – 12 p.
10) European Commission. Cybersecurity and Data Protection Policies [Electronic resource]. – 2024. – Mode of access: https://ec.europa.eu.
11) Brookings Institution. National Security Risks of Social Media Platforms. – 2024. – 24 p.
12) MIT Technology Review. How TikTok's Algorithm Shapes User Behavior [Electronic resource]. – 2023. – Mode of access: https://www.technologyreview.com.
13) Центр протидії дезінформації при РНБО України. Exploiting TikTok for malicious influence on Ukrainian audience [Electronic resource]. – 2024. – Mode of access: https://spravdi.gov.ua.
14) Ніколс Т. Диванні експерти. Як необмежений доступ до інформації робить нас тупішими / Т. Ніколс ; пер. з англ. Є. Кузнєцової. – Київ : Наш Формат, 2019. – 240 с.
15) Мегель А. Ворожі ІПСО. Як визначити та протистояти / А. Мегель, М. Яремчук. – Київ, 2022. – 84 с.

Фененко Богдана Олександрівна – студентка 1БС-24б, кафедри захисту інформації, ФІТКІ, ВНТУ, м. Вінниця, bfenenko1@gmail.com

Науковий керівник: ***Радченко Євгеній Валентинович*** – асистент кафедри захисту інформації, ВНТУ, м. Вінниця, e-mail: eradchenko@vntu.edu.ua

Bogdana O. Fenenko – student of 1BS-24b, Department of Information Security, FITKI, Vinnytsia National Technical University, Vinnytsia, e-mail: bfenenko1@gmail.com.

Supervisor: Yevhenii Radchenko – assistant professor, VNTU, Vinnytsia, e-mail: eradchenko@vntu.edu.ua