

Царьова Ірина Валеріївна
професор кафедри українознавства
та іноземних мов Дніпропетровського
державного університету внутрішніх справ,
доктор філологічних наук, доцент,

ПУБЛІЧНА БЕЗПЕКА В ІНТЕРНЕТІ У ВОЄННИЙ ЧАС

Розвиток світової спільноти наочно демонструє, що нині критично важливим державним ресурсом, який забезпечує національну безпеку країн, стає інформація. При цьому системи, що забезпечують керування інформаційними потоками є невід'ємним компонентом структури управління державою, економікою та обороною.

Повномасштабне вторгнення російської армії в Україну – це світова топтема весни 2022 року. Про це попереджали в грудні 2021 року американські й українські розвідники, провідні світові ЗМІ. Тему війни обговорювали на всіх міжнародних платформах. Вагомого наукового і практичного значення набувають проблеми публічного (громадського) порядку та публічної (громадської) безпеки, їх охорони та забезпечення. У той час, доки на вулицях українських міст, селищ, сіл ведуться бої, війна триває й в інтернеті. Росія атакує Україну по всіх можливих фронтах.

Навіть неусвідомлені дії в інтернеті, наприклад, залишені в соціальних мережах «лайки» дозволяють зібрати про людину достатньо персональної інформації. За словами бізнес-консультанта з безпеки Cisco Systems Олексія Лукацького, при належному аналізі поведінки користувача в соцмережі створюється його психологічний профіль, який використовується для різних завдань – пропозиції йому певного роду реклами, поданні відповідного контенту.

Сформовано безліч простих правил, що вбережуть на фронті кібервійни з окупантом. Наприклад, нікому в жодному разі не надсилати повідомлення, що містять відомості про поточне місцеперебування членів сім'ї. Функцію геолокації взагалі краще відключити на всіх гаджетах. Не варто нікому розповідати про поточну ситуацію в місті. Ця заборона стосується не тільки онлайн-друзів, а й тих, з ким знайомі в реальному житті, тих, кому повністю довіряєте. Облікові записи зламують, повідомлення перехоплюють. Використання особистих даних стає можливим багатоманітним в чому завдяки недосконалості законодавства, у якому залишається широке поле для трактування поняття «персональні дані» [2]. Ми маємо закон про захист персональних даних. Але що є персональними даними?

В Україні після майже двох місяців бойових дій виникає дилема правильного балансу між необхідністю в керуванні країною та інтересами військової цензури, з одного боку, та збереженням демократичних інституцій – з іншого. Війна має стати також приводом для перегляду та трансформації української політики на краще, шансом позбутися занедбаних хвороб – надмірного впливу олігархів, політичної корупції та маніпуляцій за допомогою ЗМІ. Внутрішня політика у воєнний час виявляється в кількох сферах та в кожній може і посилити національні інтереси, і послабити їх.

Військовий інформаційний потенціал є частиною інформаційного потенціалу держави, що забезпечує підвищення якості рівня елементів воєнного потенціалу. Як і в інформаційному потенціалі держави, у військовому інформаційному потенціалі можна виділити три компоненти: інфраструктурний, управлінський та інформаційний. За складом вони загалом повторюють аналогічні компоненти інформаційного потенціалу держави, які, проте, більш спеціалізовані на вирішення завдань забезпечення військових операцій. Військовий інформаційний потенціал є найважливішим об'єктом впливу та захисту інформаційного протистояння, яке проводиться з метою забезпечення завдань, які вирішуються на державному рівні, та для забезпечення операцій Збройних сил України.

ІТ-армія знищує ворога в кіберпросторі, кожен із нас має пам'ятати про власну кібербезпеку: поставити двофакторну аутентифікацію на акаунтах; не відповідати закритим акаунтам в Instagram; заборонити додавати себе в групи в Telegram; не публікувати, де ви перебуваєте (ні країну, ні місто, ні навіть район); жодних нових застосунків на Android (навіть якщо будуть казати, що це зручно та безпечно).

Багато хто думає, що безпека в інтернеті – це ілюзія, і бути захищеним зараз неможливо, адже веб-сайти збирають конфіденційну інформацію так тонко, що ми навіть не знаємо що саме їм відомо. Це, можливо, й так, але ця невпевненість – ще одна причина, щоб зберегти свою приватність та уникнути витоку персональних даних в інтернет [1].

Отже, підвищення обізнаності громадян про умови і правила перебування в соцмережах, небезпеки, що можуть призвести до порушення їхніх прав та свобод, а також про втручання в особисте життя користувачів – необхідний складник свідомого поведіння в соцмережах у період воєнного стану.

1. Безпека в Інтернеті: Що потрібно знати. URL: <https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrбно-znati.html>.

2. Царьова І. В. Сучасний український юридичний текст: лексико-дериваційна структура : монографія. Дніпро : ЛІРА, 2020. 446 с.