***Ващак Владислав Анатолійович,***
*аспірант кафедри цивільного права*
*Національного університету «Одеська юридична академія»*

## ДОКСІНГ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Зберігання конфіденційності є пріоритетним завданням для всіх, хто працює в Інтернеті. Той факт, що будь-яка людина, включаючи злочинців, може знайти приватну інформацію онлайн, є серйозною проблемою. Крім того, щойно такі дані стають цифровими, вони вже потенційно можуть бути скопійовані багатьма користувачами, тому при викраденні конфіденційної інформації запобігти подальшим порушенням приватності буде дуже складно.

Розміщення в Інтернеті особистої інформації з метою переслідування чи погроз іншій людині є явищем доволі поширеним і у більшості випадків суперечить закону, навіть якщо інформація є фактично точною. Часто подібними діями можуть переслідувати і, з першого погляду, добрі цілі, наприклад, пошук злочинця чи заклик до правосуддя, справедливості, але часто це призводить до цькування невинних людей, які стали жертвам фейків. Однак, публікація персональних даних та погрози щодо їх публікації у багатьох випадках вчиняються також із корисливих мотивів.

Такі види порушень конфіденційності мають назву «доксінг» (англ. doxxing), яка походить від хакерського слова «dox», яке позначає документи або іншу приватну інформацію, яка стала доступною громадськості.

Доксінг – це пошук та публікація персональної інформації про фізичну або юридичну особу зі злим умислом [1]. Доксінг став серйозною проблемою в Інтернеті, оскільки зазвичай порушує права фізичних та юридичних осіб на конфіденційність. Це форма невиправданого переслідування в Інтернеті, оскільки зловмисник ділиться особистою інформацією жертви з широким загалом і часто заохочує інших цькувати жертву. Майже кожен може постраждати від доксінгу, зважаючи на величезний набір інструментів пошуку інформації, яка є легко доступною в Інтернеті. Великі бази даних дозволили людям отримувати особисту інформацію, яку було неможливо знайти

в минулому. Зараз сторона доксінгу може відстежувати імена користувачів, виконувати пошук на веб-сайті, доменних імен, займатися фішингом, переглядати профілі соціальних мереж, переглядати записи державних реєстрів, відстежувати адресу Інтернет-протоколу («IP») або номер телефону [2].

Зловмисники використовують різні методи для своєї діяльності. Вони також можуть зламати облікові записи соціальних мереж, електронних пошт, хмарних сховищ або онлайн-банкінгу, займатися соціальним інжинірингом з метою викрадення особистої та конфіденційної інформації [3].

Історія доксингу розпочалася ще до епохи Інтернету. Так, наприкінці 1990-х років організацію Американську коаліцію активістів життя (ACLA) звинуватили у переслідуванні лікарів, які чинять аборти. Прихильники ACLA виходили із плакатами, на яких були фотографії медичних працівників, а в пресі публікували їхні імена, домашні адреси, номери телефонів та іншу особисту інформацію.

Вже в наш час, у розпал пандемії COVID-19, противники вакцинації та жорстких заходів «злили» до мережі тисячі адрес електронної пошти та паролів співробітників Всесвітньої організації охорони здоров'я, лікарень та госпіталів. У відповідь на це губернатор штату Колорадо, США у травні 2021 року ініціював законопроект, який забороняє розміщувати в Інтернеті особисту інформацію про медичних працівників, чиновників та їхні сім'ї, яка загрожує їхній безпеці [4].

Як приклад доксінгу також можна навести діяльність російської організації «Мужское государство». Вони займаються тим, що знаходять жінок, які колись знімались у порнографічних відео, мали стосунки з іноземцями, збирають їхні особисті дані та інформацію про їхнє особисте життя, з метою цькування проти них інших Інтернет-користувачів або шантажу [1].

Можна запропонувати наступне для формування необхідного рівня інформаційної безпеки як «стану захищеності життєво важливих інтересів людини, суспільства і держави, при якому відвертається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [5], для вирішення та запобігання проблеми доксінгу.

Експерти з технологій рекомендують захищати свою приватність різними методами, наприклад, маскуванням особи за допомогою віртуальної приватної мережі. Таким чином, можна приховати свою IP-адресу і не дати зловмисникам знайти ім'я або місцезнаходження. Крім того, можна захистити себе, встановивши надійне програмне забезпечення для виявлення вторгнень у комп'ютерній мережі. Важливо використовувати різні імена користувачів для кожного веб-сайту, блогу чи форуму. Іншими словами, доцільно не використовувати одне й те саме ім'я користувача в Інтернеті, оскільки це дозволить стороні доксування легко зламати облікові записи. Той самий принцип стосується облікових записів електронної пошти. Також рекомендується застосовувати найвищий рівень налаштувань конфіденційності до своїх профілів у соціальних мережах.

Двофакторна аутентифікація є ще однією лінією захисту, коли йдеться про найкращі методи. Це метод, який вимагає, щоб користувач увійшов на веб-сайт, ввівши ім'я користувача та пароль, а потім отримав одноразовий PIN-код на особистий номер телефону. Потім, коли одноразовий PIN-код буде введено на платформі веб-сайту, користувач отримує доступ. Можна також зв'язатися з веб-сайтом або пошуковою системою (наприклад, Google) і попросити їх видалити особисту/приватну інформацію. У більшості випадків це простий процес, який можна виконати на їхніх веб-сайтах [6].

Отже, підсумовуючи написане вище, можна зазначити, що з розвитком Інтернету стало як ніколи легко знайти приватну інформацію про будь-кого. Це стосується як і знаменитостей, так і звичайних людей. Щоб захистити свою конфіденційність, необхідно знати, які інструменти використати для захисту своїх прав. Знання того, де знаходяться особисті дані і хто може отримати до них доступ, має велике значення для збереження конфіденційності.

**Література:**

1. Щотакедоксінгтаяквідньогозахиститися.URL:https://netfreedom.org.ua/article/shcho-take-doksing-ta-yak-vid-nogo-zahistitisya

2. Doxing Rules and Regulations. URL: https://www.internetlawyer-blog.com/doxing-rules-and-regulations/

3. What is Doxing?. URL: https://www.internetlawyer-blog.com/what-is-doxing/

4. Что такое доксинг и как с ним бороться. URL: https://www.rspectr.com/articles/867/chto-takoe-doksing-i-kak-s-nim-borotsya

5. Харитонов Є.О., Харитонова О. І. Проблема асекурації інформаційної безпеки неповнолітніх у ІТ – сфері в контексті немайнових правовідносин батьків та дітей. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/7990/ilovepdf_com-4–6.pdf?sequence=1&isAllowed=y

6. Legal analysis of doxxing. URL: https://blog.ipleaders.in/legal-analysis-doxxing/#What_to_do_if_you_become_a_doxxing_victim