

- вжиття заходів для відновлення безпечного збирання та обробки даних в рамках певного бізнес-процесу.

Отже, використання та розголошення персональних даних без відома суб'єкта в загальному розумінні не є легальним. В даному випадку, вчиняти такі дії мають лише уповноважені на те органи та суб'єкти, і тільки лише за умови повного обґрунтування таких дій.

#### **ЛІТЕРАТУРА:**

1. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.
2. Про захист персональних даних: Закон України. URL: <http://zakon5.rada.gov.ua/laws/show/2297-17>.

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

#### **САМОЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ**

Кількість кібератак на організації та приватних користувачів зростає з кожним роком. Найбільш вразливими галузями є фінансова та телеком-сфера, а також органи державної влади. У зв'язку з цим компанії-надавачі послуг в інтернет-сфері змушені постійно вдосконалювати технології для захисту персональних даних своїх користувачів. Однак, варто зауважити, що відповідальність за збереження даних у цифровому просторі несуть і самі користувачі, які повинні бути більш пильними. Для цього необхідно розвивати цифрову грамотність населення для можливості здійснення користувачами Інтернету самостійного захисту своїх персональних даних від несанкціонованого використання.

Такі вчені як Ч.Н. Азімов, К.Н. Анненков, В.П. Грібанов, І.О. Дзера, О.С. Йоффе, В.Ф. Кириченко, Д.І. Мейєр, Й.О. Покровський, З.В. Ромовська, Г.А. Свердлик, В.І. Синайський, Є.О. Харитонов, В.Л. Яроцький досліджували самозахист у своїх роботах.

Самозахист як поняття вживається в Цивільному кодексі України, де визначається як «застосування особою засобів протидії, які не заборонені законом та не суперечать моральним засадам суспільства» [1], захист особою цивільних прав та інтересів самотужки, своїми власними діями, без звернення до суду або іншого органу, який здійснює захист цивільного права [2].

Не можна не погодитись із О.М. Берназ-Лукавецькою, яка вказує на конституційну природу права на захист персональних даних особи, яке є

похідним від права недопущення втручання в особисте життя та права на заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу [3].

В зарубіжній літературі вживається поняття «Digital self-defense» для позначення самостійного захисту користувачами своїх прав під час використання цифрових технологій, використання стратегій самозахисту користувачами Інтернету для забезпечення цифрової безпеки, захисту конфіденційної особистої електронної інформації. Цифровий самозахист вимагає від користувачів Інтернету активної участі у захисті власної особистої інформації.

Можна виділити чотири основних напрямки самозахисту: *комп'ютерний* (на рівні програмного забезпечення, яке встановлюється на персональні комп'ютери), *облікових записів* (наприклад, використання декількох облікових записів електронної пошти для розділення особистого та ділового використання), *надійності паролів* (є ключовою стратегією захисту особистої інформації, на думку Microsoft, ідеальний пароль повинен складатися щонайменше 14 символів і містити літери, розділові знаки, символи та цифри, де складність додається включенням великих літер) та *керування особистою інформацією за допомогою параметрів конфіденційності* (багато веб-сайтів надають можливість зменшити обсяг використання особистої інформації, за допомогою налаштування параметрів конфіденційності) [4].

Часто навіть безпечні для користувачів цифрові продукти можуть сприяти розповсюдженню персональних даних. Так, популярний месенджер Telegram, який зовні здається безпечною і зашифрованою платформою для обміну повідомленнями, нещодавно піддався звинуваченням через здійснення чисельних правопорушень користувачами. Це було виявлено в ході деяких досліджень, проведених фахівцями кібербезпеки, які розповіли, що Telegram використовується в якості платформи для хакерів і кіберзлочинців, де вони можуть легко обмінюватися даними мільйонів людей в групах і каналах платформи. Крім цього, постачальники послуг VPN, відомі як VPNMentor, додали, що в ході свого дослідження вони також прийшли до висновку, що Telegram діє як безпечний притулок, де хакери можуть легко обмінюватися даними людей і заманювати їх в мережу онлайн-шахрайства і злому. Все це може бути дуже небезпечним, якщо так триватиме і далі [5].

Отже, у підсумку можна зазначити, що самозахист персональних даних в Інтернеті є надзвичайно важливим та необхідним інструментом протидії їх несанкціонованому використанню. Ефективність самозахисту в першу чергу залежить від рівня цифрової та правової грамотності інтернет-користувачів, на

що потрібно звернути увагу органам державної, які реалізують політику у сфері інформаційної безпеки та компаніям, які відповідальні за збереження конфіденційності персональних даних.

#### ЛІТЕРАТУРА:

1. Цивільний Кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#n1145>
2. Харитонов Є.О. Цивільне право. URL: <https://ukrtextbook.com/civilne-pravo-ukra%D1%97ni-xaritonov-ye-o/civilne-pravo-ukra%D1%97ni-xaritonov-ye-o-9-samozaxist-civilnix-prav-ta-interesiv.html>
3. Берназ-Лукавецька О.М. Особливості захисту персональних даних у соціальній мережі. URL: <http://dspace.onua.edu.ua/handle/11300/12441>
4. Digital self-defense. URL: [https://en.wikipedia.org/wiki/Digital\\_self-defense](https://en.wikipedia.org/wiki/Digital_self-defense)
5. Telegram становиться следующим Dark Web из-за активности, которая была обнародована. URL: <https://cpamafia.top/news/telegram-stanovitsya-sleduyushhim-dark-web-iz-za-aktivnosti-kotoraya-byla-obnarodovana/>

**Котенко Олена Миколаївна,**  
*аспірантка кафедри цивільного права*  
*Національного університету «Одеська юридична академія»*

#### ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОСВІТНІЙ ГАЛУЗІ

Коронавірусна інфекція вже здійснила безпрецедентний вплив на різні сфери життєдіяльності людини. В тому числі і на її сучасний технологічний устрій.

Актуальність проблематики інформаційної безпеки в освітній галузі обумовлена, головним чином, карантинними заходами, які починаючи з березня 2020 року періодично встановлюються в Україні.

Постанова Кабінету Міністрів України «Про запобігання поширенню на території України коронавірусу COVID – 19» від 11.03.2020 №211 передбачила заборону відвідування закладів освіти всіма учасниками освітнього процесу. Це призвело до зміни усталених режимів безпечного і стійкого функціонування освітніх закладів різного типу (від позашкільних до вищих) і їх перехід на дистанційну форму навчання з використанням інформаційно-цифрових технологій.

Цифровізація освітнього процесу та робота з технологіями дистанційного навчання тісно пов'язані з безпекою роботи.