

створені особисто користувачем і які не зберігаються в хмарному сховищі, необхідно зберігати на зашифрованому зовнішньому жорсткому диску. Крім того, користувач повинен мати необхідний рівень знань для роботи із програмами шифрування дисків та окремих файлів.

Список використаних джерел:

1. Nearly 26M Amazon, Facebook, Apple, eBay user logins stolen by hackers. URL: <http://surl.li/bzmzi>
2. Устимович Ю. Масштабная утечка данных: хакеры «слили» почти 53 млн записей с персональной информацией украинцев. URL: <https://thepage.ua/news/masshtabnaya-utechka-dannyh-hakery-slili-dannye-ukraincev>
3. Check Point: большинство организаций до сих пор не обеспечили защиту удаленных сотрудников. URL: https://ko.com.ua/check_point_bolshinstvo_organizacij_do_sih_por_ne_obespechili_zashhitu_udalennyh_sotrudnikov_140240
4. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Проект Закону України №7152 від 13.03.2022. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/39215>

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ

Чеснок Б. О.

*студент 1-го курсу факультету міжнародно-правових відносин
Національного університету «Одеська юридична академія»*

Право на захист персональних даних та недоторканність приватного життя є одним із основних прав людини. Зі швидким розвитком цифрових технологій та Інтернету це право було серйозно підірвано.

Час, коли ми живемо, так звана «ера великих даних», характеризується обробкою величезної кількості різноманітних даних. Наша особиста інформація розглядається як «нова нафта». Компанії фактично стягують плату з клієнтів за свої «безкоштовні» послуги, просячи їх залишати все більше особистих даних. Ну, всі ми знаємо стару приказку: «Безкоштовних обідів не буває». Інформація про користувачів, їхню діяльність та поведінку в мережі Інтернет використовується для: аналізу та створення особистих соціально-психологічних профілів; цільове розміщення комерційних продуктів з урахуванням індивідуальних особливостей та потреб користувачів (так званий one-to-one marketing) тощо.

Діти, будучи наймолодшими користувачами Інтернету, опинилися в центрі ринку персональних даних, що постійно зростає. Особи, які не досягли 18 років (діти) відповідно до чинного законодавства також належать до суб'єктів відносин, пов'язаних із персональними даними.

Згідно зі ст. 4 Закону України «Про захист персональних даних» суб'єктами відносин, пов'язаних із персональними даними, є суб'єкт персональних даних;

володілець персональних даних; розпорядник персональних даних; третя особа; Уповноважений Верховної Ради України з прав людини.

Персональними даними є всі дані, що стосуються особи, на підставі яких ця особа може бути ідентифікована (прямо чи опосередковано) і, таким чином, її конфіденційність може бути поставлена під загрозу [1].

До персональних даних належать:

- Ім'я та прізвище.
- Адреса проживання.
- Адреса електронної пошти.
- Світлина.
- ІР – адреса.
- Місцезнаходження людини.
- Інформація, що використовується для аналізу та створення профілів користувачів (робочі здібності, економічний статус, особисті інтереси, поведінка, споживчі звички, мобільність тощо).
- Онлайн-поведінка людини (дані збираються за допомогою файлів cookie).

Європейський загальний регламент захисту даних (GDPR), який набув чинності з 25 травня 2018 року в країнах Європейського Союзу, стосується особистої інформації та є новим стандартом захисту особистих даних та конфіденційності громадян. У цьому Регламенті велика увага приділяється захисту конкретних категорій особистої інформації:

- Расова або етнічна приналежність.
- Релігійна приналежність.
- Членство у профспілках.
- Сексуальна орієнтація.
- Інформація про здоров'я (персональні дані щодо фізичного та психічного здоров'я людини, включаючи надання медичних послуг).
- Біометричні дані.
- Генетичні дані (персональні дані, що стосуються успадкованих або набутих генетичних характеристик людини, що надають унікальну інформацію про фізіологію або здоров'я людини та отримані шляхом аналізу біологічного зразка людини).

Право на недоторканність приватного життя та захист персональних даних є одним із основних прав, передбачених Конвенцією Організації Об'єднаних Націй про права дитини (стаття 16). Це право однаково відноситься і до цифрового середовища.

За словами Хелен Ніссенбаум, професора інформаційних технологій Корнельського університету, недоторканність приватного життя – це не право на секретність чи контроль, а право на належний потік особистої інформації. Що це означає? Це означає, що залежно від ситуації та контексту людина може оцінити та вирішити, чим поділитися з іншими у цифровому середовищі. Іншими

словами, людина має право знати, як і для яких цілей використовуються її дані, хто і як довго їх зберігає, а також, кому доступна така інформація. Особа також може запитати про видалення особистих даних або виправлення невірних [2].

Коли йдеться про дітей, постає питання, чи здатні вони зрозуміти, якою особистою інформацією не слід ділитися з іншими, у яких ситуаціях і чому? Хоча вони дуже стурбовані тим, яка особиста інформація потрапить до рук їхніх батьків або друзів, діти не розуміють, чому великі корпорації (такі як Facebook, Instagram або Snapchat) цікавляться такою інформацією. Згідно з деякими дослідженнями, діти дбають про своє приватне життя у відносинах з оточуючими, але, незважаючи на це, діляться нею публічно; тобто вони не знають про неправомірне використання персональних даних у комерційних цілях та в інституційному контексті (наприклад, у школі, медичному закладі).

У зв'язку з тим, що вони недостатньо обізнані про ризики, наслідки, захист і права, пов'язані з обробкою персональних даних, діти заслуговують на особливий захист конфіденційності в Інтернеті (GDPR).

Персональні дані в Інтернеті можна розділити на три категорії:

1. Активні цифрові сліди – інформація (про себе або інші), яку користувачі залишають при використанні Інтернету, як правило, свідомо, хоча і не обов'язково навмисно (наприклад, при купівлі деяких товарів, завантаженні контенту з Інтернету, завантаженні фотографій, створенні профілів у соціальних мережах).

2. Пасивні цифрові сліди – інформація, яку користувачі залишають в Інтернеті під час його використання, переважно неусвідомлено (наприклад, через файли cookie, відбитки пальців, дані про місцезнаходження, використання розумних речей та розумних іграшок).

3. Інформація, отримана шляхом аналізу перших двох категорій даних з використанням алгоритмів (через процес профілювання), можливо у поєднанні з іншими джерелами даних.

Велика кількість вебсайтів та програм (наприклад, відеоігри, соціальні мережі, сайти знайомств або азартні ігри) вимагають, щоб користувачі вказували свій вік під час створення профілів (реєстрації). Ці послуги мають мінімальний віковий ліміт для їх використання.

Причини, з яких більшість таких сервісів вимагають мінімального вікового обмеження для їх використання, полягають у наступному:

1. Деякі вебсайти та програми за змістом, призначенням або через те, що вони збирають і зберігають дані про користувачів, призначені для дорослих (людей старшого віку), а не для дітей.

2. Відповідно до Закону США про захист конфіденційності дітей в Інтернеті (COPPA) жодна організація або особа, яка користується послугами в Інтернеті (включаючи власників вебсайтів соціальних мереж), не може збирати особисті дані осіб віком до 13 років без дозволу їхніх батьків або опікунів. Більшість постачальників послуг встановили вікове обмеження на використання своїх

послуг, щоб уникнути отримання батьківської згоди для осіб, молодших за встановлений вік. Це обмеження чітко зазначено в Умовах та положеннях, вимагаючи від користувачів дотримання цих умов, перш ніж вони почнуть користуватися послугами. Щоб захистити користувачів, а також самих себе (щоб уникнути порушення закону), вебсайти зобов'язуються видаляти будь-який профіль, створений особою віком до 13 років [3].

В умовах обслуговування популярної соціальної мережі Facebook сказано, що сайт не можуть використовувати особи, які не досягли 13-річного віку (або особи, які не досягли «мінімального віку, встановленого законом у вашій країні для використання наших продуктів»). Хоча більшість соціальних мереж (таких як Facebook, Snapchat, Twitter, Instagram, Skype) вимагають мінімального вікового обмеження в 13 років (є також деякі інтерактивні сервіси, розроблені спеціально для дітей молодшого віку), дослідження показують, що великий відсоток дітей (як у Сербії, так і в інших місцях) починають використовувати ці мережі в більш ранньому віці, ніж запропоновано.

Багато батьків стикаються з проблемою дозволити своїм дітям створити профіль у соціальній мережі у більш ранньому віці, ніж належить. Можливо мати особистий профіль у віці молодше встановленого лише у тому випадку, якщо користувач вводить неправильний вік під час створення профілю.

Для того, щоб захистити свої персональні дані в Інтернеті слід пам'ятати про те, що Інтернет є загальнодоступним простором і дані, розміщені в Інтернеті, доступні для громадськості, пам'ятати про те, що конфіденційність в онлайн-середовищі така ж важлива, як і в реальному світі, про те, що ви залишаєте свої особисті дані на будь-якій вебсторінці, яку ви відвідуєте і тим самим формуєте свою унікальну цифрову особистість - що дозволяє однозначно ідентифікувати вашу особу в мережі.

Список використаних джерел:

1. Про захист персональних даних: Закон України від 01.06.2010 р. №2297-VI *Відомості Верховної Ради України*. 2010. №34, стор. 1188, стаття 481.
2. Dobrinka Kuzmanović, PhD: Personal data protection and privacy on the Internet URL: <https://cutt.ly/zHz6vOQ>.
3. Захист персональних даних. URL: <https://cutt.ly/MHz5ZJw>

Науковий керівник: доцент Чанишев Р. І.