Секция «Компьютерное право и информационная безопасность»

Безопасность личных данных в интернете: что нужно знать каждому пользователю

Научный руководитель – Нургазина Гульмира Есимбаевна

Артикова Алина Каримовна
Студент (бакалавр)
Российская государственная академия интеллектуальной собственности, Москва, Россия
E-mail: artikova_ artik@mail.ru

Фото в интернете на отдыхе, номер телефона – все это является личными данными конкретной личности, а постоянные звонки от «представителей банков» или спам-сообщения – это результат их утечки. За 2023 год Роскомнадзор подтвердил почти 170 утечек личных данных, по итогам которых в сеть попали больше 300 миллионов записей, что превосходит численность населения РФ в 2 раза. Поэтому защита личных данных пользователя остается актуальной проблемой и по сей день.

К персональной информации относятся сведения, которые позволяют прямым или косвенным образом идентифицировать личность. В федеральном законе «О персональных данных» №152 прописаны большинство видов данных: от имени, даты рождения человека до ссылок на его профиль и посещаемых сайтах. Их можно поделить на 4 крупные группы: общие (базовая информация, фамилия, номер абонента, e-mail), специальные (политические убеждения, раса, физическое состояние), биометрические (физиобиологические особенности, сетчатка, голос, почерк, ДНК) и иные (корпоративная информация, как заработная плата работника). Персональные данные можно классифицировать как общедоступные, если пользователь самостоятельно открыл доступ, или обезличенные, хотя по определению подобная информация должна указывать на конкретную личность. По ним нельзя однозначно идентифицировать лицо без дополнительных разъяснений, что позволяет защититься от несанкционированного доступа.

Так, есть информация о некой Екатерине Беловой, которая родилась 03.10.2005 и имеет 1 группу крови с положительным резусом-фактором. Нужно собрать статистические данные о группах крови по г. Москва в 2024 году среди студентов. Без согласия нельзя публиковать биометрические и специальные данные Екатерины, но их можно обезличить, например, по методике идентификаторов. Получается АА99, 1+, 03.10.2005, Москва. Таким образом не ясно, о каком лице идёт речь. Однако существует отдельная таблица со значениями идентификаторов, чтобы можно было установить конкретный субъект, включая личные данные.

К неочевидным примерам персональных данных можно отнести наличие татуировок, историю покупок, поисковых запросов, фотографии и другое. Некоторую информацию люди ошибочно принимают за личные сведения, например, не всякий адрес электронной почты характеризуется такими данными. То есть cutegirl08914@mail.ru не является персональной информацией, а ekaterina03102005belova@mail.ru является, так как в адресе прописаны ФИО и год рождения человека. Иными словами, все перечисленные объекты становятся личными сведениями лишь когда позволяют идентифицировать конкретную личность.

Чтобы знать, как обезопасить свои персональные данные, нужно понимать, как они собираются и обрабатываются сайтом, он же оператор персональной информации. Для этого человек должен сознательно и однозначно дать свое согласие на обработку личных данных. В целях их защиты взаимодействие с персональными материалами без согласия наказуемо и запрещено, если законом не предусмотрено иное. Обычно данные собираются

2 способами: самолично и автоматически. В первом случае пользователь собственноручно вводит данные при регистрации, прохождении опроса, анкеты и прочем. Во втором случае выступают файлы cookie, временные текстовые документы, которые содержат в себе информацию о действиях человека на сайте. Благодаря им интернет-ресурсы сохраняют пароли, товары в корзине, местоположение и так далее. Оператор получает информацию, кто и с какого устройства посетил сайт, запоминает его выбор, что позволяет определить целевую аудиторию и подобрать более таргетированную рекламу для отдельно взятого клиента. Поэтому при посещении сайта часто можно увидеть всплывающее сообщение «пользуясь сайтом, вы соглашаетесь с использованием cookies».

С одной стороны, это облегчает повторный вход на платформы или помогает определить рекомендации. С другой, всегда нужно понимать, что сайт с введенными данными могут взломать, обойдя защиту, украв сведения о человеке, чтобы продать их третьим лицам, снять деньги со счета, шантажировать или проводить мошеннические сделки от имени жертвы.

Недавно преступники научились воровать деньги через трансляцию экрана смартфона, создавая фейковый, но схожий с аккаунтом банка профиль. Они звонят своей жертве и спрашивают, обновляла ли она мобильное приложение, убеждая, что нужно произвести биометрию с помощью демонстрации экрана. Так недоброжелатели получают все нужные им данные как номера карт, коды в СМС и прочее.

Как же обезопасить себя от утечки данных? Нужно понимать, что ни одна из защит не сможет уберечь на 100%. Но чтобы снизить эту вероятность, необходимо:

1) использовать надежные пароли. Они состоят из более 8 разных элементов, которые желательно менять в течение нескольких месяцев и никогда не составлять из личной информации. Можно использовать различные пароли, аккаунты для сайтов, почты для работы и покупок [1, с. 410].

2) использовать многофакторную аутентификации. Это способ проверки клиента по нескольким параметрам, помимо пароля используется биометрия, ответ на секретный вопрос, код на почту и прочее;

3) стараться не заходить на небезопасные сайты. Не переходите по подозрительным и заманчивым ссылкам, посещайте сайты с защищенным соединением и протоколом https, который в отличие от http дополнительно шифрует данные;

4) отслеживать активность аккаунтов и банковских операций. При обнаружении подозрительных входов обратитесь в службу поддержки сервиса;

5) для покупок использовать банковские, виртуальные карты с малым количеством средств, поставив лимит на траты. Если злоумышленники получат доступ к карте, они не смогут списать большую сумму.

6) не выкладывать в сеть фото документов. Даже билет на поезд в Пензу может многое рассказать о своем владельце (время, место, электронный номер).

7) очищать файлы cookie, читать политику конфиденциальности, избегать WI-FI в общественных местах, проверять устройство на вирусы и прочее - существует огромное множество других способов сохранить свою личную информацию.

Чтобы не попасть на уловки мошенников, важно знать, что такое «персональные данные» и как защитить и обезопасить свои личные данные от незаконного и несанкционированного пользования третьими лицами.

Источники и литература

1) Самошкина П.С. Защита прав человека в эпоху глобализации и информационных технологий // Международный научный журнал «Вестник науки» № 1 (70) Том 2. [Электронный ресурс] - 2024 г. - с. 410 - URL: https://cyberleninka.ru/article/n/za

schita-prav-cheloveka-v-epohu-globalizatsii-i-informatsionnyh-tehnologiy (дата обращения: 27.02.2024)