

ПРОБЛЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Литвинова Анастасия Константиновна

студент 1 курса, факультет экономики и финансов

Сибирский институт управления – филиал РАНХиГС, г. Новосибирск

Аннотация. В настоящее время большое количество времени и внимания люди уделяют социальным сетям. В статье рассматривается необходимость защиты персональных данных в социальных сетях. Для них необходима защита от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования. Многие не воспринимают это всерьёз, и потом жалеют об этом. В статье приведены необходимые рекомендации, которые помогут пользователям социальных сетей улучшить защиту персональных данных.

Ключевые слова: персональные данные, социальные сети, защита персональных данных, обезличивание.

В наш век информационных технологий, развивающихся стремительно, информация, и особенно вопросы защиты персональных человека, приобретают особую актуальность и значимость. Государство стремится защитить информационные потоки путем правового регулирования, то есть издания различных нормативных актов.

Проводя такое огромное количество времени в социальных сетях, невозможно не оставить о себе хоть какую-то личную информацию. Выкладывая различные фотографии, оставляя различные публикации на своих страницах, ведя переписку, мы автоматически оставляем о себе информацию, которая может быть использована против нас. [5] В данном случае эта информация, согласно Федеральному закону «О персональных данных», является персональными данными, для которых необходима защита.[1]

Деятельность по обработке персональных данных регулирует Федеральный закон «О персональных данных» . Под обработкой персональных данных понимают любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), обезличивание, блокирование, удаление, уничтожение персональных данных. [1]

Будь то государственный или муниципальный орган, юридическое или физическое лицо и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных. [3]

Назовем часто встречающиеся утечки персональных данных (по версии

аналитического центра Perimetrix):

- кража или потеря носителей с персональными данными;
- Web-утечка – случайная публикация персональных данных в общедоступных местах;
- спланированный инсайд – умышленная кража информации сотрудником, имеющим легальный доступ к ней;
- бумажная утечка – печать и распространение персональных данных на бумажных носителях
- внешний взлом корпоративной сети. [5]

Таким образом, если информация личного характера окажется в руках злоумышленников, то это может привести к печальным последствиям. Например, самое распространённое - это шантаж. Получив конфиденциальную информацию о вас, злоумышленники тут же пытаются извлечь из этого выгоду (деньги, различные ценности и т.д.). Конечно же, лучше этого не допускать, предварительно позаботившись о защите персональных данных.

Изучив эту проблему, я попыталась вывести 5 основных рекомендаций по защите персональных данных в социальных сетях:

1. Не следует запускать сомнительные программы, присланные от незнакомого человека, или даже от знакомого (т.к. его страница может быть взломана и находиться в руках злоумышленников).
2. Старайтесь не открывать сомнительные письма от любых адресатов людей, а уж тем более не переходите по ссылкам, которые могут содержаться в этих письмах, так как это могут быть вредоносные ссылки. Например, вы переходите по ссылке, и ваш компьютер автоматически скачивает программу, которая закреплена там злоумышленниками.
3. Проверяйте все скачанные файлы антивирусом, так как в них могут быть помещены специальные вредоносные программы. Например, программа, которая отправляет информацию с вашего компьютера на абсолютно любой другой, в основном на компьютер злоумышленника.
4. При вводе пароля внимательно проверяйте точно ли это настоящая главная страница социальной сети (существуют сайты, которые созданы для того чтобы получать информацию, вводимую пользователем в строки «пароль» и «логин»), например, главная страница «Вконтакте» - <https://vk.com>. Если, выделяя ссылку, мы увидим лишнюю букву, или хоть какие-то изменения, такие как - <https://vkontakte.com>, то будьте уверены – этот сайт создан злоумышленниками.
5. При пользовании чужим компьютером следуют помнить, что вся введённая вами

информация (пароли, переписки и т.д.) может дублироваться в специальных текстовых документах, не говоря уже о том, что не нужно ставить галочку запомнить пароли, а тем более не нужно забывать выходить с социальных сетей, в которых вы авторизовались. [2]

Разобравшись в этой проблеме, я смогла найти решение, которое, по моему мнению, сможет усилить защиту персональных данных в социальных сетях. Мое решение – это защита персональных данных с помощью обезличивания. [4] Согласно статье 3 пункту 8 Федерального закона «О персональных данных», обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных. [1]

Так как же обезличить персональные данные? Основные методы обезличивания информации утверждены в Приказе Роскомнадзора, органа осуществляющего надзор за реализацией государственной политики в сфере массовой коммуникации. В наши дни используются четыре основных метода обезличивания.

- 1) Введение идентификаторов (часть информации заменяется соответствующими идентификаторами. Для реализации метода создается таблица или справочник, только через таблицу/справочник информацию можно расшифровать).
- 2) Замена состава или семантики информации (оператор удаляет часть сведений, обобщает их, например, вместо конкретных адресов вписывает только города. Кроме этого, разновидностью метода назовем замену ПД статистической информацией – вместо ФИО каждого гражданина, оператор оставляет необходимую ему возрастную/гендерную статистику или другие ведомости.
- 3) Декомпозиция (разбиение одного массива информации на меньшие блоки, которые сами по себе не дают возможности идентифицировать человека).
- 4) Метод перемешивания (группы сведений в одном документе перемешиваются таким образом, что установить принадлежность лицу не представляется возможным). [6]

Применение и использование приведенных выше мер защиты минимизирует угрозы, которые связаны с несанкционированной кражей личных данных.

В заключение хочется сказать, что всегда следует помнить, что при желании можно взломать почти любую страницу в любой социальной сети и все эти данные легко окажутся в руках кибер преступников, а что будет дальше, уже описывалось выше. Поэтому следует серьёзно относиться ко всем действиям в Интернете, ведь каждое выполненное вами действие в мировой паутине может быть использовано против вас.

Список литературы:

1. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
2. <https://elibrary.ru/item.asp?id=27290925>
3. <https://elibrary.ru/item.asp?id=29318228>
4. <https://elibrary.ru/item.asp?id=15214886>
5. <https://elibrary.ru/item.asp?id=27316460>
6. Что такое обезличивание персональных данных, для чего нужно, каковы правила работы с ними? [Электронный ресурс] URL: https://101million.com/personal/priem-na-rabotu/konfidentsialnaya-informatsiya/personalnye-dannye/obezlichivanie.html#dlya-chego-neobhodimo-?utm_source=table_of_content