УДК 34

К ВОПРОСУ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ «ИНТЕРНЕТ»

Бабанов Е. О., Лебедев Д. А., Шиханова Е. Г.

Самарский национальный исследовательский университет
имени академика С. П. Королёва, Самара

Необходимость защиты персональных данных сложно недооценить. Каждый из нас вводил какие-то данные о себе в сети Интернет: Фейсбуке, Вконтакте, Твиттере, Инстаграме, Тамблере, сайтах интернет-магазинов и прочее. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар.

Возросшие технические возможности по копированию и распространению информации вынуждают нас бережнее относиться к персональным данным и стремиться защитить их, потому что уровень информационных технологий достиг той реперной точки, когда банальный антивирус или стандартные системы интернет сервисов не способны надежно скрыть вашу деятельность в мировой сети.

Положения Конституции Российской Федерации говорят о стремительном переходе государства на дорогу создания демократического общества, где главной ценностью является человек и его права. Россия на этом пути столкнулась с рядом требующих решения проблем, среди которых можно выделить обеспечение защиты сферы частной жизни гражданина в сети «Интернет».

Современное законодательство в области компьютерных и информационных технологий не предполагает абсолютную защиту конфиденциальных данных физических лиц от несанкционированного доступа к ним и последующего использования.

Для начала необходимо определить, что мы понимаем под «персональными данными» и «конфиденциальностью». Персональные данные — «любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)» [1]. «Размещение на страницах сайтов в сети «Интернет» фамилии, имени и отчества (равно, как и другие данные) без дополнительной информации, позволяющей идентифицировать физическое лицо как субъекта персональных данных, не может свидетельствовать об обработке персональных данных конкретного физического лица» [2]. Камнем преткновения является вопрос, считать ли всю информацию об определенном или поддающемся определению физическом лице персональными данными или только в том случае, когда можно безошибочно идентифицировать личность, а отдельно взятые данные персональными не являются. А.М. Лушников считает, что «персональные данные», как более узкое понятие входит в состав понятия «частная жизнь», однако вместе с тем полагает, что персональные данные можно разместить в общедоступных справочниках (это предусмотрено действующим законодательством), тогда как сведения о частной жизни, будучи общедоступными, теряют свойства неприкосновенности» [3].

Конфиденциальность — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя. Согласно этому же закону «информация — сведения (сообщения, данные) независимо от формы их представления» [4]. Таким образом, в Российской Федерации конфиденциальность определяется как обязательное для выполнения лицом, получившим доступ к определенным сведениям (сообщениям, данным) независимо от формы их представления, требование не передавать их третьим лицам, без согласия лица, самостоятельно создавшего информацию, либо получившего на основании закона или договора право разрешать или ограничивать доступ

к информации, определяемой по каким-либо признакам. Таким образом, по нашему мнению, конфиденциальность персональных данных — это неразглашение персональных данных третьим лицам, кроме случаев, определённых законом.

Не всегда нарушения возникают со стороны ответственных за хранение наших данных, порой мы сами можем быть более внимательными в использовании интернет-ресурсов, используя протокол «https». Https - это протокол, который гарантирует, что данные, которыми вы обмениваетесь с серверами, хранятся у провайдера в зашифрованном виде. Например, если в адресной строке вашего браузера сейчас https, это значит, что власти или злоумышленники могут видеть, сколько вы сидели на сайте и когда, но, что именно делали, не знают. Если в адресной строке http, это значит, что трафик не шифруется, и можно узнать больше информации. Такие технологические решения позволяют шифровать данные таким образом, что третьим лицам тяжелее получить доступ к информации, так как она хранится в зашифрованном виде.

Также для защиты информации в сети Интернет пользователь может использовать свободное программное обеспечение для реализации второго поколения так называемой «луковой маршрутизации». Это система, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Для людей слабо осведомленных в области права в интернете можно привести пример, связанный с культурным достоянием России – матрешкой. Данные находятся внутри самой маленькой из трех, при этом все матрешки зашифрованы. Вы передаёте матрешку случайному человеку из сообщества Tor, который открывает первую матрешку, и передает любому другому случайному члену сообщества. Третий – передает тому, кому вы изначально хотели передать свои данные. Тогда ответ обратно посылается вам, в этих же матрешках, после чего люди в цепочке не меняют соседей по передаче данных именно с такими параметрами. Теперь данные, отправленные для соответствующего сервера будут запрашиваться из сети Tor в обычный Интернет с IP-адресом третьего (последнего из трех случайных пользователей) шлюза в сети, который не только не знает адрес отправителя, но так же не знает через кого изначально была передана первая матрешка.

С помощью Tor пользователи могут сохранять анонимность при посещении веб-сайтов, публикации материалов, отправке сообщений и при работе с другими приложениями, использующими протокол TCP. Технология Tor обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только анонимность пользователя, но также конфиденциальность бизнес-данных, деловых контактов и др.[5]

Защита персональных данных должна быть трехсторонней: со стороны государства, со стороны бизнеса (юридические лица, которые совершают обработку данных) и со стороны гражданина. Защита персональных данных - личная ответственность каждого.

Государство может путем внесения соответствующих изменений в законодательные акты составить актуальный перечень персональных данных, которым можно было бы руководствоваться для выявления нарушений в данной сфере. Основная доля ответственности ложится на плечи самого гражданина. Именно от него зависит безопасность размещаемых им данных. В качестве рекомендации хотелось бы посоветовать гражданам самостоятельно определять перечень информации, которая может быть доступна публично, далее строго придерживаться данного перечня.

На основе вышесказанного можно сделать вывод, что защита персональных данных несовершенна, но каждый человек имеет полное право и возможность

самостоятельно обеспечить безопасность своих конфиденциальных данных пока законодатель не способен сделать это для своих граждан.

Библиографический список

1. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"// https://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/.
2. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] // https://77.rkn.gov.ru/p3852/p13239/.
3. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. 2009. № 9. С. 93-101.
4. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // https://www.consultant.ru/document/cons_doc_LAW_61798/c505178223 3acca771e9adb35b47d3fb82c9ff1c/.
5. Овамад Кумарди статья "Анонимизация в Интернет с помощью браузера TOR" [Электронный ресурс]: Русскоязычный информационный сайт bits.media, 2012. // https://forum.bits.media/index.php?/topic/578-anonimizatciia-v-internet-s-pomoschiu-brauzera-tor-po/.