РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему Защита персональных данных в социальных сетях

Дисциплина: Информационная безопасность

Студент: Шутенко Виктория Михайловна

Группа: НФИбд-02-19

МОСКВА
2022 г.

Защита персональных данных в социальных сетях

В нашем мире уже невозможно обойтись без социальных сетей. Каждый человек, независимо от пола и возраста, зарегистрирован хотя бы в одной. Соцсети стали тем миром, который способен, хоть и условно, заменить собой реальный, давая человеку возможность получить желаемое здесь и сейчас.

Вовлекаясь в этот увлекательный процесс, каждый человек раскрывает для неограниченного круга лиц персональную информацию о себе. Многие могут не согласиться, сказав, что соцсети дают возможность ограничений, оставляя доступ только для выбранной категории пользователей. Это, безусловно, так, но любой без исключения сайт требует от нас ввода личной информации, от простейшей – в виде имени, номера телефона или почты – до подробной, включая ФИО, дату рождения и т.д. Мы подчас не задумываемся о том, что происходит с нашими данными потом. Должны ли мы заботиться об этом? Безопасность персональных данных пользователей должна обеспечиваться оператором, который осуществляет их обработку, независимо от того, знают ли пользователи или субъекты персональных данных о последствиях уязвимости. На первый план выходят требования Федерального закона "О персональных данных".

Так, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" устанавливает, что обработка допускается только с согласия субъекта персональных данных на обработку его персональных данных (ст. 6). Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (ст. 7). При этом согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме (ст. 9). Получается, что если пользователь дает согласие использовать его данные в одном ресурсе, это не значит, что их можно использовать для сопряженной социальной сети, что является проблемой для связанных между собой сервисов.

Защита персональных данных в социальных сетях подразумевает в том числе, что личные данные пользователя удаляются с серверов ресурса, если пользователь удалил свой аккаунт. Это одно из основных положений политики конфиденциальности многих социальных сетей. Но нужно помнить, что в целях обеспечения пользователю возможности восстановить свой аккаунт в течение некоторого времени после его удаления, соцсети хранят всю информацию на протяжении определенного срока. Кроме того, ваши данные могут остаться в кэше поисковых систем и других электронных ресурсов.

Социальные сети не предоставляют личные данные своих пользователей третьим лицам. Рекламодатели могут использовать собственные рекламные сервисы социальных сетей и адресовать рекламу конкретным группам пользователей по их интересам, профессии, семейному положению и т.п., но ни Facebook, ни ВКонтакте, ни Instagram никогда не передадут огромные массивы пользовательских данных какой-то другой компании непосредственно. Защита личной информации в социальных сетях обеспечивается с помощью:

- предотвращения несанкционированного доступа к информации;
- выявления случаев несанкционированного доступа, определения причин произошедшей утечки данных и их устранения;

- предоставления владельцам аккаунтов возможности восстановить информацию, уничтоженную или измененную вследствие несанкционированного к ней доступа.

Для обеспечения защиты личных данных используются программные и криптографические средства. Программные средства:

- DLP-системы - комплексные системы, предотвращающие утечку данных;
- SIEM-системы - комплексные системы управления событиями и информационной безопасностью, отслеживающие в режиме реального времени событий безопасности (тревог).
- Криптографические средства - это шифрование информации, удостоверение входа и действий на сайте и некоторые другие инструменты.

Меры, принимаемые социальными сетями для защиты данных своих пользователей, внушают уважение. К сожалению, у мошенников тоже есть ресурсы, чтобы создавать свои программные продукты, которые в состоянии пробить брешь в защитных системах. Базы пользовательских данных - невероятно дорогой продукт. С практически повсеместной цифровизацией общества они стали главным активом любой компании, занимающейся коммерческой деятельностью.

Поэтому принимайте дополнительные меры, чтобы обезопасить себя:

- не используйте для регистрации на общедоступных ресурсах почту, которая связана с важными процессами (например, рабочими и финансовыми сервисами);
- устанавливайте свой пароль для каждого ресурса, избегайте классических комбинаций типа «12345»;
- для восстановления или подтверждения пароля используйте мобильный телефон, а не электронную почту;
- делитесь личной информацией в соцсетях осторожно - продумывайте, какие последствия может повлечь за собой размещение тех или иных сведений в общем доступе;
- не добавляйте в друзья незнакомых людей и не переходите по всем ссылкам подряд;
- не публикуйте в соцсетях фотографии важных документов, не пересылайте такие документы через личные сообщения;
- не скачивайте предлагаемые вам через соцсети приложения, если не уверены в том, что это официальный продукт известной вам компании.
И обязательно подключайте двухфакторную аутентификацию там, где она реализована.

Выводы:

- социальные сети - не общедоступные источники персональных данных;
- для того, чтобы обрабатывать наши ПД из социальных сетей, в том числе использовать для пополнения готовых баз данных, необходимо получать прямое согласие на такую обработку;
- для обеспечения защиты личных данных используются программные и криптографические средства
- нужно соблюдать дополнительные меры безопасности в соцсетях.