**УДК 004.056**

**Сухова Алина Рашитовна, Гатиятуллин Тимур Радикович**
студенты 4 курса
Института управления и безопасности предпринимательства
ФГБОУ ВПО Башкирский государственный университет
г. Уфа, Российская Федерация
E-mail: lynn.malino@gmail.com

# К ВОПРОСУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

**Аннотация**

В статье рассмотрены проблемы безопасности персональных данных участников социальных сетей и предложены меры по защите.

**Ключевые слова**

Персональные данные, безопасность, социальные сети, защита данных.

На сегодняшний день социальные сети являются мощнейшим инструментом для различных коммуникаций, продвижения товаров и услуг. Участники соцсетей ежедневно, помимо сообщений, обмениваются аудио-, видео- и фотоматериалами. Однако любой подобный онлайн-сервис предполагает, что пользователь, получивший аккаунт или личную страницу, предоставляет некоторую информацию о себе, которая может относиться к персональным данным (ПДн). Спектр такой информации весьма широк: от фамилии, имени, отчества до религиозных и политических убеждений. Помимо этого беспечные молодые люди в последнее время часто выкладывают в сеть фотографии с правами, паспортами, электронными билетами, чеками. Известен случай, когда девушка потеряла выигрыш, выложив селфи, где был запечатлен чек со штрих-кодом, позволяющим получить деньги. Один из подписчиков воспользовался ее невнимательностью и забрал деньги, поднеся штрих-код к автомату, который выдает выигрыши [2]. В связи с этим становится актуальным вопрос защиты персональных данных.

На уровне законодательства государство требует обеспечения защиты персональных данных от организаций и физических лиц, занимающихся их обработкой. Требования описаны в основополагающем в этой области Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015). В соответствии с этим законом обработка ПДн должна производиться оператором социальной сети, но, стоит отметить, что при этом за конфиденциальность и безопасность своих личных данных отвечает сам пользователь, так как субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие именно в письменном виде не требуется [1]. Следовательно, если лицо само делает информацию общедоступной, то согласие предполагается.

Меры, с помощью которых можно обеспечить безопасность персональных данных в социальной сети, можно разделить на 2 группы: предоставляемые веб-сайтом и независящие от него [3].

Основным инструментом первой группы является разграничение доступа. Это механизм безопасности, предоставляемый почти всеми социальными сетями, который позволяет только определенной категории участников совершать те или иные действия в отношении информации на странице пользователя. Например, при загрузке фотографий можно ограничивать доступ посторонним таким образом, чтобы просматривать их могли только друзья. Стоит отметить, что в текущее время регуляторы в области ПДн (ФСБ РФ, ФСТЭК РФ, Роскомнадзор) относят фотографии к категории биометрических персональных данных, то есть к сведениям, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность [2].

Ко второй группе можно отнести следующие меры. Во-первых, сокращение количества предоставляемых персональных данных. Весьма эффективная мера в случае, если пользователь недавно зарегистрировался в соцсети и еще не успел внести много личных данных. Во-вторых, создание отдельного

e-mail для регистрации в соцсети и его сокрытие с использованием настроек приватности. Необходимость такой защиты объясняется тем, что при указании адреса электронной почты в открытом доступе существует риск попасть в базу данных спамеров и ежедневно получать массу ненужных писем, в том числе вредоносных. Следовательно, третьей мерой можно обозначить игнорирование подозрительных сообщений. Однако если все-таки произошел переход по вредоносной ссылке, то защитить свои персональные данные можно с помощью антивирусных программ и их своевременного обновления. Последняя мера – использование псевдонима. Но это не всегда осуществимо, так как многие сайты придерживаются «политики настоящих имён».

Обобщая вышеизложенное, можно сделать вывод, что социальные сети представляют собой мощный и удобный способ общения с миром. Не стоит забывать, что к данным, в принципе, может получить доступ любой пользователь соцсети. Поэтому чтобы обеспечить безопасность своих персональных данных целесообразно воспользоваться предложенными мерами и прекратить доверчиво публиковать много информации о себе.

**Список использованной литературы:**

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015)
2. Австралийка потеряла выигрыш, выложив в Сеть селфи с призовым чеком // Вести.ru [Электронный ресурс]. – Режим доступа http://www.vesti.ru/doc.html?id=2683507 (дата обращения: 20.11.2015).
3. Мамедов Р. Защита персональных данных в социальных сетях // Information Security [Электронный ресурс]. – Режим доступа http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/ (Дата обращения: 15.12.2015).



**УДК УДК 621.391**

**Танаева Елена Геннадьевна**
аспирант 1 курса,
радиотехнический факультет,
ФГБОУ ВПО «ПГТУ», г. Йошкар-Ола, РФ
E-mail: elena-309@mail.ru
**Хафизов Ринат Гафиятуллович**
доктор технич. наук, профессор
ФГБОУ ВПО «ПГТУ»,
г. Йошкар-Ола, РФ
E-mail: HafizovRG@volgatech.net

## АЛГОРИТМ ВЫДЕЛЕНИЯ СОСУДИСТОЙ СИСТЕМЫ СЕТЧАТКИ НА ИЗОБРАЖЕНИЯХ ГЛАЗНОГО ДНА НА ОСНОВЕ КОНТУРНОГО АНАЛИЗА

**Аннотация**

Предложены алгоритмы контурного анализа для обнаружения и выделения сосудов сетчатки. Применен подход, использованный для обнаружения и прослеживания изображений коммуникационных объектов на сложных ландшафтных сценах

**Ключевые слова**

Сосудистая система сетчатки. Глазное дно. Контурный анализ.