Доклад

на тему «Защита персональных данных в социальных сетях»
дисциплина «Информационная безопасность»

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

Введение

В современном мире социальные сети играют ключевую роль в повседневной жизни людей, выступая как средство общения, обмена информацией и платформой для личного и профессионального развития. Однако с ростом популярности этих сервисов возрастает и угроза нарушения конфиденциальности персональных данных, что делает вопросы информационной безопасности крайне актуальными.

Персональные данные пользователей становятся объектом интереса для хакеров, рекламодателей и недобросовестных организаций, что может привести к утечке информации, ее хищению, вымогательству и другим серьезным последствиям. Публикация конфиденциальных сведений без должной осмотрительности, слабая защита учетных записей и распространение вредоносного ПО — это лишь часть угроз, с которыми сталкиваются люди в социальных сетях. Поэтому для эффективной защиты данных необходимо учитывать как личные меры предосторожности, так и правовые и технологические инструменты. В условиях стремительного роста цифровых технологий эта тема приобретает особую важность [1].

Цель доклада заключается в изучении основных угроз, связанных с защитой персональных данных в социальных сетях, рассмотрении существующих мер по их защите и рекомендациях по повышению уровня безопасности данных пользователей.

Глава 1. Персональные данные в социальных сетях

Персональные данные — это информация, которая прямо или косвенно позволяет идентифицировать личность человека. В контексте социальных сетей под персональными данными подразумеваются как общие сведения (имя, дата рождения, контакты), так и более детализированные данные, например, место проживания, фотографии, интересы, сведения о друзьях и подписках, история активности.

Социальные сети собирают различные типы данных о пользователях. Среди наиболее распространенных категорий:

- Общедоступные данные: имя, фамилия, возраст, пол, фото профиля.
- Контактные данные: номера телефонов, адреса электронной почты.
- Личные предпочтения: лайки, комментарии, подписки, интересы.
- Данные о местоположении: геолокация при использовании приложений.
- Технические данные: IP-адрес, информация об используемых устройствах и браузерах.

Эти данные не только помогают улучшать персонализированные сервисы, но и могут стать целью для кибератак или незаконного использования третьими лицами.

Защита персональных данных регулируется рядом законодательных актов, направленных на обеспечение конфиденциальности и безопасности информации. В Европейском Союзе действует Общий регламент по защите данных (General Data Protection Regulation, GDPR), который вводит строгие правила по сбору, хранению и обработке личных данных,

а также предусматривает значительные штрафы за его нарушение. В России аналогичную функцию выполняет Федеральный закон “О персональных данных” от 27.07.2006 N 152-ФЗ (последняя редакция), который регулирует порядок обработки данных, права субъектов персональных данных и обязанности операторов. В России за соблюдение закона о персональных данных отвечает Роскомнадзор. Он контролирует работу компаний, обрабатывающих данные, и в случае нарушения может вынести предписание, наложить штраф или блокировать доступ к ресурсу [2].

Эти законы обязывают социальные сети защищать персональные данные пользователей, предоставлять им контроль над своими данными и уведомлять о любых нарушениях безопасности.

Глава 2. Основные угрозы безопасности персональных данных

Социальные сети благодаря большому объему хранимых данных становятся привлекательной целью для злоумышленников. Рассмотрим ключевые угрозы, с которыми могут столкнуться пользователи:

1. **Социальная инженерия и фишинг**

Социальная инженерия — это метод воздействия на людей с целью получения конфиденциальной информации путем манипуляций. В социальных сетях злоумышленники могут выстраивать доверительные отношения с пользователями, обманывая их для получения паролей, финансовой информации или личных данных.

Фишинг — это разновидность социальной инженерии, при которой создаются поддельные страницы или отправляются ложные сообщения, чтобы выманить у пользователей их данные. Например, злоумышленники могут присылать ссылки на фальшивые страницы входа, маскируясь под популярные социальные сети или сервисы, чтобы собрать пароли.

2. **Взломы и утечки данных**

Одной из наиболее серьезных угроз является взлом учетных записей пользователей. Это может произойти через подбор слабых паролей, кражу паролей с других сервисов или использование уязвимостей в системах безопасности. Как только злоумышленники получают доступ к аккаунту, они могут использовать данные пользователя для шантажа, мошенничества или продажи информации.

Утечки данных случаются как из-за целенаправленных атак на социальные сети, так и по причине внутренних ошибок в их инфраструктуре. В результате таких утечек персо-

нальные данные миллионов пользователей могут оказаться в руках злоумышленников. Например, известны случаи массовых утечек данных пользователей из таких социальных сетей, как Facebook и LinkedIn (американская социальная сеть для поиска и установления деловых контактов) [3].

3. **Недостатки конфиденциальности по умолчанию**

Многие социальные сети имеют недостаточные настройки приватности по умолчанию, что может приводить к тому, что пользовательские данные становятся доступны широкому кругу людей без явного согласия владельцев данных. Неправильные или недостаточные настройки конфиденциальности могут позволить злоумышленникам получать доступ к личной информации, включая фотографии, список друзей, местоположение и другую чувствительную информацию.

Особенно опасны такие ситуации, когда пользователи не осознают, что их данные видны публично или доступны третьим лицам, что создает дополнительные риски для их безопасности.

4. **Трекинг и поведенческий анализ**

Социальные сети активно используют трекеры (программы отслеживания действий пользователя в интернете) и аналитику для отслеживания поведения пользователей. Эти инструменты позволяют собирать данные о действиях пользователя, его предпочтениях и взаимодействиях с контентом. На основе этих данных могут быть составлены детализированные профили личности, которые затем используются для таргетированной рекламы или передаются третьим лицам без явного согласия пользователя.

Также стоит учитывать риск утечки этих профилей или их использования злоумышленниками для манипуляций и мошенничества. Поведенческий анализ может использоваться для предсказания действий пользователя и построения целевых атак с использованием персональных данных [3].

Глава 3. Методы защиты персональных данных в социальных сетях

В условиях роста угроз безопасности персональных данных социальные сети внедряют различные механизмы защиты для предотвращения утечек и неправомерного использования информации. Рассмотрим основные из них:

1. **Политики конфиденциальности и их соблюдение**

Политика конфиденциальности — это документ, в котором социальная сеть объясняет, какие данные она собирает, как они используются, с кем могут быть поделены и как пользователи могут управлять своей информацией. Политика призвана обеспечить прозрачность и информировать пользователей о том, как их персональные данные защищаются.

Социальные сети обязаны придерживаться заявленных в политике стандартов и следить за соблюдением законодательства, например, таких законов, как GDPR. В случае нарушения политики или утечки данных компании могут подвергаться штрафам, что мотивирует их уделять внимание защите информации.

2. **Шифрование данных и безопасные протоколы**

Шифрование — это метод защиты данных, при котором информация кодируется таким образом, что доступ к ней могут получить только авторизованные пользователи. В социальных сетях применяют различные уровни шифрования для защиты персональных данных при передаче и хранении.

Шифрование данных при передаче: для защиты данных при передаче между устройством пользователя и серверами социальных сетей используется протокол HTTPS (HyperText Transfer Protocol Secure). Этот протокол защищает передаваемую информацию от перехвата злоумышленниками.

Шифрование данных при хранении: для защиты информации на серверах компании может применяться шифрование, которое делает данные недоступными без ключа расшифровки. Это помогает предотвратить доступ к данным даже в случае взлома серверов.

3. **Управление доступом к данным**

Управление доступом — это система контроля, которая определяет, кто и на каких условиях может получать доступ к персональным данным пользователя. Социальные сети позволяют пользователям настраивать уровень доступа к своей информации, например, с помощью настроек приватности [4].

Пользователи могут выбирать, кто может видеть их публикации, фотографии, информацию профиля и другие данные (например, только друзья, друзья друзей или все пользователи).

Управление доступом также включает в себя возможность блокировки других пользователей, ограничения доступа приложений к персональной информации и контроль над тем, какие данные можно делить с третьими лицами.

Эти настройки позволяют пользователям лучше контролировать свою конфиденциальность и предотвращать случайный доступ к данным [4].

4. **Аутентификация и двухфакторная аутентификация (2FA)**

Аутентификация — это процесс подтверждения личности пользователя при входе в аккаунт. Социальные сети используют различные методы аутентификации для повышения безопасности.

Стандартная аутентификация через логин и пароль. Здесь важно использовать сложные и уникальные пароли, которые труднее подобрать злоумышленникам.

Двухфакторная аутентификация (2FA) — это дополнительный уровень безопасности, который требует ввода второго фактора (кроме пароля) для подтверждения личности.

Например, пользователь вводит код, полученный по SMS, через приложение или на электронную почту. Это значительно снижает риск взлома учетной записи, даже если пароль был украден [5].

Многие социальные сети рекомендуют и даже по умолчанию предлагают включить 2FA для повышения уровня безопасности аккаунтов, особенно если аккаунт содержит чувствительную информацию.

Эти механизмы защиты помогают минимизировать риски утечки данных и дают пользователям инструменты для контроля своей приватности. Важно, чтобы пользователи сами активно использовали доступные функции и настраивали безопасность своих аккаунтов в соответствии с личными предпочтениями и уровнем риска.

5. **Пример практик цифровой гигиены**

Цифровая гигиена — это набор привычек, которые помогают пользователям оставаться в безопасности в онлайн-среде.

Регулярное обновление программного обеспечения — обновления часто включают исправления уязвимостей, поэтому своевременное обновление ОС, приложений и браузеров крайне важно.

Двухфакторная аутентификация (2FA) — этот механизм добавляет дополнительный слой защиты: даже если злоумышленник получит пароль, ему потребуется второй фактор (например, код из SMS или приложение-аутентификатор).

Использование антивирусных программ и блокировщиков рекламы, чтобы избежать заражения вредоносным ПО.

Регулярная проверка активности аккаунта — важно проверять, нет ли подозрительных входов в аккаунт или изменений в настройках безопасности.

6. **Блокчейн и децентрализованные платформы**

Блокчейн — это технология, которая активно исследуется как средство повышения безопасности данных в социальных сетях. Она предлагает децентрализованный подход к хранению и защите информации [6].

- Децентрализованное хранение данных. В отличие от централизованных систем, в которых данные хранятся на серверах компаний, блокчейн позволяет хранить

данные на множестве узлов. Это значительно снижает риск утечек, так как взлом одного узла не даст злоумышленникам доступ ко всей информации.

- Прозрачность и неизменяемость данных. Каждая транзакция или изменение данных в блокчейне записывается в публичный реестр и не может быть изменена без согласия участников сети. Это создает высокий уровень доверия и защищает данные от несанкционированных изменений.
- Контроль пользователя над своими данными. Блокчейн позволяет пользователям управлять своими персональными данными, решая, кто может получить доступ к их информации. Пользователи могут выдавать временные права на доступ, что увеличивает уровень контроля и приватности.

Эти меры помогут защитить персональные данные и минимизировать риски, связанные с использованием социальных сетей.

Заключение

В ходе исследования было выявлено, что социальные сети, играя важную роль в нашей жизни, также представляют собой значительные риски для безопасности персональных данных. Основные угрозы, такие как социальная инженерия, взломы и недостатки конфиденциальности, требуют внимательного подхода как со стороны пользователей, так и со стороны самих социальных платформ.

Для повышения уровня безопасности данных рекомендуется [6]:

- Активно использовать настройки конфиденциальности, предоставляемые социальными сетями, чтобы контролировать доступ к своей информации.
- Внедрять механизмы двухфакторной аутентификации для защиты учетных записей.
- Регулярно обновлять пароли и использовать сложные комбинации, чтобы предотвратить их взлом.
- Быть бдительными и осторожными при взаимодействии с подозрительными сообщениями и ссылками.

Важно отметить, что осведомленность пользователей о рисках и методах защиты персональных данных является ключевым аспектом для обеспечения их безопасности в цифровом пространстве. Чем больше люди знают о возможных угрозах и способах защиты, тем эффективнее они смогут защищать свою информацию и минимизировать риски. Таким образом, совместные усилия пользователей и социальных платформ в области информационной безопасности являются залогом надежной защиты персональных данных.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ (последняя редакция) «О персональных данных».
2. 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: 24.09.2024).
3. 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: 24.09.2024).
4. Безопасность в социальных сетях [Электронный ресурс] — Режим доступа — https://whoer.net/blog/bezopasnost-v-socialnyx-setyax/ (дата обращения: 24.09.2024)
5. Шестакова Я. Безопасность персональных данных в социальных сетях // Гуманитарные научные исследования. 2015. № 11 [Электронный ресурс]. URL: https://human.snauka.ru/2015/11/13018 (дата обращения: 24.09.2024).
6. Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза// Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254. DOI: 10.17323/2072-8166.2018.1.234.254