Российский Университет Дружбы Народов

Факультет Физико-Математических и Естественных наук

Направление “Прикладная Математика и Информатика”

Кафедра Прикладной Информатики и Теории Вероятности

Дисциплина

«Основы информационной безопасности»

Реферат на тему: “Защита персональных данных в социальных сетях”

Работу выполнила

Студентка группы НПМбд-02-21

Бабина Юлия Олеговна

№ студенческого билета 1032216525

Москва 2024

В данном реферате мы обсудим важность персональных данных в современном мире и способы ее защиты.

Цель работы: рассмотреть проблему защиты персональных данных в социальных сетях и способы защиты.

Задачи исследования:

- Рассмотреть понятие персональных данных и их значение в современном мире.
- Изучить методы защиты личной информации в социальных сетях.
- Сформулировать рекомендации и наилучшие приемы для защиты персональных данных в социальных сетях.

Введение.

Тема защиты персональных данных в социальных сетях становится все более актуальной и важной для любого пользователя сети. Важно понимать, какие меры защиты применять, чтобы снизить риск кибератак и краж данных. Прежде всего, необходимо понять, что такое персональные данные, и что такое социальная сеть.

Закон о персональных данных.

С точки зрения Федерального закона персональные данные представляют собой любую информацию, прямо или косвенно связанную с определенным лицом (субъектом персональных данных).

Центральное место в системе российского национального законодательства в области персональных данных занимает Федеральный закон "О персональных данных", основанный на конституционных положениях, гарантирующих защиту прав на неприкосновенность частной жизни, личную и семейную тайну. Федеральный закон "О персональных данных" закрепил статус и полномочия российского уполномоченного органа.

Браузер. Режимы использования.

Браузер — это программное обеспечение, которое позволяет выполнять запросы и просматривать веб-сайты.

Браузеры имеют несколько **режимов использования**:

- **Основной режим**
  Браузер сохраняет много информации: история просмотров, закладки, пароли, изображения и др.
- **Режим синхронизации браузера с аккаунтом**
  Личная информация пользователя сохранится на серверах компании, будет работать автозаполнение и автоматический доступ к информации.
- **Гостевой режим и режим инкогнито**
  Загружаемые сайты и файлы не будут записываться в историю.

Социальная сеть. Предоставляемые документы.

Социальная сеть — интерактивный многопользовательский ресурс, содержание которого наполняется участниками сети.

При регистрации социальная сеть предоставляет текст Согласия на обработку персональных данных, Пользовательского соглашения и Политики конфиденциальности.

Согласие на обработку персональных данных - добровольное и информированное согласие субъекта данных на использование его личной информации определенными организациями.

- Включает различные аспекты, такие как цель обработки, тип данных, срок хранения и т.д.
- Согласие должно быть четко выражено, например, через галочку или подписку.

Пользовательское соглашение регулирует отношения между владельцем сайта и посетителем:

- Обладает силой договора.
- В нем определяется статус контента, способ регистрации учетной записи, объем обрабатываемых персональных данных.

Политика конфиденциальности встречается на сайтах, где применяются веб-технологии сбора и обработки персональных данных: если на сайте нужно заполнять профиль при регистрации, если есть механизм подписки, если нужно заполнить форму обратной связи и т.д.

- В **Политике** владелец сайта сообщает, каким образом, кому и когда он будет передавать конфиденциальную информацию, в том числе и персональные данные пользователя и указывает, какие права есть у пользователя, сколько хранятся данные, куда можно обратиться, чтобы прекратить обработку личных данных.
- Иногда в Политике конфиденциальности указывается возможность передачи данных неименованным 3 лицам. **Это запрещено законом.**

Рекомендации для защиты персональных данных в социальных сетях:

- Используйте разные пароли для соцсети и для электронной почты, которую указываете в социальной сети. Пользуйтесь специализированными генераторами паролей или выбирайте сложные пароли, регулярно их меняйте и не храните в открытом виде.
- Заведите два адреса электронной почты:
    - частный – для переписки (который не публикуете в общедоступных источниках)
    - публичный – для соцсетей, форумов, чатов и т.д.

  Если нужно сообщить свой приватный адрес в переписке, лучше сделать это способом, непригодным для автоматического прочтения сборщиком адресов, например, в виде картинки.

- Установите двухфакторную идентификацию, чтобы иметь возможность подтвердить вход в ваш профиль с нового устройства с помощью дополнительного кода, направляемого в СМС-сообщении.
- Настройте ваш профиль в социальной сети таким образом, чтобы только друзья могли его просматривать. Такая настройка лишит злоумышленников возможности получить доступ к информации, которую вы скрыли для просмотра незнакомцев.
- Внимательно относитесь к информации, которую публикуете о себе в социальной сети. Используйте никнейм. Злоумышленник может использовать вашу личную информацию и войти в Вашу учетную запись, а также создать правдоподобные истории для злоупотребления вашим доверием и хищения ваших денег.
- Перед тем как выложить фотографию, оцените каждую деталь: свой внешний вид, окружающую местность, людей, находящихся рядом с вами, и многое другое. Даже если вы сразу удалили публикацию, кто-то мог ее сохранить. Помните о возможных репутационных рисках.
- Не устанавливайте приложения для соцсетей, которые позволяют отследить активность подписчиков на вашей странице.

Огромное количество пользователей ищут способ посмотреть, кто заходил на страницу, и, не разбираясь в теме, верят в то, что есть быстрое и бесплатное решение.
Как правило, при установке такие сервисы запрашивают логин и пароль от аккаунта – все это ухищрения хакеров, создающие риски последующего взлома страницы.

- Не отправляйте важные документы через социальные сети и не публикуйте фотографии документов. Часто обнаруживается, что молодые люди, когда получают водительские права, публикуют их фотографии в открытом доступе. Такими фотографиями могут воспользоваться злоумышленники, изменив их с помощью графических редакторов. Впоследствии от вашего они могут совершать действия, которые будут иметь юридически значимые последствия.
- Перепроверяйте сообщения от друзей с просьбой срочно выслать денег. Сначала перезвоните другу и удостоверьтесь, что просьба действительно направлена от него.
- Проявляйте осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей, если вы не знакомы с отправителем.
- Воздерживайтесь от ответа на провокационные сообщения и комментарии других пользователей. Блокируйте навязчивых провокаторов.
- При завершении работы в социальной сети выходите из своего аккаунта.

Заключение.

В моей работе были рассмотрены возможные способы защиты персональных данных в социальных сетях. Прежде всего, следует отметить, что пользователь сам должен понять, какая информация может быть опубликована, а какая нет. Мы должны публиковать как можно меньше личной информации, чтобы злоумышленники не могли использовать ее в своих целях. Современные социальные сети поддерживают огромный функционал, чтобы персональные данные не стали общедоступными.

Список литературы:

- Ищейнов В. Я. Персональные данные в законодательных и нормативных документах Российской Федерации и информационных системах.: Делопроизводство 2022
- Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) https://corp.mail.ru/ru/press/infograph/9037/
- Буянов, Д. С. Информационная безопасность в социальных сетях / Д. С. Буянов. Молодой ученый. — 2018. — № 39 (225). — С. 14-16. — URL: https://moluch.ru/archive/225/52820/ (дата обращения: 28.09.2024).