Защита персональных данных в социальных сетях

Имаев Камиль Маратович

Информатика

11 класс, МАОУ лицей №94 г. Уфы, г. Уфа, Республика Башкортостан

Научный руководитель: Карабельская Ирина Владимировна, доцент кафедры цифровых технологий и моделирования Уфимского государственного нефтяного технического университета

Актуальность

Существование в современном глобальном информационном пространстве невозможно без предоставления какого-либо вида персональных данных. При регистрации пользователь обязан указать сведения о себе, которые автоматически переносятся в информационную систему учета. К самой популярной информации такого рода относится: ФИО, номер телефона, e-mail-адрес (электронная почта), место проживания и т.д. В зависимости от специфики также могут добавляться второстепенные вопросы, такие как: имя домашнего питомца, любимый цвет, девичья фамилия матери и т.д. В связи со стремительным развитием мошенничества в сети Интернет возникает потребность в защите персональных данных пользователей, что обуславливает актуальность темы данной статьи.

Пожалуй, одна из самых важных задач обеспечения безопасности – конфиденциальность. Многие платформы в глобальной сети предусматривают возможность ограниченности видимости персональной информации только для выбранных лиц (например, друзей или родственников). Параллельно с этим актуализируются задачи сохранения целостности представляемых данных, а также создание гарантий их подлинности (последнее связано с ростом страниц «клонов» и «фейков»). Для защиты собственных страниц и данных необходимо пользоваться механизмами безопасности – как теми, что предлагают различные социальные сети, так и общими механизмами безопасности Интернета. Также предельно важным фактором является бдительность пользователя и его поведенческая стратегия, на чем мы и сконцентрируемся в данной статье.

Пользовательская активность жителей России в глобальной сети Интернет увеличивается с каждым годом в несколько раз. Как указывают

данные общедоступной статистики, практически 100% людей ежедневно пользуются онлайн-сервисами для различных целей. Соответственно, можно сделать вывод о том, что человеку в XXI веке стало трудно обходиться без Интернета. К сожалению, из-за низкого уровня социальной ответственности или неосведомленности многие оказываются жертвами мошенников из-за предоставления излишней информации о себе. Именно поэтому проблема правового регулирования обработки персональных данных в Интернете становится с каждым днем все более актуальной.

Пользователи в онлайн-пространстве подразделяются на тех, кто использует ресурсы для пользы – поиска информации, заказа товаров и услуг, и тех, кто преследует гедонистические цели – прослушивание музыки и подкастов, просмотр фильмов, ведение социальных сетей, прохождение игр. Вторая категория пользователей, как правило, редко задумывается о наличии правообладателей у всех типов просматриваемого контента. Именно поэтому пользователи часто оказываются заложниками собственных действий.

Материалы и методы

В последние годы активно ведется обсуждение кибербезопасности в средствах массовой информации – радио, телевидении, периодических изданиях. На основе опросов можно сделать вывод о том, что большинство пользователей даже не знакомы с нормами поведения в Интернете. К сожалению, практически безграничная свобода и доступ к информации не разрешает ее свободное использование и распространение.

Как же это регулируется на сегодняшний день? В случае, если человек добровольно предоставил о себе данные в открытом доступе, тогда эта информация автоматически становится общедоступной для всех пользователей Интернета. Это правило действует на основании Федерального закона №149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 [2], конкретно статья 7, пункт 2: «общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации».

Поэтому каждый пользователь должен бдительно относится к той информации, что он предоставляет на своих страницах в социальных сетях и других онлайн-ресурсах. Информация может использоваться мошенниками и злоумышленниками для самых различных целей[3]. К примеру, номер телефона или домашний адрес используются мошенниками

для совершения преступлений в Интернете. Они воруют данные и используют их в личных целях.

Нельзя забывать о том, что все, что однажды попало во «всемирную паутину» – навсегда останется там. Это работает также крайне часто и против не предусмотрительных мошенников, так как в юридической практике стали частыми случаи использования данных анкет в социальных сетях при рассмотрении уголовных дел.

Каким образом можно обезопасить себя и свои данные в социальных сетях и Интернете[4]? Безусловно, знание простых, но важных правил поможет спастись от неприятных последствий.

В первую очередь не стоит добавлять и добавляться в друзья/подписываться на подозрительных и незнакомых лиц. Именно на таких ресурсах размещают вредоносные ссылки, по которым с легкостью взламываются защиты телефона. Мошенники попадают в телефон и воруют все пароли не только от страниц в социальных сетях, но и пароли от онлайн-банков. Кроме того, злоумышленники получают доступ к вашим фотографиям и личным перепискам. Именно поэтому категорически запрещается переходить по любым подозрительным ссылкам на внешние ресурсы[5].

Также стоит внимательно изучать пользовательские настройки любых ресурсов, куда вы вносите свои данные, такие как: ФИО, e-mail, номер телефона и т.д. Политика конфиденциальности многих популярных ресурсов выстроена таким образом, что пользователь самостоятельно может определить круг лиц, кому будет доступна личная информация и все персональные данные. Фильтрация поможет скрыть информацию от злоумышленников и использовать ресурсы Интернета только в свою пользу.

Вывод

Таким образом, бдительность и выполнение простых правил позволит максимально обезопасить персональные данные пользователей в глобальной сети. Важно постоянно быть «начеку» и контролировать отправляемые сообщения в личных и групповых переписках, а также при публикации фотографий и других материалов в общий доступ. Для взломщиков и мошенников преград нет, поэтому пользователи должны быть уверены в том, что даже если страницу взломают – никакая информация внутри переписок не будет иметь веса и использована против человека в корыстных целях. Бдительность, спокойствие и ответственность

за каждое действие в Интернете обеспечивает внушительный уровень безопасности для пользователей. Также следует отметить, что с ростом мошенничества в Интернете, растет и уровень решение в области информационной безопасности в целом. Таким образом компании все внимательнее относятся к публичным данным и информации, все усложняя условия для развития кибермошенничества в России.

Список использованных источников:

1. Конституция Российской Федерации: утверждена на всенародном голосовании 12 декабря 1993 года. [Электронный ресурс]. Режим доступа: http://www.constitution.ru /. (дата обращения: 25.02.2025).
2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798 /. (дата обращения: 25.02.2025).
3. Кочеткова Е. Как защитить личные данные в Интернете [Электронный ресурс]. Режим доступа: https://blog.kaspersky.kz/privacy-ten-tips/10390 /. (дата обращения: 4.03.2025)
4. О защите персональных данных в интернете/АО "Лаборатория Касперского"/[Электронный ресурс]. Режим доступа: https://support.kaspersky.com/help/Kaspersky/Win21.17/ru-RU/82527.htm /.(дата обращения: 4.03.2025)
5. Конфиденциальность и предотвращение утечки данных в социальных сетях /АО "Лаборатория Касперского"/[Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/social-media-privacy /.(дата обращения:4.03.2025)