

Быкадоров Константин Дмитриевич

студент

Кривошеев Сергей Владимирович

старший преподаватель

ФГБОУ ВО «Донской государственный технический университет»

г. Ростов-на-Дону, Ростовская область

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ И ЗАЩИТЫ ДАННЫХ В ЭПОХУ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: статья затрагивает актуальные вопросы конфиденциальности и защиты данных в условиях стремительного развития информационных технологий. Авторами обсуждаются основные вызовы, с которыми сталкиваются пользователи и организации, включая увеличение объемов персональных данных, недостаточную осведомленность пользователей о своих данных и недостатки в законодательстве. Рассматриваются технологические решения по усилению защиты данных, такие как шифрование и блокчейн.

Ключевые слова: конфиденциальность данных, защита данных, информационные технологии, цифровая безопасность, утечка данных, правовое регулирование, шифрование, блокчейн.

В современном мире, где каждый аспект нашей жизни всё более цифровизируется, вопросы конфиденциальности и защиты личных данных приобретают особую значимость. С ростом объемов генерируемых данных и их интеграцией в различные аспекты нашего бытия – от социальных сетей до телемедицины и финансовых услуг – возникают новые вызовы для защиты нашей приватности [1]. Эти данные, будучи ценным ресурсом, могут также стать уязвимыми точками, подвергая риску личную и финансовую безопасность миллионов людей.

По мере того, как информационные технологии продолжают развиваться, также развиваются и методы, с помощью которых злоумышленники могут эксплуатировать личные данные. Таким образом, становится критически важным уделять внимание мерам защиты данных и методам обеспечения

конфиденциальности, чтобы обеспечить безопасность и доверие в цифровую эпоху. В статье рассмотрены основные проблемы и вызовы, с которыми сталкиваются современные пользователи и организации в связи с конфиденциальностью и защитой данных в условиях быстро меняющегося технологического ландшафта.

В эпоху информационных технологий проблемы конфиденциальности и защиты данных становятся все более актуальными. С каждым днем возрастает объем данных, которые пользователи оставляют в интернете через социальные сети, банковские услуги, медицинские записи и другие сервисы. Эта информация часто становится целью для киберпреступников, что подчеркивает необходимость более строгих мер безопасности.

Рост уязвимости данных.

С развитием технологий увеличивается не только количество собираемой информации, но и способы ее использования. Интеллектуальный анализ данных позволяет компаниям настраивать маркетинг под конкретного пользователя, что может приводить к нарушению приватности. Кроме того, уязвимости в программном обеспечении и хранении данных могут стать причиной их утечек.

Недостаток осведомленности среди пользователей.

Многие пользователи не осознают, как много личной информации они оставляют в интернете, и как эта информация может быть использована. Отсутствие понимания принципов работы интернет-технологий и сложности правовых документов, таких как политика конфиденциальности, только усугубляет проблему.

Нормативно-правовая база.

Законодательство в области защиты данных часто отстает от темпов развития технологий. Примером может служить общий регламент защиты данных (GDPR) в Европейском союзе, который стал шагом вперед в попытке регулировать обработку личных данных. Однако даже такие комплексные меры не всегда могут предотвратить все случаи злоупотребления.

Технические аспекты защиты данных.

Существует множество технологических решений для усиления защиты данных, включая шифрование, двухфакторную аутентификацию и блокчейн. Однако их реализация требует значительных ресурсов и специализированных знаний, что может быть недоступно многим организациям.

В заключение, проблемы конфиденциальности и защиты данных в эпоху информационных технологий требуют комплексного подхода и активного взаимодействия между технологиями, законодательством и общественным сознанием. Мы стоим на пороге новой эры, где каждый клик, каждое сообщение и каждая транзакция может быть записана, проанализирована и использована [2]. Это создает как невероятные возможности для прогресса, так и серьезные риски для личной приватности. Для защиты данных на всех уровнях необходимо не только применение передовых технологий, но и строгое соблюдение нормативных стандартов, а также повышение уровня осведомленности и образованности пользователей. Пользователи должны быть более информированы о том, как и где их данные используются и какие меры они могут предпринять для их защиты.

Список литературы

1. Гидденс Э. Судьба, риск и безопасность / Э. Гидденс // THESIS. – 1994. – №5. – С. 108–109.
2. Баглай М.В. Конституционное право Российской Федерации: учеб. для вузов / М.В. Баглай. – 6-е изд., изм. и доп. – М.: Норма, 2007. – 784 с. EDN PZUDKV