Emro Science and Education
International open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · "Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnol... DOI: 10.5281/zenodo.24319084

materiallar to'plami

АНАЛИЗ И СТРАТЕГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ: СОВРЕМЕННЫЕ ВЫЗОВЫ И РЕШЕНИЯ

Рахимов Дилмурад Бахадирович, Старший преподаватель, Андижанский машиностроительный институт, Город Андижан, Республика Узбекистан.

АННОТАЦИЯ

В условиях нарастающей цифровизации и использования технологий, персональные данные становятся все более важным активом в обществе. Использование информационных технологий и цифровых услуг в стране растет с каждым годом, что вызывает необходимость обеспечения надлежащей защиты персональной информации граждан. Охрана этих данных становится основным приоритетом для пользователей, организаций и государства. В данной статье представлен обзор современных вызовов и решений в области обеспечения безопасности персональных данных с учетом технологического развития и регулятивных мер.

Ключевые слова: персональные данные, киберпреступники, социальная инженерия, кибербезопасность, шифрование данных, управление доступом, авторизация.

Введение: Современная цифровая эпоха характеризуется высоким уровнем доступности и обработки персональных данных. Однако, с ростом количества сетевых нарушений и киберпреступности, вопрос обеспечения безопасности персональных данных становится все более важным. В данной статье представлен обзор существующих методов и вызовов в области безопасности персональных данных, а также предложены рекомендации для их защиты.

Использование базы данных, интернета и смарт-устройств, сбор и обработка персональных данных стало незаменимой практикой для многих организаций в бизнесе, здравоохранении, образовании и государственных структурах.

Для регулирования отношений возникающие при обработке и защите персональных данных, независимо от применяемых средств обработки, включая информационные технологи, был принят Закон Республики Узбекистан от 02 июля 2019 года за № ЗРУ-547 "О персональных данных" [1].

Преимущества создания персональных данных:

- Структурированное и организованное хранение данных;
- Управление данными;
- Широкий доступ;
- Повышенная производительность;
- Легкость анализа данных.

Однако, данная практика влечет за собой ряд рисков и угроз безопасности персональных данных. Данные могут быть скомпрометированы, украдены или

Published: 10.11.2023

Cite this article: Рахимов Дилмурад Бахадирович (2023). Анализ и стратегии обеспечения безопасности персональных данных: современные вызовы и решения. Emro Science and Education, 1(1). https://doi.org/10.5281/zenodo.24319084

© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

использованы несанкционированным образом, что может привести к серьезным последствиям для общества в целом.

При анализе современных вызовов были выявлены ряд новых угроз. С развитием технологий, появляются новые способы атак на системы хранения и обработки персональных данных. Киберпреступники становятся все более изощренными и криптографических методов защиты данных все сложнее взломать. В условиях глобального информационного пространства, данные могут передаваться через границы государств и юрисдикций, что создает сложности в их защите и регулировании.

Человеческий фактор остается одним из наиболее уязвимых звеньев в цепи безопасности персональных данных. “Социальная инженерия” позволяет злоумышленникам получать доступ к данным путем манипуляции людьми (слабо защищенные социальные слои населения, пенсионеры).

Социальная инженерия - метод манипуляции и взаимодействия с людьми с целью получения конфиденциальной информации, внедрения в организацию или выполнения незаконных действий. Основная идея социальной инженерии заключается в использовании манипуляций и уловок для убеждения людей в необходимости раскрыть секреты, установить доверие или предоставить доступ к защищенной информации. Эта практика широко используется хакерами, мошенниками и другими злоумышленниками для несанкционированного доступа к информации или выполнения противоправных действий [2].

Так в июле 2020 года согласно статье сайта Spot данные миллионов пользователей мессенджера Telegram утекли в сеть. В Центре кибербезопасности сообщили, что речь идет о синтезе нескольких баз данных, содержащих такие данные, как name, fname, phone, uid и nickname. Всего таких строк в находящейся в свободном доступе базе 40640449, из которых 50062 относятся к номерам узбекских сотовых операторов [3].

Повторный случай произошёл 18 октября 2023 года, когда специалистами ГУП “Центр кибербезопасности” в ходе мониторинга сети Интернет выявили базу учетных записей пользователей различных информационных ресурсов по всему миру, в том числе и нашей республики.

Специалистами в ходе изучения опубликованной в Telegram канале базы скомпрометированных учётных записей установлено более 200,000 учётных записей, большая часть которых является актуальными и несут угрозы кибербезопасности в отношении информационных систем и ресурсов государственных органов и иных организаций [4].

Для дальнейшего обеспечения безопасности персональных данных граждан Республики Узбекистан необходимо разработать Стратегию обеспечения безопасности:

К ним относятся - шифрование данных, управление доступом и авторизация, обучение персонала особенно социально уязвимые слои населения.

Строгое соблюдение рекомендаций экспертов ГУП “Центр кибербезопасности” о наиболее вероятных причинах утечек персональных данных:

- использовать только официальные версии программ и приложений;
- не открывать файлы и не переходить по ссылкам в сообщениях, группах и каналах, без уверенности в отправителе и его благонадежности;
- использовать надежные антивирусные программы;
- оградить компьютеры и другие устройства, используемых для удаленной работы, от использования посторонними лицами;
- не передавать, оставлять персональные данные и их носителей незнакомым лицам (паспорт, водительское удостоверение и др.)
- пользоваться надёжными паролями;
- своевременное выявление инсайдеров (недовольный чем-либо сотрудник компании, имеющий доступ к клиентской базе, крадёт конфиденциальные данные для последующей продажи).

Заключение:

В современном информационном обществе безопасность персональных данных является ключевым элементом для защиты индивидуальных прав и свобод граждан. В целом, данная научная статья обнаружила и проанализировала текущую ситуацию с безопасностью персональных данных в Узбекистане.

Результаты исследования показали, что в Узбекистане существуют определенные недостатки и проблемы в области безопасности данных, такие как недостаточное развитие законодательства, слабое информационное образование и недостаточное уровень осведомленности населения.

Однако, статья также выявила некоторые положительные сдвиги и усилия, предпринятые правительством и компаниями для улучшения ситуации, такие как создание законодательства и разработка средств безопасности данных. Реализация гарантированной безопасности персональных данных в Узбекистане является сложной задачей, но совместные усилия всех заинтересованных сторон могут привести к решению данной проблемы и созданию надежной системы защиты данных в стране.

Литература

1. **Закон Республики Узбекистан № ЗРУ-547 “О персональных данных” от 02 июля 2019 года за https://lex.uz/docs/4396428**
2. ***Кристофер Хэднеги, Искусство обмана. Социальная инженерия в мошеннических схемах, Москва: Альпина Паблишер, 2020, p. 322.***
3. **https://www.spot.uz/ru/2020/07/06**
4. **https://kun.uz/ru/news/2023/10/20**