ДОИ

УДК 001.11

Кодиров Зохид Зокирханович
доцент кафедры «Управление бизнесом»
Turan International University
Республика Узбекистан, г.Наманган

Собиржонов Хумоюн Бобуржон угли
преподаватель кафедры «Управление бизнесом»
Turan International University
Республика Узбекистан, г.Наманган

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ В УЗБЕКИСТАНЕ

Аннотация. В статье раскрываются меры защиты информации в социальных сетей в Узбекистане. Республике Узбекистан планомерно осуществляются мероприятия по обеспечению защиты информации в средствах ИКТ. Следует также отметить, внимание руководства страны к обеспечению кибербезопасности в Республике Узбекистан.

Ключевые слова: социальный сеть, информационная безопастность, кибербезопасность, киберугрозы, кибер атака, защита информации, пароли и аутентификация.

Kodirov Zohid Zokirkhanovich
Associate Professor of the Department of Business Management
Turan International University

Republic of Uzbekistan, Namangan
Sobirjonov Khumoyun Boburjon ugli
Lecturer of the Department of Business Management
Turan International University
Republic of Uzbekistan, Namangan

MEASURES OF PROTECT INFORMATION IN SOCIAL NETWORKS IN UZBEKISTAN

Annotation. The article reveals measures to protect information on social networks in Uzbekistan. The Republic of Uzbekistan is systematically implementing measures to ensure the protection of information in ICT facilities. It should also be noted that the country's leadership pays attention to ensuring cybersecurity in the Republic of Uzbekistan.

Keywords: social network, information security, cybersecurity, cyber threats, cyber attack, information protection, passwords and authentication.

В эпоху цифровизации и массового использования социальных сетей защита персональных данных пользователей становится одной из ключевых проблем информационной безопасности. Социальные сети, являясь платформами для общения и обмена информацией, собирают огромное количество данных о пользователях, включая их личные данные, интересы, контакты и предпочтения. Это делает их уязвимыми к утечкам, кибератакам и манипуляциям. Основными угрозами для информации в социальных сетях являются несанкционированный доступ, фишинг, утечка данных и неправомерное использование персональной информации третьими лицами. Для защиты данных пользователей необходимы такие меры, как сильная аутентификация, шифрование данных, контроль над

настройками приватности, а также регулярное повышение цифровой грамотности среди пользователей.

С развитием цифровых технологий и растущей популярностью социальных сетей в Узбекистане вопрос защиты информации становится все более актуальным. В условиях быстрого распространения интернета и активного использования соцсетей населением, защита персональных данных пользователей сталкивается с рядом вызовов, таких как кибератаки, несанкционированный доступ и утечка данных. Правительство Узбекистана принимает меры по усилению информационной безопасности, включая принятие законов, направленных на защиту персональных данных, таких как Закон "О персональных данных". Однако для повышения эффективности защиты информации необходима активная работа по улучшению цифровой грамотности пользователей, усилению механизмов контроля за соблюдением конфиденциальности данных и внедрению передовых технологий, таких как двухфакторная аутентификация и шифрование.

Улучшение цифровой грамотности пользователей социальных сетей в Узбекистане - это важная задача, направленная на повышение безопасности и ответственности граждан при использовании интернета. В условиях стремительного роста числа пользователей социальных сетей и цифровых сервисов в стране важно формировать навыки безопасного поведения онлайн, что включает в себя:

1. **Осведомленность о киберугрозах**: Пользователи должны понимать, какие угрозы существуют в сети — фишинг, мошенничество, кража данных — и как избежать их. Для этого необходимы образовательные программы и регулярные кампании по повышению осведомленности.
2. **Защита личной информации**: Люди должны знать, как настраивать приватность в социальных сетях, чтобы контролировать, кто видит их личную информацию, фотографии и посты.

3. **Безопасные пароли и аутентификация**: Обучение созданию надежных паролей и использование методов двухфакторной аутентификации могут значительно снизить риски взлома аккаунтов.

4. **Критическое мышление**: Важно развивать у пользователей способность критически оценивать информацию, чтобы не поддаваться на фейковые новости и манипуляции в социальных сетях.

5. **Ответственное поведение онлайн**: Пользователи должны быть информированы о цифровом этикете, уважении к правам других и ответственности за свои действия в сети.

6. **Государственные и общественные инициативы**: В Узбекистане можно усилить сотрудничество между государственными органами, образовательными учреждениями и частным сектором для проведения тренингов, семинаров и создания образовательных платформ, которые помогут пользователям лучше ориентироваться в вопросах безопасности в интернете.

Эти шаги помогут повысить цифровую грамотность и снизить риски, связанные с киберугрозами, что, в свою очередь, обеспечит безопасное и ответственное использование социальных сетей в Узбекистане.

Меры защиты информации в социальных сетях в Узбекистане включают как государственные инициативы, так и действия со стороны самих пользователей и платформ для обеспечения безопасности персональных данных. Основные меры:

1. Законодательные меры

- **Закон "О персональных данных"**: В Узбекистане действует закон, который регулирует сбор, обработку и хранение персональных данных граждан, включая данные, предоставленные в социальных сетях. Он требует от организаций соблюдения строгих стандартов защиты данных.

– **Кибербезопасность**: Государственные органы, такие как Центр кибербезопасности, занимаются мониторингом и предотвращением кибератак, направленных на социальные сети и другие онлайн-сервисы.

2. Контроль над использованием данных

– Социальные сети обязаны соблюдать законы Узбекистана и предоставлять пользователям инструменты для управления своими данными, например, настройки приватности, возможность удалять данные или ограничивать доступ к ним.

– Регулирование использования данных требует от компаний получать согласие пользователей перед обработкой их данных.

3. Технические меры

– **Шифрование данных**: Многие социальные сети используют методы шифрования для защиты передаваемой информации и сообщений от несанкционированного доступа.

– **Двухфакторная аутентификация (2FA)**: Этот метод дополнительной проверки подлинности пользователей через телефон или электронную почту помогает защитить аккаунты от взлома.

4. Пользовательские меры

– **Настройки приватности**: Пользователи могут контролировать, кто видит их профиль, посты и личную информацию, настроив уровни доступа к своим данным в социальных сетях.

– **Создание надежных паролей**: Регулярное обновление паролей и использование сложных комбинаций символов помогают защитить аккаунт.

– **Цифровая грамотность**: Важно обучение граждан безопасному поведению в интернете, включая осведомленность о фишинге, вредоносных ссылках и других угрозах.

5. Государственные инициативы

- **Информационные кампании**: Для повышения цифровой грамотности в Узбекистане проводятся кампании, направленные на обучение пользователей основам безопасного поведения в социальных сетях.
- **Национальная программа по кибербезопасности**: Включает развитие и внедрение новых стандартов защиты данных и информационных систем на государственном уровне.

Эти меры направлены на защиту данных пользователей социальных сетей и предотвращение их несанкционированного использования в Узбекистане, что особенно важно в условиях роста киберугроз.

Заключение:

Защита информации в социальных сетях в Узбекистане приобретает все большее значение на фоне активного роста цифровизации и использования интернет-платформ. В условиях глобальных киберугроз важно обеспечивать безопасность персональных данных граждан, а также предотвращать несанкционированный доступ к ним. Государственные меры, такие как законодательные акты, направленные на защиту данных, и развитие кибербезопасности, играют ключевую роль в формировании безопасной цифровой среды.

Однако, для максимальной эффективности необходимо активное сотрудничество всех участников — от государства и технологических компаний до самих пользователей. Важно продолжать развивать цифровую грамотность населения, внедрять современные технологии защиты, такие как шифрование и двухфакторная аутентификация, и усиливать контроль над обработкой персональных данных.

Таким образом, комплексный подход, сочетающий законодательные, технические и образовательные меры, является залогом надежной защиты информации в социальных сетях в Узбекистане, что способствует не только

безопасности данных, но и доверительному использованию цифровых технологий.

Список использованных литератур:

1. Закон Республики Узбекистан "О персональных данных" № ЗРУ-547 от 2 июля 2019 года.
2. Постановление Кабинета Министров Республики Узбекистан "О мерах по усилению защиты персональных данных" № ПП-4702 от 21 апреля 2020 года.
3. Абдукаримов Б.К. "Анализ правовых аспектов защиты персональных данных в Узбекистане". Журнал "Юридическая наука", 2020.
4. Маматкулов И.И. "Киберугрозы и методы защиты данных в социальных сетях: опыт Узбекистана". Вестник информационных технологий, 2021.
5. Каримова Д.А. "Цифровая грамотность и ее роль в защите персональной информации в социальных сетях". Журнал "Информационные технологии и безопасность", 2022.
6. З. З. Кодиров, Д. В. Студенкова, Д. Ф. Косимов. “Возможности географических информационных систем в Узбекистане” - Молодой ученый учредители: ООО, 2022.
7. Inamova, G. A., & Kodirov, Z. Z. (2020). RELEVANCE AND DEVELOPMENT OF DISTANCE LEARNING IN UZBEKISTAN. Theoretical & Applied Science, (7), 60-62.
8. Официальный сайт Комитета по защите персональных данных Узбекистана. dpm.gov.uz
9. Международные исследования по вопросам кибербезопасности, доступные на платформах Cybersecurity Ventures и Global Cybersecurity Index.