**810414400660**

**87711519918**

****

**СУЛЕЙМЕНОВА Айман Пакитовна,**

**Ө.Жолдасбеков атындағы №9 IT лицейінің информатика пәні мұғалімі.**

**Шымкент қаласы**

**ТЕМА СТАТЬИ: КИБЕРБЕЗОПАСНОСТЬ И ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ: ВЫЗОВЫ СОВРЕМЕННОСТИ**

**Актуальность темы**

В современном мире цифровые технологии стремительно развиваются, охватывая все сферы жизни. Онлайн-банкинг, электронные документы, социальные сети и государственные сервисы — всё это требует надежных механизмов цифровой идентификации и защиты персональных данных. Однако с увеличением количества цифровых сервисов растет и число киберугроз: мошенничество, кража данных, фишинговые атаки, несанкционированный доступ и другие виды киберпреступности. Особенно актуально это в свете увеличения числа дистанционных сервисов и удаленной работы, что делает пользователей более уязвимыми.

В связи с этим вопрос кибербезопасности и цифровой идентификации становится как никогда актуальным, требуя новых решений и подходов к защите данных. Онлайн-банкинг, электронные документы, социальные сети и государственные сервисы — всё это требует надежных механизмов цифровой идентификации и защиты персональных данных. Однако с увеличением количества цифровых сервисов растет и число киберугроз: мошенничество, кража данных, фишинговые атаки, несанкционированный доступ и другие виды киберпреступности. В связи с этим вопрос кибербезопасности и цифровой идентификации становится как никогда актуальным.

**Цифровая идентификация: фундамент цифровой безопасности и эффективного управления личными данными**

Цифровая идентификация — важный элемент цифровой безопасности, который обеспечивает надежность и защиту персональных данных. это процесс подтверждения личности пользователя в онлайн-пространстве. Она необходима для безопасного доступа к финансовым, государственным и корпоративным сервисам. Основные методы цифровой идентификации включают как традиционные, так и современные технологии, направленные на повышение надежности защиты данных и удобства пользователей:

1. **Пароли и PIN-коды** – традиционные, но подверженные взлому методы.
2. **Биометрическая идентификация** – распознавание лица, отпечатков пальцев, радужной оболочки глаза.
3. **Двухфакторная и многофакторная аутентификация (2FA, MFA)** – комбинация пароля и дополнительного подтверждения через SMS, email или биометрию.
4. **Электронные подписи и цифровые сертификаты** – используются для юридически значимых действий в сети.

**Угрозы цифровой идентификации**

Несмотря на развитие технологий, цифровая идентификация остаётся уязвимой перед киберугрозами, которые становятся всё более изощрёнными. Киберпреступники используют новейшие методы взлома, включая искусственный интеллект для генерации поддельных данных, обход биометрической защиты и атаки на облачные сервисы. Основные риски включают:

* **Фишинговые атаки** – мошенники пытаются выманить личные данные через поддельные сайты и письма.
* **Кража учетных данных** – использование утекших баз данных для несанкционированного доступа.
* **Вредоносное ПО** – программы, перехватывающие данные пользователей.
* **Социальная инженерия** – манипуляции, направленные на получение конфиденциальной информации.
* **Атаки на мобильные устройства** – рост популярности мобильных платежей и приложений делает их целью для злоумышленников.
* **Компрометация биометрических данных** – несмотря на высокий уровень защиты, биометрическая информация также может быть украдена или использована в обходных схемах.. Основные риски включают:

**Способы защиты цифровой идентичности**

Чтобы минимизировать риски, необходимо соблюдать ряд правил:

* Использовать сложные и уникальные пароли, менять их регулярно.
* Включить двухфакторную аутентификацию.
* Проверять подлинность сайтов перед вводом личных данных.
* Не передавать пароли и личные данные третьим лицам.
* Использовать антивирусное ПО и регулярно обновлять программное обеспечение.
* Применять аппаратные ключи безопасности для дополнительной защиты.
* Ограничивать доступ к личным данным и использовать минимально необходимый объем информации при регистрации на онлайн-сервисах.
* Регулярно проверять свои учетные записи на предмет утечки данных и при необходимости менять пароли.

Чтобы минимизировать риски, необходимо соблюдать ряд правил:

* Использовать сложные и уникальные пароли, менять их регулярно.
* Включить двухфакторную аутентификацию.
* Проверять подлинность сайтов перед вводом личных данных.
* Не передавать пароли и личные данные третьим лицам.
* Использовать антивирусное ПО и регулярно обновлять программное обеспечение.

**Заключение**

Кибербезопасность и цифровая идентификация — это не только ответственность компаний и государства, но и каждого пользователя. Важно осознавать угрозы и предпринимать меры по защите своих данных. В условиях цифровой трансформации высокий уровень осведомленности и грамотное использование технологий станут залогом безопасности в онлайн-пространстве.

Кроме того, необходима государственная поддержка в виде ужесточения законодательных мер, создания национальных стратегий по кибербезопасности и популяризации образовательных программ. Только комплексный подход поможет защитить цифровую идентичность граждан и создать безопасную цифровую среду.

Дополнительно, важно развивать международное сотрудничество в области кибербезопасности, поскольку киберугрозы не имеют границ. Обмен опытом, совместные исследования и внедрение глобальных стандартов помогут эффективно бороться с новыми угрозами и укрепить доверие в цифровом мире.

**Список литературы:**

1. **Калинин, И. В.** (2021). Цифровая идентификация и кибербезопасность: теоретические аспекты и практика применения. М.: Научный мир.
2. **Смирнов, А. Н.** (2022). Современные угрозы кибербезопасности и методы защиты персональных данных. Санкт-Петербург: Издательство "РосБизнес".
3. **Тимофеев, В. П.** (2023). Биометрическая идентификация в условиях цифровой трансформации. Москва: Физматлит.
4. **Шевченко, О. Г.** (2020). Киберугрозы и методы их предотвращения: от фишинга до использования искусственного интеллекта. М.: ИТЕК.
5. **Баринов, Д. И.** (2021). Электронная подпись и цифровая идентификация: правовые и технические аспекты. Новосибирск: Сибирское университетское издательство.
6. **FBI Cyber Crime Division.** (2022). Cybersecurity and Identity Theft. Available at: https://www.fbi.gov/investigate/cyber.
7. **ISO/IEC 27001:2013.** Information security management systems — Requirements. International Organization for Standardization (ISO), 2013.
8. **Bishop, M.** (2021). Computer Security: Art and Science. Addison-Wesley.