Яппаров Даниэль Фанилевич
студент
ФГБОУ ВО «Кубанский государственный аграрный
университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

ЦИФРОВАЯ ГИГИЕНА: КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В СОВРЕМЕННОЙ ЦИФРОВОЙ СРЕДЕ

Аннотация: *автор статьи подчеркивает, что в эпоху активной цифровизации личные данные граждан находятся в опасности. В работе проанализировал практические правила для использования инновационных технологий. Эти основы предназначены для защиты персональных данных, финансовых активов (акции, облигации, ценных бумаг) и цифровой репутации, что обеспечит безопасность в информационной среде.*

Ключевые слова: *цифровая гигиена, защита данных, кибербезопасность, конфиденциальность, персональные данные, многофакторная аутентификация.*

Все действия пользователей в информационной среде оставляют после себя детализированный цифровой след. Он отражает историю поисковых запросов, интересов потребителя, предпочтения в социальных сетях и его местоположение. Маркетплейсы и другие аналогичные интернет-платформы заинтересованы в аналитике подобных данных и осуществляют анализ посредством использования определенных алгоритмов, поскольку это важный компонент для формирования рекомендаций для пользователя. Благодаря этим процессуальным действиям онлайн-сервисы стремятся оптимизировать вовлеченность пользователей и обеспечить свою экономическую стабильность. Несмотря на это, указанные информационные данные представляют ценность и для правонарушителей, мошенников, которые могут применить их в своей противоправной деятельности для извлечения незаконной прибыли [1]. Из этого следует, что для пользователя управление цифровым следом является основой персональной кибербезопасности, требующей внедрения цифровой гигиены [2].

Она представляет собой не одноразовую процедуру, а систему регулярных действий, которые направлены на минимизацию рисков и повышения уровня безопасности пользователя интернета [3].

Использование простых парольных комбинаций, например, «12345678» или состоящие из личной информации больше не соответствуют современным меркам надежной защиты [4]. Указанные пароли очень уязвимы, что делает их крайне восприимчивыми к грубуму перебору (brute force). Инновационные технологии способны перебирать миллиарды комбинаций в минуту [5]. Восьмизначный пароль, состоящий только из цифр, может быть взломан мгновенно, тогда как сложный пароль, включающий в себя разные регистры букв и специальные символы, увеличивают теоретическое время взлома до нескольких десятков лет за счет резкого увеличения количества возможных комбинаций.

Идеальный пароль должен характеризоваться длиной (10–12 символов), сложностью (использование всех различных классов символов) и уникальностью [4; 5]. Каждый сервис должен быть защищен уникальным паролем [2]. Для управления множеством уникальных паролей рекомендуется использование менеджеров паролей – специализированных систем, которые обеспечивают безопасное хранение и автоматическую подстановку данных, что снимает лишнюю нагрузку на пользователя и ускоряет процесс работы [2; 6].

Несмотря на то, какой бы надежный не был бы пароль – он не гарантирует абсолютною безопасность, именно поэтому следует ввести еще один независимый уровень проверки – многофакторную аутентификацию, основанную на комбинации факторов [2; 7]:

− что вы знаете – (пароль или логин);

− что у вас есть – (телефон или физический ключ);

− кто вы есть – (отпечаток или face ID).

Представим классификацию паролей по уровню безопасности.

Наименее безопасный – смс-коды, уязвимые к атакам.

Более безопасный – приложения аутентификаторы (Google Authenticator, Microsoft Authenticator), генерирующие одноразовые коды. Для доступа не требуется интернет, что делает этот способ менее опасней.

Самый надежный – аппаратные ключи безопасности. Этот метод устойчив к фишингу и перехвату кодов, что делает его самым безопасным [6; 7].

По мере роста технической защищенности систем, злоумышленники все чаще используют методы социальной инженерии [1]. Мошенникам проще обмануть доверчивого человека. Атаки варьируются от массового фишинга до целенаправленного таргетированного фишинга (определенная цель) и вишинга (метод социальной инженерии, связанный с телефонными звонками), где преступник умело маскируется под доверенное лицо, используя информацию из открытых источников.

Для противодействия мошенническим действиям можно предложить ряд мер. Среди них:

− проверка неожиданных запросов через альтернативные каналы связи для подтверждения той или иной просьбы;

− осведомленность о современных возможностях технологий, таких как подделки голоса или видео, при помощи искусственного интеллекта, а также знание о современных способах обмана;

− использование контекстных вопросов, которые может знать только известный вам собеседник [1; 2].

Безопасность данных зависит не только от надежного пароля и многофакторного аутентификатора, но и от состояния устройства и сети [4; 5].

Для устранения уязвимостей, которые активно используют мошенники в корыстных целях, необходимо регулярное обеспечение операционной системы и приложений. Своевременные обновления защитят технику от подобных методов мошенничества, что позволит справиться с трансформирующимися информационными и технологическими вызовами [2; 8; 9].

Для обеспечения безопасности необходимо использование встроенных или сторонних решений с активной и надежной защитой в реальном времени [5].

Для домашних сетей обязательным условием является использование стойких стандартов шифрования (WPA2/WPA3) на маршрутизаторе с надежным паролем доступа. Устаревшие стандарты, такие как (WEP) считаются полностью небезопасными [5]. Публичные Wi-Fi сети следует рассматривать как потенциально враждебную среду, так как к ней способен подключиться злоумышленник, который может перехватить трафик. Использование публичных интернет-сетей требует обязательного применения VPN для шифрования трафика от мошенников [6].

Для обеспечения отказоустойчивости и защиты от потери данных вследствие сбоя устройства, программ-вымогателей или физического повреждения – рекомендуется внедрение стратегии 3–2–1 резервного копирования [2; 5]: 3 копии данных (основная и две резервные); 2 различных типа носителей (флешка, жесткий диск, облачное хранение); 1 копия должна хранится удаленно для предотвращения потери всех данных.

Внедрение практик цифровой гигиены, требующих последовательности и постоянства определенных действий, обеспечат надежную безопасность в современном мире [2; 3]. Рекомендации постепенного, но системного подхода, начинаются с внедрения менеджера паролей и замены ключевых паролей на более универсальные и современные, активации многофакторной аутентификации для основных сервисов и настройки автоматического резервного копирования. В эпоху активного технологического прогресса, киберграмотность – это обязательный компонент личной и профессиональной ответственности в цифровом мире [4; 7].

Список литературы

1. Гордин А.И. Безопасное информационное поведение человека: учеб. пособие для СПО / А.И. Гордин, О.В. Гордина. – СПб.: Лань, 2025. – 260 с.

2. Ашманов И.С. Цифровая гигиена / И.С. Ашманов, Н.И. Касперская. – СПб.: Питер, 2024. – 400 с.

3. Еремин А.Л. Информационная и цифровая гигиена: учеб. пособие для вузов / А.Л. Еремин. – М.: Лань, 2023. – 92 с.

4. Баланов А.Н. Кибербезопасность: учеб. пособие для вузов / А.Н. Баланов. – СПб.: Лань, 2025. – 680 с.

5. Краковский Ю.М. Методы и средства защиты информации: учеб. пособие для вузов / Ю.М. Краковский. – СПб.: Лань, 2024. – 272 с. EDN SWECXC

6. Баланов А.Н. Комплексная информационная безопасность: учеб. пособие для вузов / А.Н. Баланов. – СПб.: Лань, 2024. – 400 с.

7. Баланов А.Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А.Н. Баланов. – СПб.: Лань, 2025. – 280 с.

8. Российские ответы на технологические вызовы: стратегии и решения в условиях современного менеджмента / О.В. Терещенко, Д.В. Еськов, С.А. Шульга [и др.] // Естественно-гуманитарные исследования. – 2025. – №4(60). – С. 842–847. EDN PFQHPU

9. Российские информационные вызовы и ответы на них / Г.В. Арустамян, Д.О. Шестак, Р.А. Дилбандян [и др.] // Культура Мира. – 2025. – Т. 13. №47(4). – С. 181–195. EDN IKDNZR