

УДК 004.056.5

DOI 10.5281/zenodo.17647946

Милушев Э. Х., Киселева В. С., Багиева С. С.

Милушев Эдуард Ханифович, кандидат технических наук, доцент, Воронежский государственный технический университет, д. 84, ул. 20-летия Октября, Воронеж, Россия, 394006. E-mail: vika.kiseleva05@mail.ru.

Киселева Виктория Сергеевна, Воронежский государственный технический университет, д. 84, ул. 20-летия Октября, Воронеж, Россия, 394006. E-mail: vika.kiseleva05@mail.ru.

Багиева Светлана Сергеевна, Воронежский государственный технический университет, д. 84, ул. 20-летия Октября, Воронеж, Россия, 394006. E-mail: vika.kiseleva05@mail.ru.

Методы и технологии цифровой гигиены для защиты персональных данных пользователей

Аннотация. В статье рассматривается проблема цифровой гигиены как ключевого элемента информационной безопасности личности. В условиях роста киберпреступности и увеличения числа мошеннических схем особую актуальность приобретают правила безопасного поведения в цифровой среде. Методология данного исследования, основанная на анализе научной литературы, позволяет раскрыть основные направления цифровой гигиены: защита персональных данных, формирование устойчивых привычек работы с информацией, осторожное поведение в социальных сетях и профилактика интернет-зависимости у подростков. Подчеркивается, что цифровая гигиена имеет междисциплинарный характер, охватывает технические, правовые, социальные и этические аспекты и требует комплексного внедрения в образовательную и общественную практику. Сделан вывод о том, что цифровая гигиена выступает не только индивидуальным средством защиты, но и важным элементом национальной кибербезопасности.

Ключевые слова: цифровая гигиена, персональные данные, киберпреступность, информационная безопасность, социальная инженерия, кибербуллинг, интернет-зависимость.

Milushev E. H., Kiseleva V. S., Bagieva S. S.

Milushev Eduard Khanifovich, Candidate of Technical Sciences, Associate Professor, Voronezh State Technical University, 84, 20th Anniversary of October str., Voronezh, Russia, 394006. E-mail: vika.kiseleva05@mail.ru.

Kiseleva Victoria Sergeevna, Voronezh State Technical University, 84, 20th Anniversary of October str., Voronezh, Russia, 394006. E-mail: vika.kiseleva05@mail.ru.

Bagieva Svetlana Sergeevna, Voronezh State Technical University, 84, 20th Anniversary of October str., Voronezh, Russia, 394006. E-mail: vika.kiseleva05@mail.ru.

Digital hygiene methods and technologies to protect users' personal data

Abstract. The article examines the problem of digital hygiene as a key element of personal information security. With the growth of cybercrime and the increasing number of fraudulent

schemes, the rules of safe behavior in the digital environment have become highly relevant. The methodology of this study, based on the analysis of scientific literature, allows us to reveal the main directions of digital hygiene: personal data protection, the formation of sustainable information management habits, cautious behavior in social networks, and the prevention of Internet addiction among adolescents. It is emphasized that digital hygiene has an interdisciplinary nature, covering technical, legal, social, and ethical aspects, and requires comprehensive implementation in educational and social practices. It is concluded that digital hygiene serves not only as an individual protection tool but also as an important element of national cybersecurity.

Key words: digital hygiene, personal data, cybercrime, information security, social engineering, cyberbullying, internet addiction.

Современное общество все глубже погружается в цифровую среду, где информационные технологии становятся неотъемлемой частью повседневной жизни. Виртуальное пространство предоставляет огромные возможности для обучения, работы и общения, но одновременно несет в себе новые риски. На первый план выходит проблема защиты персональных данных, так как именно они являются основной целью мошенников и киберпреступников [6].

Понятие цифровой гигиены обозначает комплекс правил и привычек, позволяющих минимизировать угрозы при использовании информационно-коммуникационных технологий. Если ранее акцент делался на технических аспектах киберзащиты, то сегодня особое значение приобретает человеческий фактор: осведомленность пользователя и его готовность соблюдать базовые меры предосторожности [2].

Исследователи отмечают, что соблюдение цифровой гигиены становится не только индивидуальной обязанностью, но и важной социальной практикой. Нарушение элементарных правил — использование слабых паролей, передача личной информации третьим лицам, неосторожное поведение в социальных сетях — повышает риск стать жертвой мошенников. При этом меры профилактики оказываются наиболее эффективными именно тогда, когда они интегрированы в образовательные процессы и сопровождаются формированием цифровой культуры среди разных возрастных групп.

В условиях роста числа киберугроз цифровая гигиена выступает ключевым

инструментом защиты личности. Она охватывает не только технические навыки, но и правовую, психологическую и этическую составляющие. Особое внимание уделяется защите детей и подростков, наиболее уязвимых перед деструктивными воздействиями в сети. Таким образом, цифровая гигиена становится основой личной безопасности в информационном пространстве и важным элементом национальной киберзащиты.

Цифровая гигиена представляет собой набор правил и привычек, направленных на обеспечение информационной безопасности личности. Наиболее частыми мишенями для киберпреступников становятся персональные данные пользователей, которые позволяют получить доступ к банковским счетам, социальным сетям и другим ресурсам. В этой связи одной из важнейших мер является создание сложных паролей, их регулярное обновление и использование разных комбинаций для отдельных сервисов [6]. Обзор литературных данных показывает, что злоумышленники часто используют социальную инженерию, то есть психологические методы воздействия на пользователей для получения секретной информации.

Особое значение приобретает формирование устойчивых привычек безопасного поведения в сети. К ним относится осторожное обращение с электронной почтой и ссылками, отказ от хранения копий документов в облачных сервисах, регулярное резервное копирование данных и обновление программного обеспечения. Многие пользователи пренебрегают этими рекомендациями, что

делает их уязвимыми для вирусных вымогателей и фишинговых атак. Подавляющее большинство киберугроз (более 99 %) реализуются вследствие ошибок пользователей, а не технических уязвимостей, о чем свидетельствуют данные ряда исследований [3; 6]. Данная статистика подтверждает решающую роль человеческого фактора в цифровой безопасности.

В последние годы киберпреступность сохраняет тенденцию к росту. Экономический ущерб от атак в цифровой среде превышает убытки от традиционных видов преступлений. Несмотря на развитие правовой базы, данные официальной статистики показывают, что раскрываемость подобных дел остается низкой, а вероятность наказания киберпреступников невелика [10]. Вследствие этого ключевая роль отводится профилактике, где цифровая гигиена выступает основным средством защиты. Граждане должны быть готовы самостоятельно заботиться о своей кибербезопасности, поскольку государственные механизмы реагирования не всегда эффективны. Подобная позиция разделяется и в научной среде, где цифровая гигиена рассматривается как элемент индивидуальной ответственности [4; 6].

Не менее важным направлением является формирование цифровой культуры в образовательной среде. Учебные заведения все чаще сталкиваются с необходимостью обучения школьников и студентов безопасному поведению в интернете. В этой связи предлагаются методики, включающие использование образовательных платформ, интерактивных заданий и специальных курсов, где акцент делается не только на технических, но и на этических аспектах цифровой безопасности. Отмечается, что в образовательной среде цифровая гигиена должна формироваться комплексно: от правил работы с учебными материалами до осознанного отношения к цифровому следу [1; 8].

Наряду с традиционными мерами цифровой гигиены, в научной среде активно обсуждаются новые методы защиты персональных данных. Одним из перспективных направлений является адаптивная аутентификация с сохранением приватности. В отличие от классических схем, где используются пароли или двухфакторные проверки, адаптивные системы анализируют контекст входа в аккаунт — устройство, местоположение, поведение пользователя — и динамически выбирают уровень проверки. Это позволяет снизить вероятность взлома, сохраняя удобство для добросовестного пользователя.

Особенностью современных разработок является применение технологий дифференциальной приватности и анонимных токенов. Они позволяют собирать необходимые данные о поведении пользователей для оценки рисков, но при этом исключают возможность прямой идентификации личности. В результате формируется баланс между эффективностью защиты и соблюдением конфиденциальности.

Научные разработки в области адаптивной аутентификации, представленные в работах [7; 9], демонстрируют ее актуальность для финансового сектора, государственных сервисов и образовательных платформ, где ценность персональных данных чрезвычайно высока. Несмотря на то, что подобные технологии пока не получили широкого распространения, они могут стать основой для развития цифровой гигиены нового поколения и значительно повысить устойчивость общества к мошенническим схемам.

Особого внимания требует защита детей и подростков. В юном возрасте они особенно уязвимы перед кибербуллингом, онлайн-грумингом и интернет-зависимостью. Эти явления не только подрывают психологическое здоровье подростков, но и создают угрозу их безопасности. Среди мер профилактики исследователи выделяют ограничение времени пребывания в сети, обучение пра-

вилам общения в социальных сетях и контроль со стороны родителей и педагогов [1; 5]. Важным элементом становится открытое взаимодействие между взрослыми и подростками, что позволяет своевременно выявить признаки деструктивного влияния.

Кроме того, цифровая гигиена включает и вопросы этики в цифровом пространстве. Как подчеркивают специалисты, формирование ответственного поведения в интернете — это не только защита персональных данных, но и соблюдение норм цифрового этикета, уважение к

информации и другим пользователям. Проблема усугубляется отсутствием единой научно обоснованной теории цифровой безопасности, что затрудняет формирование целостного подхода к воспитанию цифровой культуры [1].

Для минимизации рисков в цифровой среде необходимо придерживаться базовых правил безопасности. Сформулированные принципы цифровой гигиены, обобщенные в таблице 1, позволяют наглядно структурировать потенциальные угрозы и методы противодействия им.

Таблица 1. Основные правила цифровой гигиены

Направление	Рекомендации	Возможные угрозы при нарушении
Пароли и аутентификация	Использование сложных комбинаций, двухфакторная аутентификация	Кража аккаунтов, доступ к персональным данным
Работа с информацией	Резервное копирование, обновление ПО, осторожность при открытии ссылок	Вирусы-вымогатели, фишинг, утечка данных
Социальные сети	Ограничение публикации личной информации, настройка приватности	Социальная инженерия, мошенничество, кибербуллинг
Подростки и дети	Родительский контроль, обучение безопасному поведению, ограничение времени онлайн	Интернет-зависимость, груминг, манипуляции сознанием

В результате анализа становится очевидно, что цифровая гигиена охватывает технические, правовые, социальные и этические аспекты. Она играет роль не только в защите персональных данных, но и в формировании общей культуры поведения в цифровом пространстве. Таким образом, проблема цифровой гигиены выходит за рамки индивидуальной практики и приобретает общественное и государственное значение [5; 8].

Проведенное исследование позволяет определить цифровую гигиену как комплексную систему защиты персональных данных, эффективность которой обусловлена синтезом индивидуальных, образовательных и технологических мер.

На индивидуальном уровне безопасность обеспечивается за счет строгого соблюдения технических правил, таких как использование менеджеров паролей и

двухфакторной аутентификации, а также за счет формирования у пользователя критической компетенции, позволяющей противостоять фишингу и социальной инженерии.

Ключевую роль в профилактике играет образовательная среда, где интеграция модулей по цифровой гигиене, нацеленных на воспитание ответственного отношения к цифровому следу и этике взаимодействия, становится основой для снижения уязвимости пользователей, особенно подростков, к кибербуллингу и грумингу.

Одновременно с этим перспективным направлением развития является внедрение адаптивных систем аутентификации, анализирующих контекст поведения пользователя и минимизирующих зависимость безопасности от человеческого фактора.

Таким образом, защита от мошенничества достигается не разрозненными действиями, а через формирование целостной системы, в которой осознанное поведение пользователя, системное обра-

зование и перспективные технологии взаимно дополняют друг друга, превращая цифровую гигиену в фундамент личной и национальной киберустойчивости.

СПИСОК ЛИТЕРАТУРЫ

1. Воронов А. А. Защита персональных данных в цифровой среде: правовые и организационные аспекты. Москва: Проспект, 2021. 256 с.
2. Гаврилов К. В., Новикова Е. А. Цифровая гигиена как элемент системы кибербезопасности // Вопросы кибербезопасности. 2023. № 2 (48). С. 45–53.
3. Гусев В. А. Цифровая гигиена vs. киберпреступность // Психопедагогика в правоохранительных органах. 2022. Т. 27, № 1(88). С. 102–108. DOI 10.24412/1999-6241-2022-188-102-108.
4. Жигалова Е. Н. Формирование цифровой гигиены у школьников // Педагогика. 2023. № 1. С. 45–52.
5. Козырев С. Б. Сравнительный анализ методов криптографической защиты персональных данных в распределенных системах // Вопросы кибербезопасности. 2022. № 3 (45). С. 34–42.
6. Лукашин Ю. П. Цифровая гигиена как элемент информационной культуры личности // Информатизация образования и науки. 2021. № 2 (50). С. 58–65.
7. Надейкина В.С., Лагуткина Т.В. Анализ способов реализации системы многофакторной аутентификации // Научный результат. Информационные технологии. 2022. Вып. 7. № 4. С. 59–66.
8. Петрова Е. В. Формирование цифровой культуры студентов в условиях современных киберугроз // Высшее образование в России. 2023. № 1. С. 112–125.
9. Саломатин А.А., Исхаков А.Ю. Применение интегрированного показателя отпечатков браузера в задаче адаптивной аутентификации субъектов доступа // Информационные и математические технологии в науке и управлении. 2020. № 4 (20). С. 84–92.
10. Черепанова М. Ю. К вопросу о цифровой гигиене, рисках и вызовах цифрового мира // Цифровое воспитание: реалии и перспективы: Сборник материалов Международной научно-практической конференции, Москва, 15 сентября 2022 года. Москва: Негосударственное образовательное частное учреждение высшего образования «Московский институт психоанализа», 2022. С. 466–472.

REFERENCES (TRANSLITERATED)

1. Voronov A. A. Zashhita personal'nyh dannyh v cifrovoj srede: pravovye i organizacionnyye aspekty. Moskva: Prospekt, 2021. 256 s.
2. Gavrilov K. V., Novikova E. A. Cifrovaja gigiena kak jelement sistemy kiberbezopasnosti // Voprosy kiberbezopasnosti. 2023. № 2 (48). S. 45–53.
3. Gusev V. A. Cifrovaja gigiena vs. kiberprestupnost' // Psihopedagogika v pravoohranitel'nyh organah. 2022. T. 27, № 1(88). S. 102–108. DOI 10.24412/1999-6241-2022-188-102-108.
4. Zhigalova E. N. Formirovanie cifrovoj gigieny u shkol'nikov // Pedagogika. 2023. № 1. S. 45–52.
5. Kozyrev S. B. Sravnitel'nyj analiz metodov kriptograficheskoy zashhity personal'nyh dannyh v raspredelennyh sistemah // Voprosy kiberbezopasnosti. 2022. № 3 (45). S. 34–42.
6. Lukashin Ju. P. Cifrovaja gigiena kak jelement informacionnoj kul'tury lichnosti // Informatizacija obrazovaniya i nauki. 2021. № 2 (50). S. 58–65.
7. Nadejkina V.S., Lagutkina T.V. Analiz sposobov realizacii sistemy mnogofaktornoj autentifikacii // Nauchnyj rezul'tat. Informacionnye tehnologii. 2022. Vyp. 7. № 4. S. 59–66.
8. Petrova E. V. Formirovanie cifrovoj kul'tury studentov v uslovijah sovremennyh kiberugroz // Vysshee obrazovanie v Rossii. 2023. № 1. S. 112–125.
9. Salomatina A.A., Ishakov A.Ju. Primenenie integrirovannogo pokazatelja otpechatkov brauzera v zadache adaptivnoj autentifikacii sub#ektov dostupa // Informacionnye i matematicheskie tehnologii v nauke i upravlenii. 2020. № 4 (20). S. 84–92.

10. Cherepanova M. Ju. K voprosu o cifrovoj gigiene, riskah i vyzovah cifrovogo mira // Cifrovoe vospitanie: realii i perspektivy: Sbornik materialov Mezhdunarodnoj nauchno-prakticheskoy konferencii, Moskva, 15 sentjabrja 2022 goda. Moskva: Negosudarstvennoe obrazovatel'noe chastnoe uchrezhdenie vysshego obrazovanija «Moskovskij institut psihoanaliza», 2022. S. 466–472.

Поступила в редакцию: 03.10.2025.

Принята в печать: 21.11.2025.
