Кроква Кирилл Александрович
студент
Чумаков Алексей Александрович
студент
Научный руководитель
Терещенко Олеся Валерьевна
канд. филос. наук, доцент

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

БЕЗОПАСНОСТЬ ЛИЧНЫХ ДАННЫХ В ИНТЕРНЕТЕ: АКТУАЛЬНЫЕ УГРОЗЫ И СТРАТЕГИИ ЗАЩИТЫ

***Аннотация**: в статье рассматривается актуальная проблема обеспечения безопасности персональных данных в сети Интернет. Проводится анализ основных видов угроз, с которыми сталкивается пользователь, включая действия злоумышленников, риски, связанные с деятельностью компаний, и человеческий фактор. Особое внимание уделяется правовым аспектам защиты информации в Российской Федерации и на международной арене. В работе предложен комплекс практических мер и рекомендаций, направленных на минимизацию рисков утечки и несанкционированного использования личной информации. Статья подчеркивает важность формирования осознанного подхода к цифровой гигиене как неотъемлемого компонента современного образования.*

***Ключевые слова**: кибербезопасность, персональные данные, цифровая гигиена, фишинг, двухфакторная аутентификация, конфиденциальность, GDPR, киберугрозы.*

Современная реальность характеризуется тотальной цифровизацией и интеграцией интернет-пространства во все сферы жизни человека. От социальных взаимодействий и развлечений до профессиональной деятельности и финансо-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

вых операций – каждый шаг сопровождается генерацией и передачей огромных массивов личных данных. Под этим понятием подразумевается любая информация, относящаяся к прямо или косвенно определенному лицу: от фамилии, имени и отчества, контактных данных и геолокации до более чувствительных сведений, таких как биометрия, финансовые операции, история болезней и переписка. Однако колоссальные преимущества и удобства цифровой эпохи омрачаются стремительным ростом угроз, связанных с нарушением конфиденциальности и злонамеренным использованием этой информации. В связи с этим вопрос безопасности личных данных трансформировался из сугубо технической задачи в острую социально-значимую проблему, требующую от пользователя не только базовой грамотности, но и осознанной, активной позиции [1; 2].

Многообразие угроз информационной безопасности можно классифицировать по их источнику и характеру.

1. Угрозы со стороны физических лиц (киберпреступления). Существуют различные способы их совершения. Среди них можно выделить следующие:

− фишинг и социальная инженерия – это действия, направленные на манипулирование пользователем с целью получения конфиденциальных данных. Жертве посредством электронной почты, смс или сообщений в мессенджерах направляются поддельные уведомления от банков, государственных органов или популярных сервисов, побуждающие ввести учетные данные на фальшивых сайтах или перевести деньги;

− вредоносное программное обеспечение – вирусы, трояны, шпионское программное обеспечение (spyware), программы-вымогатели. Они могут проникать на устройства через небезопасные вложения, взломанные сайты или пиратское программное обеспечение с целью кражи данных, шифрования файлов для последующего выкупа или скрытого мониторинга действий пользователя;

− массированные кибератаки на серверы крупных компаний и государственных учреждений, приводящие к утечке баз данных, содержащих миллионы записей с персональной информацией пользователей [3; 4].

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

2. Угрозы, связанные с деятельностью компаний и сервисов:

− сбор и коммерческое использование персональных данных. Многие онлайн-платформы и мобильные приложения собирают информацию о пользователях в объемах, превышающих необходимые для предоставления услуги, которые в последующем используются для построения поведенческого профиля, таргетированной рекламы и могут передаваться третьим лицам, часто без явного и информированного согласия пользователя;

− недостаточный уровень защищенности сервисов – некоторые компании экономят на внедрении современных систем безопасности. Это делает их легкой мишенью для хакеров и приводит к утечкам по вине самой организации [5].

3. Угрозы, связанные с человеческим фактором:

− низкая цифровая грамотность (использование простых и повторяющихся паролей, пренебрежение обновлением программного обеспечения, публикация избыточной личной информации в открытом доступе (особенно в социальных сетях);

− неосознанное согласие на обработку данных (привычка бездумно принимать пользовательские соглашения, не вникая в их содержание);

− использование небезопасных каналов связи (например, совершение финансовых операций или передача конфиденциальных данных при подключении к публичным сетям Wi-Fi без использования дополнительных средств защиты).

Защита личных данных является не только технической, но и правовой категорией.

В Российской Федерации основным нормативным актом в нормотворческой области является Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». Он устанавливает требования к операторам, обрабатывающим персональные данные граждан РФ, включая обязанность обеспечивать их конфиденциальность и безопасность, получать согласие субъекта на обработку, а также предоставлять субъекту права на доступ, уточнение, блокирование и уничтожение своей информации [6].

На международном уровне эталоном считается Регламент Европейского союза General Data Protection Regulation (GDPR), который установил жесткие

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

стандарты в области защиты данных и ввел значительные штрафные санкции за их нарушение. Его принципы, такие как «право на забвение», минимальный объем данных и подотчетность, оказывают влияние на глобальную практику [7–9].

Знание своих прав, закрепленных этими документами, позволяет пользователю на законных основаниях требовать от компаний отчета о том, какие его данные и с какой целью собираются и обрабатываются.

Эффективная защита строится на многоуровневом подходе и соблюдении правил цифровой гигиены.

К ним, прежде всего, относится аутентификация (использование сложных паролей, состоящих из комбинации букв (заглавных и строчных), цифр и специальных символов. Для генерации и безопасного хранения паролей рекомендуется использовать такие менеджеры паролей, как KeePass и Bitwarden.

Двухфакторная аутентификация (2FA) предполагает для обеспечения доступа к аккаунту, помимо пароля, применять одноразовый код из смс, мобильного приложения-аутентификатора (Google Authenticator, Microsoft Authenticator) или физический ключ безопасности [10].

Защита программно-аппаратного комплекса заключается в использовании лицензионного антивирусного программного обеспечения с регулярным обновлением баз данных.

Также необходимо для обеспечения информационной безопасности устанавливать последние версии операционных систем, браузеров и приложений, так как обновления часто содержат исправления критических уязвимостей.

Следует отказаться от передачи конфиденциальной информации через открытые сети Wi-Fi в кафе, аэропортах, гостиницах. Для шифрования интернет-трафика рекомендуется использовать надежный VPN-сервис [10].

Регулярное создание резервных копий важных данных на внешних носителях или в облачных хранилищах обеспечит защиту информации от потери в случае заражения ransomware или выхода устройства из строя.

Осознанное поведение в цифровой среде требует критического мышления, проверки адресов отправителей и ссылок перед переходом.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Необходимо контролировать цифровые следы, проводить аудит настроек приватности в социальных сетях, ограничивать круг лиц, способных видеть личную информацию и список контактов. Не рекомендуется также размещать в открытом доступе сведения о месте жительства, графике отпусков, сканы документов.

При установке нового приложения на смартфон следует внимательно изучать, к каким функциям и данным оно запрашивает доступ, и отзывать ненужные разрешения.

На государственном уровне существуют специальные инициативы и программы. Среди них можно выделить национальные центры кибербезопасности, которые осуществляют координацию действий по защите информационной инфраструктуры.

Программы повышения цифровой грамотности населения способствуют получению навыков и умений по основам кибербезопасности.

Государство также осуществляет субсидирование разработки отечественных решений в области информационной безопасности [9].

На международном уровне заключаются соглашения о взаимной правовой помощи в расследовании киберпреступлений [11]; происходит гармонизация стандартов защиты данных в разных юрисдикциях [7]; формируются трансграничные механизмы контроля за соблюдением законодательства о защите данных [12].

В будущем могут возникнуть вызовы и связанные с ними риски в области квантовых вычислений (угроза современным методам шифрования); в сфере нейроинтерфейсов (вызовы в части защиты данных о мозговой активности); а в зоне дополненной реальности (AR) (риски сбора биометрических и поведенческих данных). Все указанные явления связаны с всемирным процессом глобализации и обеспечением в этих условиях устойчивого социального порядка [1].

Таким образом, в условиях роста числа киберугроз безопасность личных данных перестает быть задачей, которую можно полностью переложить на технических специалистов или законодателей. Она становится зоной личной ответственности каждого активного пользователя сети. Формирование культуры кибербезопасности, основанной на постоянном обучении, критическом воспри-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ятии информации и неукоснительном соблюдении правил цифровой гигиены, является важной составляющей современности. Студенческое сообщество, являясь наиболее продвинутой в техническом отношении частью общества, должно играть ключевую роль в продвижении этих принципов, транслируя их из узкопрофессиональной сферы в широкий общественный дискурс. Инвестиция времени и усилий в собственную цифровую безопасность сегодня – это не просто профилактика рисков, а вклад в сохранение фундаментальных прав на приватность и автономию в цифровом будущем.

Список литературы

1. Терещенко О.В. Беспорядок и преступность как одно из последствий всемирного процесса глобализации / О.В. Терещенко // Национальное здоровье. – 2016. – №1-2. – С. 191–199. EDN YHRNRV

2. 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

3. Соколов И.А. Актуальные угрозы информационной безопасности в условиях цифровой трансформации / И.А. Соколов, Т.К. Петрова // Вопросы кибербезопасности. – 2023. – №2(45). – С. 15–25.

4. 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

5. Шнайер Б. Данные и Голиаф: Скрытые сражения за сбор ваших данных и контроль над вашим миром / Б. Шнайер. – Нью-Йорк: W.W. Norton, 2015. – 320 с.

6. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ [Электронный ресурс]. – Режим доступа: https://base.garant.ru (дата обращения: 26.11.2025).

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

7. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71936226 (дата обращения: 26.11.2025).

8. Геворкян Л.А. Правовые механизмы защиты персональных данных: опыт России и ЕС / Л.А. Геворкян [Электронный ресурс]. – Режим доступа: https://www.hse.ru/ba/epa/students/diplomas/1052911202 (дата обращения: 26.11.2025).

9. Параскевов А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, Ю.А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2015. – №110. – С. 866–894. EDN UHSFJP

10. Ашманов И. Цифровая гигиена / И. Ашманов, Н. Касперская. – СПб.: Питер, 2025. – 400 с.

11. Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 26.11.2025).

12. Исмагилова О. Мировой опыт регулирования защиты, передачи и хранения данных / О. Исмагилова, К. Хаджи // Экономическая политика. – 2020. – Т. 15. № 3. – С. 152–175. DOI 10.18288/1994-5124-2020-3-152-175. EDN OBPGOR

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)