DOI 10.35775/PSI.2024.112.12.013
УДК 316.334

С.С. МОРОЗОВА
доцент кафедры российской политики
Санкт-Петербургского государственного университета,
Россия, г. Санкт- Петербург
E-mail: s.s.morozova@spbu.ru

А.Г. ДЕДУЛЬ
преподаватель факультета политологии
Санкт-Петербургского государственного университета,
Россия, г. Санкт- Петербург
E-mail: anastasia.dedul@gmail.com
ORCID 0009-0004-7813-1534

И.А. БУЛАТОВ
магистрант Санкт-Петербургского
государственного университета,
Россия, г. Санкт- Петербург
E-mail: bulatov.iwan2011@yandex.ru

ПРОБЛЕМЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ В КОНТЕКСТЕ БЕЗОПАСНОСТИ ЦИФРОВОГО ГРАЖДАНСКОГО УЧАСТИЯ[1]

Цифровизация общественной жизни привела к трансформации традиционных форм гражданского участия, открывая новые возможности для взаимодействия граждан с государственными институтами. Однако развитие цифрового гражданского участия сопровождается вызовами, связанными с обеспечением безопасности и конфиденциальности данных пользователей. В статье анализируются ключевые проблемы в данной области, включая кибератаки, утечки данных и вопросы конфиденциальности, а также предлагаются рекомендации для их минимизации. Особое внимание уделено правовым, техническим и образовательным аспектам защиты данных. Представленные выводы и рекомендации направлены на повышение уровня защищенности данных и доверия граждан к цифровым платформам.

Ключевые слова: *цифровое гражданское участие, безопасность данных, конфиденциальность, цифровизация, киберугрозы, защита информации, цифровая грамотность.*

[1] Благодарности: Статья выполнена в рамках научно-исследовательского проекта при поддержке РНФ 22-78-10049 «Государство и гражданин в условиях новой цифровой реальности».

Введение. В цифровую эпоху актуальность вопросов, связанных с защитой личной информации и персональных данных, размещаемых в Интернете, продолжает расти. Все чаще появляются сообщения о случаях утечки данных, продаже биометрической информации пользователей в даркнете, а также о взломах систем, что иногда приводит к краже данных и денег пользователей. Например, исследование Европейского агентства по кибербезопасности показывает [10. С. 154-166; 16. P. 1200], что число случаев утечки информации увеличилось на 55% за последние пять лет.

Проблема утечки данных создает серьезные угрозы безопасности гражданского участия и конфиденциальности информации в цифровом пространстве. Это особенно важно в условиях увеличения использования электронных платформ для взаимодействия с государственными учреждениями и участия в общественно-политической жизни. Исследования Международного союза электросвязи подчеркивают [9; 15; 13], что доверие граждан к таким платформам является важнейшим фактором их успешной работы.

Данная статья посвящена рассмотрению этих вызовов и разработке рекомендаций по улучшению защиты персональных данных и обеспечения конфиденциальности в цифровом пространстве. Для этого важно изучить ключевые аспекты безопасности и конфиденциальности, а также оценить международные методы, направленные на минимизацию потенциального ущерба от вышеперечисленных проблем, что в конечном итоге должно помочь в их решении.

Защита цифрового гражданского участия является важным условием для формирования доверия граждан к электронным платформам. В этом контексте безопасность включает в себя защиту данных пользователей от утечек, предотвращение кибератак и обеспеченность доступа к сервисам.

Отметим, что не существует универсального термина для определения понятия «безопасность». В Стратегии национальной безопасности Российской Федерации, принятой в 2021 году, национальная безопасность описывается как защита национальных интересов от внешних и внутренних угроз [12]. В этом документе используются такие термины, как «защищенность», «охрана», «независимость» и другие. Хотя стратегия касается безопасности в контексте государства и его суверенитета, ее можно использовать как основу для изучения концепции безопасности.

Стоит также упомянуть, что одним из стратегических приоритетов Российской Федерации в рамках этой стратегии является информационная безопасность. Укрепление информационного суверенитета России является важной целью данного документа. Информационная безопасность рассматривается как существенно важный аспект государственной независимости и защиты интересов народа. Тем не менее, четкое определение термина «информационная безопасность» в стратегии не представлено. Это связано с недостаточной конкретизацией формулировок, несмотря на значительное внимание к ним в контексте национальной безопасности.

Еще одним важным нормативным актом является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 года № 646 [13]. В этом документе информационная безопасность определяется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз...». В этом определении акцентируется внимание на понятии «информационная угроза», которое раскрывается как «совокупность действий и факторов, представляющих опасность для национальных интересов в области информации».

Кроме того, в Законе Российской Федерации от 5 марта 1992 года № 2446-1 «О безопасности» указаны следующие определения безопасности и жизненно важных интересов [3]. Первое понятие трактуется как состояние защитности жизненно важных интересов субъекта правоотношений от внешних и внутренних факторов. Второе определяется как совокупность потребностей, удовлетворение которых создает условия для успешного развития данного субъекта.

Эти определения акцентируют внимание на «состоянии защищенности», что является основным элементом концепции безопасности. Тем не менее, как отмечается в научной литературе, «состояние защищенности» не совпадает с понятием безопасности, а представляет собой один из его основных характеристик. Под состоянием защищенности понимается оптимальное психологическое состояние субъекта, сохраняемое даже в условиях воздействия различных факторов [4. С. 59-60; 6. С. 646-649; 7].

Исследователи уделяют внимание такому понятию, как информационно-психологическая безопасность личности. Этот термин охватывает состояние защищенности как сознательной, так и бессознательной психики от негативных психологических воздействий, а также от информационного вреда, который может угрожать духовному, нравственному, интеллектуальному и физическому состоянию человека [2. С. 91-97]. Информационно-психологическая безопасность подразумевает защиту от угроз, таких как кража или несанкционированное использование личных данных. Важные проблемы, с которыми сталкиваются интернет-пользователи и которые оказывают неблагоприятное влияние на психику, включают в себя:

– нарушение прав на конфиденциальность и вторжение в личную жизнь;

– кража идентичности (взлом аккаунтов и представление себя под чужим именем);

– плагиат и нарушение авторских прав;

– опасности онлайн-общения (угрозы, оскорбления, шантаж и т.д.);

– умышленное распространение дезинформации (фейковые новости);

– рассылка спама и фишинговых сообщений;

– риски, связанные с удаленной работой;

– интернет-зависимость;

– повышение уровня стресса;

– манипуляции и воздействие на сознание пользователей (вовлечение в экстремистские и секты);

– виртуальные преступления;

– мошенничество в инвестиционной сфере.

Можно выделить три ключевых уровня организации психологической защиты человека и три направления ее разработки и функционирования:

– социальный уровень;

– социально-групповой уровень;

– индивидуально-личностный уровень.

На социальном уровне защита осуществляется через регулирование информационных потоков и внедрение методов обработки информации в процессе социальной активности. Субъектами на данном уровне являются государство и общественные институты.

На социально-групповом уровне защита реализуется через обмен внутригрупповыми информационными потоками и использование специальных методов взаимодействия, характерных для конкретных комитетов или организаций. Здесь субъектами выступают группы и организации.

На индивидуально-личностном уровне защита достигается благодаря созданию особых регулятивных систем и комплекса защитных механизмов, формирующих индивидуальную психологическую защиту.

Определение конфиденциальности информации приводится в Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [14]. Согласно этому акту, конфиденциальность информации предполагает, что получатель обязан не предоставлять доступ к полученным данным третьим лицам без согласия их владельца. Это определение закладывает основу для анализа конфиденциальности как ключевого элемента защиты персональных данных пользователей.

Цифровое гражданское участие представляет собой одну из форм активного гражданского участия, при которой используются информационно-коммуникационные технологии (ИКТ). Это может принимать различные формы взаимодействия граждан с [16; 20. P. 752]:

– правительством (C2G, citizen-to-government);

– обществом (C2S, citizen-to-society);

– бизнесом (C2B, citizen-to-business).

Таким образом, изучение законодательных определений безопасности и конфиденциальности позволяет выделить основные концепты, необходимые для анализа цифрового гражданского участия. Дальнейшее исследование сосредоточится на выявлении ключевых проблем и предложении рекомендаций для повышения уровня защиты данных и обеспечения конфиденциальности в цифровой среде.

Проблемы безопасности и конфиденциальности пользовательских данных тесно взаимосвязаны. При регистрации на электронных платформах

пользователи предоставляют определенную информацию о себе. Если платформа предназначена для госуслуг, пользователи должны идентифицировать себя с помощью уникальных данных, таких как ИНН, серия и номер паспорта, данные СНИЛС, телефон и т. д. При взаимодействии с обществом достаточно минимальной информации, например, имени и фамилии. На форумах или в социальных сетях пользователи могут регистрироваться под псевдонимами, хотя некоторые платформы требуют подтверждения через номер телефона или электронную почту.

Взаимодействие с бизнесом может потребовать предоставления различного объема данных: от имени и номера телефона для записи в салон красоты до паспортных данных и справки 2-НДФЛ при оформлении кредита. Независимо от контекста взаимодействия, пользователи надеются на защиту своих данных со стороны платформ. Часто они же становятся жертвами утечек или мошеннических схем, вызванных человеческой неосторожностью или недобросовестностью третьих лиц.

Взаимодействие граждан с бизнесом в области банковских услуг представляет собой важный аспект современной экономики. В настоящее время почти каждый россиянин пользуется интернет-банкингом, будь то через веб-сайт или мобильное приложение. Однако с развитием цифровых технологий возникает новая проблема – потеря денежных средств из-за действий вредоносных программ (вирусов) или фишинговых ссылок во время онлайн-оплат.

Исследования показывают, что ежегодно число граждан, ставших жертвами мошенников в банковской сфере, растет на сотни процентов, а общая сумма убытков достигает почти 350 миллионов рублей [8. С. 640-643]. Деятельность таких злоумышленников в интернете представляет серьезную угрозу для цифровой гражданской активности.

Одной из основных угроз являются сервисы, специализирующиеся на сборе данных о людях. В качестве примера можно привести телеграмм-бот «Глаз Бога», который предоставляет информацию за плату. Эти сервисы зачастую действуют в рамках законодательства, так как используют информацию, уже доступную в открытом доступе. Источники данных включают официальные реестры (такие как ГИБДД, ПФР, ФНС, Росреестр) и популярные интернет-ресурсы (например, «ВКонтакте») [1; 9; 15]. Проблема усугубляется постоянными утечками данных из крупных компаний, что создает условия для злоупотреблений.

Ключевые аспекты проблемы:

1. Юридическая неясность. Разработчики таких сервисов соблюдают закон на формальном уровне, так как работают с открытой информацией. Например, согласно Федеральному закону № 152-ФЗ «О персональных данных», обработка персональных данных допускается в предусмотренных законом случаях. Поскольку сервис собирает информацию из интернета, формально законодательство не нарушается. Однако вопрос о том, как именно личные данные стали доступными в открытом доступе, остается открытым.

2. Анонимность создателей. В большинстве случаев личности разработчиков остаются неизвестными, что затрудняет их привлечение к ответственности. Используемые в сети псевдонимы и никнеймы зачастую не соответствуют реальным данным и не дают информации о разработчиках.

3. Невнимательность пользователей. Часто пользователи размещают в открытом доступе информацию, которую могут использовать злоумышленники. К примеру, фотографии с геометкой, содержащие личные данные, могут стать источником угроз и преследования [19; 20].

Необходимость защиты данных в цифровую эпоху обусловлена возрастающей зависимостью общества от информационных технологий и растущим числом кибератак. Как заверяют исследователи [8; 11], развитие технологий привело к появлению более сложных методов компрометации данных, что делает традиционные способы защиты менее эффективными. На основании этого пользователям рекомендуется:

1. Создавать уникальные и сложные пароли. Применение уникальных паролей для разных аккаунтов снижает вероятность их одновременного взлома. Использование алгоритмов генерации паролей, включающих случайные комбинации букв, цифр и символов, усложняет подбор пароля (1).

2. Регулярно обновлять пароли. Частая смена паролей снижает риски, связанные с утечками данных. Исследования показывают, что обновление паролей хотя бы раз в три месяца уменьшает вероятность взлома на 40% [17. P. 1-15].

3. Избегать публикации личной информации. Размещение данных, таких как адреса, номера телефонов или геолокации, увеличивает риск целевых атак. Бурцев (2019) утверждает, что большая часть компрометации данных связана с их неосторожным размещением в социальных сетях.

4. Использовать антивирусное программное обеспечение. Современные антивирусы защищают от большинства угроз, включая фишинг и вредоносные программы. Согласно данным исследований лаборатории Касперского, 85% попыток взлома предотвращаются при установке комплексного антивируса (Касперский, 2022).

5. Удалять чувствительную информацию. Удаление переписок и документов, содержащих персональные данные, после их отправки снижает риски попадания информации в руки злоумышленников. Это особенно важно для финансовых и юридических документов.

6. Следить за новостями о взломах платформ. Если поступила информация об утечке данных на используемой платформе, рекомендуется немедленно сменить пароль и проанализировать возможные последствия утечки.

Эти меры направлены на минимизацию рисков утраты данных и снижение их доступности для злоумышленников. Как отмечают эксперты [10. С. 154-166; 13; 18. P. 320], защита данных является не только технической, но и социальной задачей, требующей повышения цифровой грамотности среди населения.

Заключение. Обеспечение цифровой безопасности и конфиденциальности требует внимательного отношения как со стороны пользователей, так и разработчиков платформ. Ужесточение законодательства, повышение осведомленности граждан и обновление технологий защиты данных могут существенно уменьшить риски. Достижение высокого уровня безопасности данных является необходимым условием для развития цифрового гражданского общества.

В эпоху цифровых технологий появляются новые вызовы, связанные с обеспечением защиты и конфиденциальности данных. Состояние психологического комфорта и безопасности людей зависит как от внешних, так и от внутренних факторов. Хотя как активные пользователи цифровых платформ, начиная от государственных сервисов и заканчивая социальными сетями, мы не всегда можем влиять на уровень защиты, который они предлагают, мы можем принять необходимые меры для охраны своих данных и создания уютного психологического пространства.

Отказ от использования цифровых технологий (цифровая инаковость) в современном обществе нерентабелен, так как большинство жизненно важных процессов уже переводится в цифровой формат. Важно понимать, что осознанное взаимодействие с цифровыми платформами и следование рекомендациям по защите данных являются важными условиями для снижения рисков.

Не следует освобождать разработчиков и операторов цифровых платформ от ответственности за их действия или бездействие в вопросах безопасности. Тем не менее, осознание пользователями своей ответственности за защиту личных данных – это первый шаг на пути к созданию безопасного цифрового пространства. Применение предложенных в данной статье рекомендаций позволит пользователям уменьшить риски утечки данных и повысить уровень защиты при участии в цифровом гражданском взаимодействии.

В конечном счете, защита данных – это не только техническая, но и социальная проблема, требующая совместных усилий государства, бизнеса и гражданского общества. Только благодаря взаимодействию всех заинтересованных сторон можно создать безопасное и доверительное цифровое пространство, где каждый пользователь будет чувствовать себя защищенным, а цифровое гражданское участие станет эффективным инструментом для общественного прогресса.

ПРИМЕЧАНИЯ:

(1) Сид-фраза – это уникальная последовательность случайно сгенерированных слов, которые представляют собой все приватные ключи, связанные с определенным криптовалютным кошельком. Она позволяет восстановить доступ к содержимому определенного блокчейн-адреса даже в случае потери последнего // https://www.ledger.com/ru/academy/glossary/seed-phrase.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. БОЛЬШИЕ НОВОСТИ: криптостример потерял 100 тыс. долларов в прямом эфире // Binance square // https://www.binance.com/ru/square/post/16345770086753.
2. **Заболоцкая А.В., Ткачева Е.Г.** Психологическая безопасность личности в Интернете // Автономия личности. 2022.
3. Закон РФ от 05.03.1992 № 2446-1 (ред. от 26.06.2008) «О безопасности» // Судебные и нормативные акты РФ // https://sudact.ru/law/zakon-rf-ot-05031992-n-2446-1-o/.
4. **Ибегаева Ф.А., Гайфуллина А.Р.** Классификация потребностей А. Маслоу // Экономика и социум. 2015.
5. **Кузмичева А.** Взлом De-Fi-протокола Euler Finance унес почти $200 млн в криптовалюте // РБК // https://www.rbc.ru/crypto/news/640eef7b9a794703ee29646f.
6. **Лазарева А.Ю.** Психологическая безопасность личности // Форум молодых ученых. 2019.
7. Ничего личного: кто и зачем продает биометрию в даркнете // ИЗВЕСТИЯ // https://iz.ru/1742268/mariia-frolova/nichego-lichnogo-kto-i-zachem-prodaet-biometriiu-v-darknete.
8. **Пельменев Д.Ю., Важенина Н.В.** Экономическая безопасность в сети Интернет // Теория и практика современной науки. 2017.
9. «Привет Фридману»: что известно о сливе данных 38 млн клиентов «Альфы» // News.ru // https://news.ru/russia/privet-fridmanu-chto-izvestno-o-slive-dannyh-38-mln-klientov-alfy/.
10. **Смолева Е.О., Попов А.В.** Особенности цифрового гражданского участия в ракурсе современных исследований // Экономические и социальные перемены: факты, тенденции, прогноз. 2022.
11. Стример якобы потерял $100 тыс. в криптовалюте и разбил клавиатуру. Оказалось, что это фейк // VGTimes // https://vgtimes.ru/news/115605-strimer-yakoby-poteryal-100-tys.-v-kriptovalyute-i-razbil-klaviaturu.-okazalos-chto-eto-feyk.html.
12. Указ Президента Российской Федерации от 02.07.2021 № 400 // Kremlin.ru // http://www.kremlin.ru/acts/bank/47046.
13. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Kremlin.ru // http://www.kremlin.ru/acts/bank/41460.
14. Федеральный закон от 27.07.2006 г. № 149-ФЗ // Kremlin.ru // http://www.kremlin.ru/acts/bank/24157.
15. «Цель уже не только деньги». РКН заявил об утечке в интернете 600 млн записей о россиянах – чем это опасно // MSK1.ru // https://msk1.ru/text/world/2024/11/09/74317205/.

16. **Anderson R.** Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken: Wiley, 2020.
17. **Baumann R., Cohen M., Reaves B.** «The Impact of Digital Privacy Regulations on Security Practices» // Computers & Security. 2019. Vol. 88. DOI: 10.1016/j.cose.2019.101582.
18. **Kshetri N.** The Economics of Cybersecurity: Risk Management in an Interconnected World. Cambridge: Cambridge University Press, 2021.
19. **Schneier B.** Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015.
20. **Whitman M.E., Mattord H.J.** Principles of Information Security. 6th ed. Boston: Cengage Learning, 2018.

S.S. MOROZOVA
Associate Professor, Department of Russian Politics,
Saint Petersburg State University,
Saint Petersburg, Russia

A.G. DEDUL
Lecturer, Faculty of Political Science,
Saint Petersburg State University, Saint Petersburg, Russia

I.A. BULATOV
Master's student, Saint Petersburg State
University, Saint Petersburg, Russia

SECURITY AND PRIVACY ISSUES IN THE CONTEXT OF DIGITAL CIVIC PARTICIPATION SECURITY

The digitalization of public life has led to the transformation of traditional forms of civic participation, opening up new opportunities for citizens to interact with public institutions. However, the development of digital civic participation is accompanied by challenges related to the security and privacy of user data. The article analyzes key challenges in this area, including cyberattacks, data breaches and privacy issues, and offers recommendations to minimize them. Special attention is paid to legal, technical and educational aspects of data protection. The conclusions and recommendations presented are aimed at improving data security and citizens' trust in digital platforms.

Key words: *digital civic engagement, data security, privacy, digitalization, cyber threats, information protection, digital literacy.*