УДК 004.056.5

ПРОБЛЕМА БАЛАНСА МЕЖДУ ПЕРСОНАЛИЗАЦИЕЙ И КОНФИДЕНЦИАЛЬНОСТЬЮ В ЦИФРОВОМ ПРЕДПРИНИМАТЕЛЬСТВЕ: НОРМАТИВНО-ПРАВОВОЙ И ТЕХНИЧЕСКИЙ АСПЕКТЫ

Галимова А.Ш.
к. э. н., доцент,
ФГБОУ ВО «Уфимский университет науки и технологий»,
РФ, г. Уфа

Алчинов Р.Р.
студент,
ФГБОУ ВО «Уфимский университет науки и технологий»,
РФ, г. Уфа

Аннотация. В условиях цифровой трансформации предпринимательской деятельности персонализация клиентского опыта стала ключевым фактором конкурентоспособности, однако она неизбежно сопряжена со сбором и обработкой больших объемов персональных данных, что порождает конфликт с требованиями конфиденциальности. В данной статье рассматривается проблема достижения баланса между персонализацией и защитой персональных данных в цифровом предпринимательстве. Проанализированы основные нормативно-правовые акты, регулирующие обработку персональных данных в России (152-ФЗ, требования Роскомнадзора) и за рубежом (GDPR, CCPA). Исследованы технические инструменты, позволяющие минимизировать риски утечек и соблюдать правовые требования без потери качества персонализации. Предложена модель компромиссной стратегии для цифровых предпринимателей, учитывающая как бизнес-интересы, так и права субъектов персональных данных.

Ключевые слова: персонализация, конфиденциальность, персональные данные, цифровое предпринимательство, GDPR, 152-ФЗ, обработка данных, баланс интересов, технические средства защиты.

THE BALANCE PROBLEM BETWEEN PERSONALIZATION AND PRIVACY IN DIGITAL ENTREPRENEURSHIP: REGULATORY AND TECHNICAL ASPECTS

Galimova A.S.
Candidate of Economics, Associate Professor,
Ufa University of Science and Technology,
Ufa, Russian Federation

Alchinov R.R.
student,
Ufa University of Science and Technology,
Ufa, Russian Federation

Annotation. In the context of digital transformation of entrepreneurial activity, personalization of customer experience has become a key factor of competitiveness, but it inevitably involves the collection and processing of large volumes of personal data, which creates a conflict with privacy requirements. This article examines the problem of achieving a balance between personalization and personal data protection in digital entrepreneurship. The main regulatory legal acts governing the processing of personal data in Russia (Federal Law No. 152-FZ, requirements of Roskomnadzor) and abroad (GDPR, CCPA) are analyzed. Technical tools that minimize the risks of leaks and comply with legal requirements without losing the quality of personalization are studied. A compromise strategy model for digital entrepreneurs is proposed, taking into account both business interests and the rights of personal data subjects.

Keywords: personalization, privacy, personal data, digital entrepreneurship, GDPR, 152-FZ, data processing, balance of interests, technical means of protection.

Цифровое предпринимательство на современном этапе развития рыночных отношений немыслимо без использования персональных данных потребителей. Сбор, анализ и применение информации о поведении, предпочтениях и характеристиках клиентов позволяет компаниям предлагать персонализированные товары и услуги, повышать конверсию и лояльность

аудитории. Однако та же самая практика порождает серьезные риски нарушения прав граждан на конфиденциальность, защиту частной жизни и информационную безопасность [1].

Проблема баланса между персонализацией и конфиденциальностью приобрела особую остроту в последние годы по нескольким причинам. Во-первых, объемы собираемых данных о пользователях достигли беспрецедентных масштабов. Во-вторых, технологии анализа данных (Big Data, машинное обучение) позволяют извлекать из обезличенной на первый взгляд информации такие сведения, которые сам пользователь не намеревался раскрывать. В-третьих, ужесточение законодательства в области защиты персональных данных в России, Европейском союзе, США и других юрисдикциях создает для цифровых предпринимателей сложную и динамичную нормативно-правовую среду [2, 3].

Цель данной работы – выявить сущность противоречия между персонализацией и конфиденциальностью в цифровом предпринимательстве, проанализировать ключевые нормативно-правовые и технические аспекты данной проблемы и предложить практические рекомендации по достижению баланса. Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть экономические стимулы персонализации и правовые ограничения на обработку персональных данных;
2. Проанализировать основные требования российского и зарубежного законодательства в области защиты персональных данных;
3. Исследовать технические инструменты, позволяющие совмещать персонализацию с конфиденциальностью;
4. Разработать модель компромиссной стратегии для цифровых предпринимателей.

Персонализация представляет собой процесс адаптации продукта, сервиса или коммуникации под индивидуальные характеристики конкретного пользователя. В цифровом предпринимательстве персонализация реализуется через рекомендательные системы, таргетированную рекламу, динамический контент сайтов, персонализированные email-рассылки и другие инструменты [4].

Экономическая эффективность персонализации подтверждается многочисленными исследованиями (таблица 1). Согласно данным, внедрение персонализированных рекомендаций может увеличить выручку интернет-магазина на 10–30%, а конверсию – на 15–20%. Пользователи в среднем на 40% чаще взаимодействуют с персонализированным контентом, чем с универсальным [5]. Однако достижение этих результатов требует сбора и анализа значительных объемов данных о пользователях: история покупок, просмотров, геолокация, поведенческие паттерны, демографические характеристики и т.д.

Именно здесь возникает основное противоречие. Чем выше степень персонализации, тем больше данных необходимо собрать и проанализировать, а значит, тем выше риски нарушения конфиденциальности. Пользователи, с одной стороны, ожидают релевантных предложений и удобного интерфейса, а с другой – все чаще выражают обеспокоенность тем, как компании собирают, хранят и используют их данные [6].

Таблица 1 – Экономические стимулы и правовые ограничения персонализации: основные противоречия

Аспект	Интересы цифрового предпринимателя	Права и ожидания субъекта данных	Нормативно-правовой контекст
Объем собираемых данных	Максимизация сбора для более точной персонализации	Минимизация сбора только необходимых данных	Принцип минимизации данных (GDPR ст.5, 152-ФЗ ст.5)

Срок хранения данных	Длительное хранение для анализа динамики поведения	Ограниченное хранение, удаление после достижения целей	Ограничение срока хранения (GDPR ст.5, 152-ФЗ ст.5)
Прозрачность обработки	Минимальное информирование, сложные пользовательские соглашения	Полная и понятная информация об обработке	Информированное согласие (GDPR ст.13-14, 152-ФЗ ст.9)
Использование для новых целей	Свободное использование данных для любых бизнес-задач	Запрет на использование без отдельного согласия	Целевое ограничение (GDPR ст.5, 152-ФЗ ст.5)
Передача третьим лицам	Передача партнерам для расширения аналитики	Контроль над передачей и возможность запрета	Согласие на передачу (GDPR ст.45-49, 152-ФЗ ст.12)

**Составлено автором на основе [2, 3, 6]*

В Российской Федерации основным нормативно-правовым актом, регулирующим обработку персональных данных, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Закон устанавливает принципы и условия обработки персональных данных, права субъектов, обязанности операторов и механизмы государственного контроля [2].

Ключевые требования 152-ФЗ, значимые для цифрового предпринимательства, включают:

1. Принцип законности – обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Принцип ограничения обработки – обработка ограничивается достижением конкретных, заранее определенных и законных целей.

3. Принцип минимизации данных – обрабатываются только те данные, которые соответствуют целям их обработки.

4. Локализация данных – с 1 сентября 2015 года (ст. 18 152-ФЗ) операторы обязаны обеспечивать запись, систематизацию, накопление, хранение, уточнение и извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ.

5. Требование согласия – обработка персональных данных допускается только с согласия субъекта, за исключением прямо предусмотренных законом случаев.

Особенно важным для цифровых предпринимателей является требование о локализации данных. Это означает, что, если вы собираете персональные данные российских пользователей, технические средства их обработки (серверы, базы данных) должны физически находиться на территории России. Многие международные компании были вынуждены разворачивать собственную инфраструктуру в РФ или переносить данные из зарубежных облачных сервисов в российские дата-центры [7].

Контроль и надзор за соблюдением 152-ФЗ осуществляет Роскомнадзор, который наделен полномочиями по проведению проверок, вынесению предписаний и наложению административных штрафов. Нарушение законодательства о персональных данных влечет административную ответственность по ст. 13.11 КоАП РФ, предусматривающую штрафы для юридических лиц от 60 000 до 100 000 рублей за отдельные нарушения, а за повторное нарушение или отказ локализовать данные – до 18 млн рублей.

Сопоставимым по значимости и более жестким по санкциям является Общий регламент по защите данных Европейского союза (GDPR), вступивший в силу 25 мая 2018 года [3]. GDPR распространяется на все компании, обрабатывающие персональные данные граждан ЕС, независимо от местонахождения самой компании (принцип экстерриториальности). Таким

образом, российские цифровые предприниматели, имеющие клиентов из стран ЕС, обязаны соблюдать требования GDPR.

Ключевые положения GDPR включают:

– Право на забвение (ст. 17) – субъект данных может требовать удаления своих данных при отсутствии законных оснований для их хранения.

– Право на переносимость данных (ст. 20) — субъект вправе получить свои данные в структурированном, машиночитаемом формате и передать их другому оператору.

– Privacy by Design and by Default (ст. 25) – принцип встраивания защиты данных в разрабатываемые системы и процессы по умолчанию.

– Оценка воздействия на защиту данных (DPIA) (ст. 35) – обязательная процедура для операций с высокими рисками для прав и свобод субъектов.

– Уведомление об утечках (ст. 33-34) – обязанность в течение 72 часов уведомить надзорный орган и субъектов о произошедшей утечке данных.

Штрафы за нарушение GDPR достигают 20 миллионов евро или 4% от годового глобального оборота компании (в зависимости от того, какая сумма больше). Это создает мощный стимул для цифровых предпринимателей инвестировать в соблюдение требований [8].

В США основным регулирующим актом на уровне штата является Калифорнийский закон о защите прав потребителей (CCPA), вступивший в силу 1 января 2020 года. CCPA предоставляет потребителям право знать, какие персональные данные собираются о них, право на удаление данных и право отказаться от продажи своих данных третьим лицам. Рассмотрим ключевые нормативно-правовые акты, представленные в таблице 2.

Таблица 2 – Сравнительный анализ ключевых нормативно-правовых актов

Критерий	152-ФЗ (Россия)	GDPR (ЕС)	CCPA (Калифорния, США)

Территориальная сфера	Обработка данных граждан РФ	Обработка данных граждан ЕС (экстерриториально)	Компании, работающие с жителями Калифорнии
Основание обработки	Согласие, договор, закон	6 легитимных оснований (согласие, договор, законный интерес и др.)	Согласие, выполнение контракта
Право на удаление	Предусмотрено (ст. 14)	Да, «право на забвение» (ст. 17)	Да (ст. 1798.105)
Уведомление об утечках	Обязательно (ст. 21, уведомление РКН)	В течение 72 часов (ст. 33)	Без необоснованной задержки
Максимальный штраф	До 18 млн руб.	€20 млн или 4% оборота	$7 500 за нарушение
Принцип локализации	Да (ст. 18)	Нет, но трансграничная передача ограничена	Нет

**Составлено автором на основе [2, 3, 8]*

Соблюдение нормативно-правовых требований при сохранении возможностей персонализации требует внедрения специальных технических решений. Современные технологии позволяют собирать, анализировать и использовать данные о пользователях без нарушения их конфиденциальности и с соблюдением принципов минимизации данных и целевого ограничения.

Анонимизация представляет собой процесс удаления из набора данных всей информации, позволяющей идентифицировать конкретного субъекта. В отличие от псевдонимизации (замены прямых идентификаторов на псевдонимы), анонимизация считается необратимой – при правильном выполнении восстановить связь между данными и субъектом невозможно [9].

Для цифрового предпринимательства анонимизация открывает возможности: анонимные данные не подпадают под действие 152-ФЗ и GDPR,

поскольку не являются персональными. Это означает, что компании могут собирать и анализировать анонимные данные о поведении пользователей без получения согласия, хранения в локализованных базах данных и прочих ограничений.

Однако важно понимать ограничения анонимизации. Во-первых, полностью анонимные данные непригодны для персонализации на уровне отдельного пользователя – только для агрегированных статистик и трендов. Во-вторых, исследования показывают, что даже анонимные данные часто могут быть реидентифицированы при сопоставлении с другими источниками данных.

Более перспективным для баланса персонализации и конфиденциальности является использование технологий повышения конфиденциальности (Privacy-Enhancing Technologies – PETs) [10]. Ключевые PETs, применимые в цифровом предпринимательстве, включают:

Дифференциальная приватность (Differential Privacy). Технология, разработанная в Microsoft и Apple, позволяет анализировать данные о группах пользователей с добавлением математически обоснованного «шума» — случайных искажений, которые не влияют на общую точность анализа, но делают невозможным выделение данных конкретного человека. Компания Apple использует дифференциальную приватность для анализа популярных эмодзи, часто вводимых слов и других поведенческих паттернов миллионов пользователей iPhone без доступа к их личным данным.

Федеративное обучение (Federated Learning). Технология машинного обучения, при которой модель обучается на устройствах пользователей (смартфонах, ноутбуках), а не в централизованном облаке. На сервер передаются только обновленные веса модели (математические коэффициенты), но не исходные данные пользователей. Google использует федеративное обучение для улучшения предсказания следующего слова в клавиатуре Gboard: каждый смартфон обучает модель на своих данных о нажатиях пользователя, затем анонимно отправляет только улучшения на центральный сервер.

Безопасные многосторонние вычисления (Secure Multi-Party Computation – SMPC). Технология, позволяющая нескольким сторонам совместно анализировать данные, не раскрывая их друг другу. Это может быть полезно, например, при объединении данных о клиентах из нескольких независимых сервисов для кросс-персонализации без передачи баз данных.

Доказательства с нулевым разглашением (Zero-Knowledge Proofs). Технология, позволяющая одной стороне доказать другой, что она обладает определенной информацией (например, что пользователь старше 18 лет или проживает в определенном регионе), не раскрывая саму эту информацию.

Проведенное исследование проблемы баланса между персонализацией и конфиденциальностью в цифровом предпринимательстве позволяет сформулировать следующие выводы.

Во-первых, противоречие между экономическими стимулами цифровых предпринимателей (стремящихся к максимальному сбору и анализу данных для персонализации) и правовыми ограничениями (152-ФЗ, GDPR, CCPA, требующими минимизации, целевого ограничения и согласия) является объективным и не может быть полностью устранено. Однако оно может быть смягчено за счет грамотного выбора технических и организационных решений.

Во-вторых, российское законодательство (152-ФЗ) и зарубежные акты (GDPR) при всех различиях сходятся в ключевых принципах: законность обработки, минимизация данных, целевое ограничение, информированное согласие и обеспечение прав субъектов. Для цифровых предпринимателей, работающих на международных рынках, наиболее жесткие требования предъявляет GDPR (экстерриториальность, штрафы до 4% оборота, право на забвение), в то время как 152-ФЗ добавляет специфическое требование локализации баз данных граждан РФ.

В-третьих, технические инструменты достижения баланса существуют и активно развиваются. Анонимизация и псевдонимизация позволяют снизить риски при сохранении части аналитических возможностей. Технологии

повышения конфиденциальности (дифференциальная приватность, федеративное обучение, безопасные многосторонние вычисления) открывают новые горизонты для персонализации без доступа к идентифицированным данным. Однако их внедрение требует инвестиций в разработку и привлечения квалифицированных специалистов.

Перспективы дальнейших исследований связаны с развитием технологий PETs, изучением поведения пользователей в отношении согласий на обработку данных (consent fatigue и способы ее преодоления), а также с анализом правоприменительной практики по 152-ФЗ и GDPR в части цифрового предпринимательства.

Библиографический список

1. Кузнецов С. В. Персонализация в цифровом маркетинге: возможности и риски // Маркетинг в России и за рубежом. – 2024. – № 2. – С. 23-35.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2025).

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

4. Смирнова О. А. Цифровое предпринимательство: трансформация бизнес-моделей // Экономика и управление. – 2023. – № 7. – С. 58-67.

5. McKinsey & Company. The value of getting personalization right – and the cost of getting it wrong. – 2024. – 28 p.

6. Захаров А. В. Конфиденциальность в цифровую эпоху: баланс интересов бизнеса и потребителей // Вопросы экономики. – 2024. – № 11. – С. 89-104.

7. Роскомнадзор. Разъяснения по вопросу локализации баз данных персональных данных граждан РФ. – 2024. [Электронный ресурс]. – Режим доступа: https://rkn.gov.ru (дата обращения: 10.05.2026).

8. Калинина Т. С. Влияние GDPR на российский бизнес: опыт адаптации // Международное право и международные организации. – 2023. – № 4. – С. 42-56.

9. Васильев П. П. Анонимизация и псевдонимизация персональных данных: правовые и технические аспекты // Информационное право. – 2024. – № 1. – С. 15-28.

10. Григорьев М. И. Технологии повышения конфиденциальности (PETs): обзор и перспективы применения в бизнесе // Цифровая экономика. – 2025. – № 2. – С. 33-47.