

НИКИТА КУЛИКОВ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

Руководство для граждан и бизнеса



Опыт АНО «ПравоРоботов»

Никита Куликов

Защита персональных данных в интернете

<https://litres.ru/74564344>

SelfPub; 2026

Аннотация

Мы живем в эпоху, когда данные стали новой нефтью, а информация о человеке — ценнейшим товаром. Каждое наше действие в цифровом мире: поисковый запрос, покупка в интернет-магазине, отметка в социальной сети, использование мобильного приложения — оставляет цифровой след. Этот след превращается в массив персональных данных, который анализируется, продается и используется для самых разных целей — от показа персонализированной рекламы до влияния на политические процессы.

Согласно опросам ВЦИОМ, более 70% россиян обеспокоены вопросами безопасности своих личных данных в интернете, но лишь 15% регулярно читают политики конфиденциальности перед использованием сервисов. Более того, даже среди тех, кто читает политики, лишь малая часть понимает их юридическое содержание, что делает проблему еще более острой.

Я постарался изложить сложный материал простым и понятным языком, снабдив его практическими примерами

и рекомендациями, которые можно применить сразу после прочтения.

Содержание

ВВЕДЕНИЕ	6
Глава 2. Современные вызовы и риски в цифровой среде	25
Конец ознакомительного фрагмента.	30

Никита Куликов

Защита персональных данных в интернете

ТИТУЛЬНЫЙ ЛИСТ

**ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕР-
НЕТЕ**

Руководство для граждан и бизнеса

Опыт компании АНО «ПравоРоботов»

Никита Куликов

ВВЕДЕНИЕ

Мы живем в эпоху, когда данные стали новой нефтью, а информация о человеке — ценнейшим товаром. Каждое наше действие в цифровом мире: поисковый запрос, покупка в интернет-магазине, отметка в социальной сети, использование мобильного приложения — оставляет цифровой след. Этот след превращается в массив персональных данных, который анализируется, продается и используется для самых разных целей — от показа персонализированной рекламы до влияния на политические процессы.

По оценкам экспертов, в 2025 году объем генерируемых данных в мире достиг 175 зеттабайт, и значительная часть этой информации содержит персональные данные. Россия является одним из лидеров по проникновению интернета и использованию цифровых сервисов, что делает вопрос защиты данных особенно актуальным для нашей страны.

В России, как и во всем мире, остро стоит проблема защиты персональных данных. С одной стороны, у нас есть один из самых прогрессивных законов в этой сфере — Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», который постоянно совершенствуется и дополняется с учетом новых вызовов.

С другой стороны, правоприменительная практика и ре-

альная ситуация с защитой прав граждан оставляют желать лучшего. Закон работает не в полную силу, а граждане зачастую даже не подозревают о масштабах сбора их данных и о тех рисках, которым они подвергаются.

Согласно опросам ВЦИОМ, более 70% россиян обеспокоены вопросами безопасности своих личных данных в интернете, но лишь 15% регулярно читают политики конфиденциальности перед использованием сервисов. Этот разрыв между восприятием угрозы и реальными действиями по ее предотвращению является одной из ключевых проблем, которую призвана решить эта книга. Более того, даже среди тех, кто читает политики, лишь малая часть понимает их юридическое содержание, что делает проблему еще более острой.

Эта книга призвана стать путеводителем в сложном и запутанном мире защиты персональных данных в интернете. Она написана для широкого круга читателей: для юристов, которые хотят разобраться в тонкостях законодательства и последних изменений в правоприменительной практике; для IT-специалистов, разрабатывающих продукты с учетом требований закона и стремящихся минимизировать риски для пользователей; для предпринимателей, которые хотят строить свой бизнес с соблюдением всех требований закона; и, самое главное, для обычных пользователей, которые хотят знать, как защитить свои права и личную информацию в условиях тотальной цифровизации.

Я постарался изложить сложный с точки зрения восприятия материал простым и понятным языком, снабдив его практическими примерами и рекомендациями, которые можно применить сразу после прочтения.

В основе книги лежит масштабное исследование, проведенное в рамках совместного проекта АНО «Российская система качества» (Роскачество) и АНО «ПравоРоботов».

Мы проанализировали более 600 политик конфиденциальности различных интернет-сервисов по более 35 направлениям, от маркетплейсов и такси до приложений для женского здоровья и родительского контроля.

Эта работа, не имеющая аналогов в России по своему масштабу, позволила не только оценить формальное соответствие документов требованиям 152-ФЗ, но и выявить реальные практики сбора и передачи данных, которые часто скрыты от глаз пользователя за многостраничными юридическими текстами.

Я благодарен нашим партнерам из Роскачества за предоставленную возможность провести это исследование. Результаты этого проекта уже помогли тысячам пользователей сделать осознанный выбор сервисов и защитить свои права.

Оглавление

ВВЕДЕНИЕ

Глава 1. Теоретические основы защиты персональных данных

Глава 2. Современные вызовы и риски в цифровой среде

Глава 3. Прикладной анализ соответствия политик конфиденциальности: исследование АНО Роскачества и АНО «ПравоРоботов»

Глава 4. Правовой механизм защиты прав субъектов ПДН

Глава 5. Практические рекомендации для пользователей

Глава 6. Актуальные проблемы и пути их решения

Глава 7. Отраслевые особенности защиты персональных данных

Глава 8. Как создавать политику конфиденциальности, которая действительно защищает пользователей: инновационный подход АНО «ПравоРоботов»

Глава 9. Защита персональных данных детей

Заключение

Приложение

НИКИТА КУЛИКОВ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

Руководство для граждан и бизнеса



Опыт АНО «ПравоРоботов»

Глава 1. Теоретические основы защиты персональных данных

1.1. Что такое персональные данные? Определение и правовая природа

Прежде чем говорить о защите, необходимо четко определить объект защиты. Согласно пункту 1 статьи 3 Федерального закона № 152-ФЗ, персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Это определение является ключевым и охватывает практически любую информацию, которая может идентифицировать человека. К персональным данным относятся: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также иные сведения.

В эпоху цифровизации этот список расширился за счет IP-адресов, файлов cookie, идентификаторов устройств (IDFA, Android ID), данных о геолокации, истории просмотров и покупок. Все это, особенно в совокупности, позволяет «вычислить» конкретного человека, даже если прямо его имя не указывается. Например, даже без указания имени, уникальная комбинация геолокационных данных, истории посещений и идентификатора устройства может с высокой точно-

стью идентифицировать пользователя.

Важно понимать, что персональные данные — это не просто набор сведений. Это нематериальное благо, тесно связанное с правом на частную жизнь, личную и семейную тайну (статья 23 Конституции РФ). Конституционный Суд РФ неоднократно подчеркивал, что право на неприкосновенность частной жизни является фундаментальным и неотъемлемым, вытекающим из самого понятия человеческого достоинства.

Поэтому оборот этих данных — это не просто экономическая деятельность, а сфера, затрагивающая основополагающие права человека. Любое вмешательство в эту сферу должно быть строго регламентировано законом и осуществляться только на законных основаниях. Именно поэтому законодатель установил жесткие требования к обработке персональных данных, а также механизмы контроля и ответственности для операторов.

Особую категорию составляют специальные и биометрические персональные данные. Специальные данные касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни. Биометрические данные — это физиологические и биологические характеристики человека (отпечатки пальцев, изображение лица, ДНК, голос).

Их обработка допускается только с письменного согласия

субъекта и в строго ограниченных случаях. В связи с развитием технологий искусственного интеллекта и распознавания лиц, правовое регулирование биометрических данных становится одним из самых быстрорастущих и обсуждаемых направлений в законодательстве.

1.2. Принципы обработки персональных данных

Закон № 152-ФЗ устанавливает ряд принципов, которым обязан следовать любой оператор (государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и/или осуществляющие обработку персональных данных, а также определяющие ее цели и состав данных).

Эти принципы являются краеугольным камнем всей системы защиты и призваны обеспечить баланс интересов субъектов и операторов. Рассмотрим их подробнее с примерами:

Законность и справедливость. Обработка должна осуществляться на законной основе, а не быть произвольной. Пользователь не должен вводиться в заблуждение относительно целей и способов обработки его данных. Это означает, что все действия оператора должны быть предсказуемыми и соответствовать не только букве, но и духу закона.

Справедливость подразумевает, что бремя сбора данных должно быть соразмерно выгоде, получаемой субъектом от использования сервиса. Например, несправедливо требовать

доступ к контактам для приложения-фонарика, так как это не дает пользователю никакой дополнительной выгоды, а лишь создает для него риски.

Соразмерность и минимизация. Оператор должен обрабатывать только те данные и только в том объеме, которые необходимы для достижения конкретных, заранее определенных и законных целей. Нельзя собирать данные «про запас» или на случай, если они когда-нибудь пригодятся. Например, приложению-фонарику не нужен доступ к контактам и микрофону, а сервису доставки пиццы не нужны данные о состоянии здоровья пользователя.

Нарушение этого принципа является одним из самых распространенных. Компании часто собирают как можно больше данных, чтобы в будущем иметь возможность их монетизировать.

Определенность целей. Цели обработки должны быть четко сформулированы и не могут быть изменены впоследствии без согласия субъекта. Нельзя собирать данные для одной цели (например, доставка заказа), а использовать их для другой (например, рекламный спам).

Оператор обязан заранее уведомить пользователя о том, для чего именно он собирает его данные, и не расширять эти цели без получения нового согласия. Политика конфиденциальности должна содержать исчерпывающий перечень целей обработки.

Актуальность и достаточность. Данные должны быть

точными и актуальными. Оператор обязан принимать меры для их уточнения или удаления, если они являются неполными или устаревшими. Это особенно важно для данных, используемых в юридически значимых действиях, например, для оформления кредита или заключения договора.

Субъект имеет право требовать исправления неточных данных. Например, если у вас изменился адрес, вы можете потребовать от оператора обновить эту информацию в его базе данных.

Ограниченность сроков хранения. Данные должны храниться не дольше, чем этого требуют цели обработки. После их достижения (или утраты необходимости в них) данные должны быть уничтожены или обезличены. Закон не устанавливает единых сроков для всех случаев, но требует, чтобы оператор определил их самостоятельно и закрепил во внутренних документах.

Бесконечное хранение данных без цели является нарушением. Например, нельзя хранить данные о доставке пиццы в течение 10 лет, если они не нужны для налогового учета или для решения споров.

Безопасность. Обработка данных должна обеспечивать их защиту от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, распространения. Оператор обязан принимать организационные (назначение ответственных лиц, разработка политик безопасности) и технические (шифрование, антивирусы, межсетевые экраны)

меры для защиты данных.

Уровень защиты должен быть адекватен характеру обрабатываемых данных и потенциальным угрозам. Например, для банковских данных требуется самый высокий уровень защиты.

1.3. Субъекты и объекты правоотношений

Правовое поле в этой области образуют три основных субъекта, взаимодействие которых определяет весь процесс обработки данных:

Субъект персональных данных — это физическое лицо, к которому относятся данные. Это любой человек, чьи данные собираются и обрабатываются. Он является носителем прав, в первую очередь, права на защиту своей частной жизни. Ключевое право субъекта — давать или не давать согласие на обработку своих данных, а также отзывать его в любой момент.

Субъект также имеет право на доступ к своим данным, их исправление и блокировку. Важно понимать, что субъектом может быть как взрослый дееспособный гражданин, так и ребенок или недееспособное лицо, чьи права защищаются законными представителями. Особый порядок обработки данных детей установлен статьей 9 152-ФЗ, которая требует получения согласия родителей.

Оператор — это государственный орган, муниципальный орган, юридическое или физическое лицо, организую-

щие и/или осуществляющие обработку персональных данных, а также определяющие ее цели и состав данных. Именно на оператора возложена основная обязанность по соблюдению закона.

Он должен не только законно собирать данные, но и обеспечивать их безопасность, а также отвечать на запросы субъектов. С 2022 года операторы, обрабатывающие значительные объемы данных, обязаны назначать ответственных за организацию обработки персональных данных. Этот институт призван обеспечить более эффективный контроль за соблюдением законодательства внутри организации.

Уполномоченный орган по защите прав субъектов персональных данных — это федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В России это Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

В его полномочия входит ведение реестра операторов, проведение проверок, рассмотрение жалоб граждан и привлечение нарушителей к административной ответственности. Роскомнадзор также активно участвует в разработке нормативных актов и разъяснении законодательства, публикуя на своем сайте письма и рекомендации для операторов.

1.4. Ключевые положения 152-ФЗ и последние из-

менения

Федеральный закон № 152-ФЗ является базовым документом, регулирующим все аспекты обработки персональных данных. За время своего существования он претерпел множество изменений, направленных на усиление защиты прав граждан.

Одним из ключевых нововведений стало требование об обязательной локализации баз данных российских граждан на территории РФ (так называемый «закон о локализации»). Это означает, что операторы обязаны записывать, систематизировать, накапливать и хранить данные российских пользователей с использованием серверов, находящихся на территории России.

Это требование вступило в силу с 1 сентября 2015 года и является одним из самых жестких в мире. Оно призвано обеспечить доступность данных для российских правоохранительных органов и защитить их от несанкционированного доступа из-за рубежа.

Другим важным изменением стало введение института уполномоченных лиц по защите данных и ужесточение требований к порядку получения согласия. Теперь согласие должно быть более конкретным и информированным.

Закон также расширил перечень случаев, когда требуется письменное согласие (например, для обработки биометрических данных). В последние годы активно обсуждаются новые поправки, касающиеся обработки данных при исполь-

зовании искусственного интеллекта и биометрической идентификации, что говорит о динамичном развитии законодательства в этой сфере.

С 2024 года вступили в силу изменения, усиливающие ответственность операторов за утечки данных, включая оборотные штрафы (до 1% от годовой выручки). Это стало реакцией законодателя на участвовавшие случаи крупных утечек данных, затронувших миллионы россиян.

Также ужесточены требования к уведомлению Роскомнадзора об утечках — теперь это нужно делать в течение 24 часов с момента инцидента.

1.5. Международные стандарты и опыт зарубежных стран

Для понимания места российского законодательства в глобальном контексте важно рассмотреть международные стандарты. Основным документом является Общий регламент по защите данных (GDPR) Европейского Союза, который вступил в силу в 2018 году.

GDPR считается самым строгим и детальным законом о защите данных в мире. Он устанавливает экстерриториальный принцип действия, что означает, что требования GDPR распространяются на все компании, обрабатывающие данные граждан ЕС, независимо от места их нахождения.

GDPR ввел такие понятия, как «право на забвение», «портативность данных», а также установил колоссальные

штрафы — до 20 миллионов евро или 4% от годового оборота компании.

Углубленное сравнение подходов ЕС, США и Китая

Для более глубокого понимания места российского законодательства в глобальном контексте, рассмотрим ключевые различия между основными регуляторными моделями:

Характер

ЕС (GDPR)

США (секторальный подход)

Китай (PIPL)

Россия (152-ФЗ)

Основной принцип

Защита прав человека

Свобода рынка и защита потребителя

Национальная безопасность и суверенитет

Защита прав человека и государственный контроль

Террито-риальный охват

Экстеррито-риальный

В основном национальный

Экстеррито-риальный (с оговорками)

Экстерриториальный (для данных россиян)

Ключевое понятие

Право на забвение, портативность данных
Право знать, право отказаться от продажи
Безопасность данных, суверенитет
Локализация данных, согласие

Штрафы

До 20 млн евро или 4% оборота

Вариативные, в основном от 2 500 до 7 500 долларов за нарушение

До 50 млн юаней или 5% оборота

До 1,5 млн рублей (оборотные штрафы до 1% с 2024 г.)

Орган надзора

Европейский совет по защите данных (EDPB)

Федеральная торговая комиссия (FTC) и отраслевые регуляторы

Управление по защите персональных данных (PIPB)

Роскомнадзор

Различия в подходах:

Правовая природа: GDPR исходит из того, что данные принадлежат человеку, и он является их «владельцем». Российский закон говорит о «субъекте», чьи права защищаются, но данные при этом находятся в обороте. Китайский подход делает акцент на праве государства контролировать данные в целях национальной безопасности.

Согласие: В ЕС и России требуется активное, информированное согласие. В США согласие часто «встраивается» в условия использования, а отказ от сбора данных может быть сложным. Китай требует отдельного согласия для передачи данных третьим лицам.

Локализация: Это уникальное требование России и Китая. В ЕС данные могут храниться где угодно, но с условием адекватного уровня защиты. В США законы о локализации действуют лишь для некоторых отраслей (например, данные о состоянии здоровья).

Право на забвение: В ЕС оно закреплено жестко (ст. 17 GDPR). В России оно действует в ограниченном виде (только для недостоверных данных). В США оно отсутствует на федеральном уровне, но действует в Калифорнии. В Китае оно не закреплено, но есть требование удалять данные по достижении целей обработки.

Влияние на бизнес: Различия в подходах создают серьезные сложности для транснациональных компаний. Например, политика конфиденциальности для пользователей из ЕС должна соответствовать GDPR, для российских пользователей — 152-ФЗ, а для китайских — PIPL. Это требует создания отдельных документов и систем хранения данных для каждой юрисдикции.

1.6. Международные тренды и вызовы

На международном уровне выделяются несколько гло-

бальных трендов, которые влияют и на российское законодательство:

Регулирование искусственного интеллекта (ИИ). ЕС готовит «Закон об ИИ» (AI Act), который классифицирует системы ИИ по уровню риска и устанавливает требования к данным, используемым для обучения. В России также обсуждается необходимость регулирования ИИ, особенно в части использования биометрических данных и «черных ящиков» алгоритмов, которые принимают решения о гражданах.

Цифровой суверенитет. Все больше стран (Китай, Россия, Индия) стремятся к созданию собственных независимых цифровых инфраструктур, чтобы снизить зависимость от американских технологических гигантов. Это влияет на требования к локализации данных и использованию национальных облачных платформ.

Право на портативность данных. GDPR закрепил право пользователя переносить свои данные от одного оператора к другому. В России эта концепция пока активно обсуждается, но не реализована в полной мере. В будущем это может стать важным инструментом для пользователей и создания конкурентной среды.

Ужесточение ответственности за утечки. По всему миру штрафы за утечки данных растут. В России с 2024 года введены оборотные штрафы, в Китае они достигают 5% оборота, в ЕС — 4%. Это заставляет компании инвестировать в безопасность не как в затраты, а как в необходимый

элемент бизнеса.

Борьба с дипфейками. В США и ЕС уже принимают законы, обязывающие маркировать контент, созданный с помощью ИИ. В России также обсуждаются поправки к закону «Об информации», которые запретят использование дипфейков без маркировки.

Глава 2. Современные вызовы и риски в цифровой среде

2.1. Рост цифровизации и проблема «слепого» согласия

Мы наблюдаем стремительную цифровизацию всех сфер жизни. Услуги банков, доставка еды, покупка билетов, общение с близкими — все это теперь происходит онлайн. Для оказания услуги сервисы неизбежно собирают персональные данные. Однако, чем больше данных, тем они ценнее и привлекательнее для злоумышленников и маркетологов.

Возникает естественное противоречие: сервисы заинтересованы в сборе максимального объема информации, а пользователи — в ее минимизации и контроле над ее использованием. Это противоречие усугубляется тем, что пользователи часто не имеют реального выбора: либо согласиться на все условия, включая сбор данных, либо отказаться от использования сервиса.

Ключевой проблемой является так называемое «слепое» согласие. Прежде чем начать пользоваться приложением, пользователь почти всегда вынужден нажать «Согласен» с политикой конфиденциальности. Однако мало кто читает этот многостраничный документ, написанный сложным юридическим языком.

Исследования показывают, что средний пользователь тратит на чтение политик конфиденциальности менее 1 минуты в год. В результате, пользователь автоматически соглашается на условия, которые могут быть крайне невыгодными для него, включая передачу данных десяткам «партнеров» и использование их в маркетинговых целях.

Это подрывает саму суть принципа информированного согласия. Пользователь формально соглашается, но фактически не понимает, на что он идет, что превращает его согласие в юридическую фикцию. Многие операторы намеренно делают политики сложными и длинными, чтобы пользователи их не читали.

Проблема усугубляется тем, что приложения часто запрашивают согласие на обработку данных не в момент установки, а потом, в процессе использования, когда пользователь уже вовлечен в работу с сервисом и менее склонен отказаться.

Например, приложение может запросить доступ к геолокации только тогда, когда пользователь уже заказал такси, и отказ в доступе сделает заказ невозможным. Это создаст психологическое давление на пользователя и фактически лишает его свободы выбора.

2.2. Избыточные разрешения и скрытый сбор данных

Ярким примером проблемы являются мобильные прило-

жения, запрашивающие доступ к функциям, абсолютно не нужным для их основной работы. В рамках нашего совместного с Роскачеством исследования мы выявили множество таких случаев.

Наиболее показательный пример — приложение-фонарик. Казалось бы, его задача — просто включать светодиод. Однако оно запрашивало доступ к контактам, микрофону, камере и другим данным. Очевидно, что эти данные собирались с иными целями, не связанными с основной функцией, что является прямым нарушением принципа минимизации данных.

Такие приложения, по сути, являются программами-шпионажами, которые под видом безобидного функционала похищают личную информацию. Это явление получило название «функциональная ползучесть» (function creep), когда данные, собранные для одной цели, начинают использоваться для других.

Другой громкий пример — приложение GetContact. Оно предлагает пользователям узнать, кто и как их записал в телефонной книге. На первый взгляд — безобидная и даже забавная функция. Однако для ее работы приложение фактически копирует всю записную книжку пользователя на свои серверы. И получается, что пользователь не просто делится своими контактами, но и раскрывает контакты всех своих друзей, родственников и коллег, которые зачастую не давали на это никакого согласия. Собранная база данных затем

может использоваться для массовых спам-обзвонov и других целей.

Этот случай ярко демонстрирует, как бизнес-модели могут вступать в конфликт с правом на неприкосновенность частной жизни и правами третьих лиц. В результате таких действий страдают не только сами пользователи, но и люди, которых нет в приложении, но чьи данные оказались в базе без их ведома. Такие приложения часто не уточняют, как долго будут храниться данные и будут ли они удалены после удаления приложения.

Особую проблему представляют приложения, которые собирают данные о поведении пользователя в фоновом режиме, даже когда приложение не активно. Например, некоторые приложения отслеживают геолокацию пользователя в фоне, чтобы анализировать его перемещения и показывать целевую рекламу. Это нарушает не только принцип минимизации, но и право на частную жизнь, так как пользователь не контролирует, когда и какие данные о нем собираются.

2.3. Передача данных третьим лицам как основной риск

Один из самых значительных рисков — это передача персональных данных третьим лицам. Политики конфиденциальности часто содержат пункты, позволяющие оператору передавать данные неограниченному кругу партнеров, подрядчиков и аффилированных лиц.

Зачастую эти третьи лица находятся за пределами России, что создает дополнительные риски в связи с различиями в правовых режимах защиты данных. Передача данных за рубеж требует отдельного согласия пользователя и соблюдения ряда условий, однако на практике этот процесс часто остается непрозрачным.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.