

Д. В. Гавчук

**Правовое
регулирование
защиты
персональных
данных
в гостиничной
индустрии
России и Китая**

Монография

Денис Гавчук

**Правовое регулирование
защиты персональных данных
в гостиничной индустрии
России и Китая. Монография**

«Издательские решения»

Гавчук Д. В.

Правовое регулирование защиты персональных данных
в гостиничной индустрии России и Китая. Монография /
Д. В. Гавчук — «Издательские решения»,

ISBN 978-5-00-694103-8

Монография посвящена изучению правовых аспектов защиты персональных данных в гостиничном бизнесе России и Китая. Основное внимание уделяется правовым нормам, регулирующим обработку персональных данных, их защите и применению в реальной практике гостиничного сектора. Монография предназначена для широкого круга читателей, включая юристов, менеджеров гостиничного бизнеса, преподавателей и исследователей, занимающихся вопросами защиты персональных данных.

ISBN 978-5-00-694103-8

© Гавчук Д. В.
© Издательские решения

Содержание

| | |
|------------------------------------------------------------------------------------------------------------|----|
| ВВЕДЕНИЕ | 6 |
| ГЛАВА 1. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСТИНИЧНОМ БИЗНЕСЕ | 8 |
| 1.1. Понятие и правовая природа персональных данных в российском и китайском законодательстве | 8 |
| 1.2. Нормативная база защиты персональных данных в гостиничном бизнесе России | 12 |
| 1.3. Особенности правового регулирования защиты персональных данных в гостиничном бизнесе Китая | 16 |
| Выводы по первой главе | 19 |
| ГЛАВА 2. ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСТИНИЧНОМ БИЗНЕСЕ РОССИИ И КИТАЯ | 20 |
| 2.1. Недостатки российского законодательства о защите персональных данных в контексте гостиничного сектора | 20 |
| Конец ознакомительного фрагмента. | 23 |

**Правовое регулирование защиты
персональных данных в гостиничной
индустрии России и Китая
Монография**

Денис Васильевич Гавчук

© Денис Васильевич Гавчук, 2026

ISBN 978-5-0069-4103-8

Создано в интеллектуальной издательской системе Ridero

ВВЕДЕНИЕ

Актуальность исследования. В условиях современного информационного общества вопрос защиты персональных данных становится особо актуальным. Гостиничный бизнес, являясь одной из ключевых отраслей сферы услуг, активно используют данные клиентов для:

- улучшения качества обслуживания;
- персонализации услуг;
- повышения конкурентоспособности. Но именно в этом контексте возникают значительные риски, связанные с утечками информации.

Сравнение правовых систем России и Китая также подчеркивает необходимость глубокого анализа тематического поля. Российская Федерация приняла Федеральный закон №152-ФЗ «О персональных данных», активно продолжая его модернизацию в условиях меняющегося международного правового поля. Параллельно этому, Китай ввел в действие с 2021 года Закон о защите персональной информации (Personal Information Protection Law, PIPL), вводящий строгие нормы обработки и хранения личной информации, что представляет значительный интерес для научных исследований в области информационной защиты и правоприменительной практики. Указанные два подхода к правовому регулированию могут иллюстрировать разные социальные особенности, определяющие подходы к защите данных.

Дополнительно, актуальность темы обостряется с учетом роста числа кибератак, связанных с утечками данных. Гостиницы, как организации, собирающие значительное количество личной информации клиентов, становятся привлекательными целями для злоумышленников. Именно это создает репутационную угрозу для бизнеса.

Перспективы правового регулирования в гостиничном бизнесе также заслуживают внимания. На фоне глобализации, усиления международного сотрудничества необходимо учитывать действующее законодательство, именно это послужит открытию новых горизонтов для гостиничного бизнеса повышая уровень защиты персональных данных.

Степень разработанности данной темы. В последние годы наблюдается рост интереса к вопросам защиты персональных данных в гостиничном бизнесе, большинство существующих исследований сосредоточено на общих аспектах законодательства о защите данных: Жириков И. К., Сычева М. И., Линь Д., Гун Н., Крюкова Д. Ю., Аджиева З. И., Ногайлиева М. Х., Кубанов М. Б., Попова Е. К., Моросанова А. А.. Сравнительные исследования между Россией и Китаем все еще недостаточно распространены. Специфика гостиничного бизнеса, который обрабатывает большой объем персональной информации, требует более детального изучения действующих правовых норм, а также препятствий, с которыми сталкиваются гостиничные предприятия.

Цель исследования. Анализ существующих проблем и перспектив развития правовых механизмов защиты персональных данных в гостиничном секторе двух стран.

Задачи исследования:

- изучить понятие и правовую природу персональных данных в российском и китайском законодательстве;
- рассмотреть нормативную базу защиты персональных данных в гостиничном бизнесе России;
- определить особенности правового регулирования защиты персональных данных в гостиничном бизнесе Китая;
- выявить недостатки российского законодательства о защите персональных данных в контексте гостиничного сектора;
- проанализировать вызовы китайского законодательства в области защиты персональных данных в гостиничном бизнесе;

- сравнить подходы к защите персональных данных в гостиничном бизнесе России и Китая;
- найти пути улучшения российского законодательства о защите персональных данных в гостиничном секторе;
- выявить направления модернизации китайского законодательства о защите персональных данных в гостиничном бизнесе;
- провести анализ международного сотрудничества в области защиты персональных данных.

Объект исследования – правовые отношения в сфере защиты персональных данных в гостиничном бизнесе.

Предмет исследования – нормы права, регулирующие защиту персональных данных в гостиничном бизнесе в России и Китае, практика их применения, теоретические разработки по теме исследования.

Методы исследования:

- обзор научной литературы;
- сравнительно-правовой метод;
- системный подход;
- статистический анализ;
- методы анализа документов и судебной практики.

Обзор научной литературы использовался для формирования теоретической базы исследования, выявления ключевых концепций и определения степени изученности темы в российской, китайской и международной доктрине.

Сравнительно-правовой метод выступил в качестве основного. Он был применен для детального сопоставления норм российского Федерального закона №152-ФЗ «О персональных данных» и китайского Закона о защите персональной информации (PIPL), а также подзаконных актов в сфере гостиничного бизнеса. Целью сравнения было выявление сходств, различий, достоинств и недостатков правовых моделей двух стран.

Системный подход позволил рассмотреть правовые механизмы защиты персональных данных не изолированно, а как часть целостной системы правового регулирования гостиничной деятельности, учитывая их взаимосвязь с нормами административного, гражданского, туристского права и техническими стандартами.

Статистический анализ был использован для обработки данных Роскомнадзора и китайских регуляторов о количестве и типах нарушений в сфере защиты данных, что позволило эмпирически подтвердить существующие пробелы и проблемы правоприменения.

Методы анализа документов и судебной практики включали изучение текстов законов, постановлений правительств, отраслевых стандартов, а также решений судов. Это дало возможность оценить не только формальные нормы, но и реальные механизмы их реализации и правоприменения.

Теоретическая значимость исследования заключается в комплексном сравнительно-правовом анализе двух различных правовых моделей регулирования защиты персональных данных в контексте гостиничного бизнеса. Работа вносит вклад в развитие доктрины информационного права, систематизируя и детализируя правовой режим персональных данных клиентов отелей.

Практическая значимость исследования состоит в том, что его выводы и рекомендации могут быть использованы законодательными органами России и Китая для совершенствования национального законодательства, субъектами гостиничного бизнеса (как российскими, так и международными сетями, работающими в Китае) для минимизации правовых рисков и выстраивания политики обработки данных.

ГЛАВА 1. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСТИНИЧНОМ БИЗНЕСЕ

1.1. Понятие и правовая природа персональных данных в российском и китайском законодательстве

Персональные данные включают всю информацию, позволяющую прямо или косвенно установить личность конкретного физического лица.¹ Данный термин является ключевым в сфере защиты данных и приватности, обладает юридическим значением в рамках нормативных актов, регулирующих защиту персональных данных, таких как Общий регламент о защите данных (GDPR)² Европейского Союза и аналогичные законодательные акты в иных государствах, включая Российскую Федерацию.

Идентифицируемым физическим лицом считается субъект, которого возможно однозначно определить прямым либо косвенным образом посредством таких сведений, как личные данные (имя, фамилия), уникальный идентификатор, координаты местонахождения, сетевые маркеры идентификации либо через совокупность признаков, характеризующих физические, биологические, генетические, психологические, экономические, культурные или социальные особенности индивида.

Так, обладая именем и фамилией гражданина, процесс установления его личности существенно упрощается. Однако даже в случаях, когда информация кажется менее явной, можно сделать выводы о личности, используя сочетания данных.

Основные аспекты, касающиеся персональных данных, охватывают два ключевых момента. Первый заключается в том, что персональные данные могут существовать как отдельно, так и в составе совокупных массивов информации. Так, отдельные сведения вроде возраста, пола или уровня дохода сами по себе кажутся недостаточно уникальными, однако в комбинации с прочими данными способны обеспечить идентификацию конкретной персоны. Второй аспект подразумевает включение в категорию персональных данных как очевидных элементов (таких как ФИО и контактные данные), так и скрытых характеристик (например, поведенческих шаблонов, используемых для формирования детального профиля человека).

Обработка персональных данных подчиняется жестким правилам, обязывающим организации соблюдать установленные нормы и стандарты.³ Компании должны уведомлять пользователей о порядке использования их личной информации и получать согласие на её сбор и обработку. Однако существуют многочисленные исключения и региональные особенности, усложняющие данную сферу.

¹ Китана, А. Н. А. Понятие и признаки персональных данных в российском праве / А. Н. А. Китана // Современная наука в условиях модернизационных процессов: проблемы, реалии, перспективы: Сборник научных статей по материалам VII Международной научно-практической конференции, Уфа, 12 января 2022 года. – Уфа: Общество с ограниченной ответственностью «Научно-издательский центр «Вестник науки», 2022. – С. 35—40. – EDN RXDSJS.

² Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27.04.2016 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 данных, GDPR) [Электронный ресурс]. URL: <https://gdpr-text.com/ru/> (дата обращения: 14.01.2026).

³ Батыгова, Г. Б. Защита персональных данных / Г. Б. Батыгова // Синергия Наук. – 2021. – №62. – С. 161—165. – EDN ITHRFC.

В настоящее время вопросы важности защиты прав на личные данные существенно обострились ввиду развития цифровых технологий, которые позволили существенным образом повысить качество обслуживания.

Понимание понятия «персональные данные» является основополагающим для всех, кто работает с информацией о физических лицах. Защита таких данных становится все более актуальной, поэтому знание прав и обязанностей, связанных с обработкой персональных данных, необходимо как для бизнеса, так и для пользователей.

Вопрос классификации персональных данных является важным, как в России, так и в Китае, поскольку эти страны имеют свои специфические законодательные рамки, касающиеся сбора, хранения и обработки данных о физических лицах. Давайте рассмотрим классификацию персональных данных в России и Китае более подробно.

В России основным нормативным актом, регулирующим вопросы, связанные с персональными данными, является Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»⁴. Закон четко определяет и классифицирует персональные данные, подразделяя их на несколько категорий, представленных в таблице 1.

Таблица 1 – Категории персональных данных в российском законодательстве

| № | Название | Описание |
|---|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Обычные персональные данные | Данные, которые не относятся к категории специальных. К ним относятся информация, идентифицирующая физическое лицо, например, имя, фамилия, дата рождения, адрес, контактная информация и другие идентификаторы. |
| 2 | Специальные категории персональных данных | К ним относятся данные, которые подлежат повышенной защите из-за их чувствительности. Это информация о расовой или национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, сексуальной жизни, а также биометрические данные (например, отпечатки пальцев, изображения лица и т. д.). Обработка таких данных допускается только в строго определенных случаях, например, с согласия субъекта или на основании закона. |
| 3 | Общие персональные данные | Информация, которая не относится к конкретному физическому лицу или не может быть использована для его дальнейшей идентификации. Важно отметить, что даже общие данные могли бы быть использованы в сочетании с другими источниками для определения личности, поэтому они должны обрабатываться с осторожностью. |

В последние годы китайское законодательство в области персональных данных ужесточилось, главным образом благодаря вступлению в силу 1 ноября 2021 года Закона о защите персональных данных. Этот документ вводит обязательную классификацию персональных данных и возлагает дополнительные обязанности на организации, осуществляющие их обработку.

⁴ Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (ред. от 24.06.2025) // СПС «КонсультантПлюс».

Таблица 2 – Категории персональных данных в КНР⁵

| № | Классификация | Описание |
|---|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Обычные персональные данные | Под понятие обычных персональных данных попадают все данные, которые могут идентифицировать личность пользователя, включая имя, идентификационный номер, адрес, телефонный номер и электронную почту. Организации обязаны защищать эти данные и обрабатывать их в соответствии с принципами законности, справедливости и прозрачности. |
| 2 | Специальные персональные данные | Как и в России, специальными данными в Китае считаются те, которые требуют особой защиты. К ним относятся биометрические данные, данные о состоянии здоровья, о сексуальной ориентации, расе и этнической принадлежности, а также информация, касающаяся личных финансов. Закон требует от организаций получить четкое согласие от пользователей на обработку таких данных. |
| 3 | Критически важные персональные данные | В соответствии с китайским законодательством существуют дополнительные требования для критически важных данных, которые требуют еще большего уровня защиты. Это данные, которые могут угрожать безопасности должностных лиц или национальной безопасности. Примеры могут включать данные, используемые в оборонной или правительственной сферах. |

Китайский закон о защите персональных данных ввёл ряд новых требований относительно передачи данных за рубеж, среди которых оценка возможных рисков и обеспечение аналогичного уровню китайского законодательства уровня защиты данных. Анализируя классификации персональных данных в России и Китае, можно выявить определённые сходства и различия. Оба государства выделяют общие и специальные категории данных, отражая стремление защитить наиболее важную личную информацию. Отличительная черта Китая заключается в усиленной охране критически значимых данных, что, вероятно, обусловлено специфическими соображениями национальной безопасности и государственной политики.

Законы обоих государств устанавливают обязательное условие получения согласия субъекта на обработку его персональных данных, однако Китай усиливает этот принцип дополнительными обязанностями организаций по информированию пользователей. Реализация этих положений существенно зависит от культурных, социальных и политических особенностей каждой страны. Компаниям, работающим в России и Китае, важно учитывать не только юридические нормы, но и национальные предпочтения населения в вопросах защиты частной информации. Хотя обе страны стремятся обеспечить конфиденциальность данных, различия в правовом регулировании представляют собой особые вызовы для бизнеса, действующего одновременно в двух юрисдикциях.⁶

Защита персональных данных имеет важнейшее значение для сохранения прав и свобод каждого гражданина. Основные принципы обработки персональных данных были сформу-

⁵ Политика обеспечения безопасности киберпространства: опыт китайской народной республики – <https://elibrary.ru/item.asp?id=39322163> – Дата просмотра 02.09.2025 г.

⁶ Сапронов, Д. Ю. Историческая ретроспектива правового регулирования персональных данных в некоторых странах / Д. Ю. Сапронов // Труды по интеллектуальной собственности. – 2022. – Т. 42, №3. – С. 26—31. – DOI 10.17323/tis.2022.15931. – EDN ULSYYW.

лированы в международных и национальных нормативных актах, включая Общий регламент по защите данных (GDPR) в Европейском Союзе и Закон о персональных данных в России.⁷ Проведем подробное рассмотрение этих принципов.

Первый принцип обработки данных гласит, что любые операции с персональными данными должны осуществляться правомерно, честно и прозрачно. Это означает, что работа с персональными данными должна осуществляться в полном соответствии с законодательством.

Действия организации должны строго соответствовать принципу целевого ограничения. Сбор и использование персональных данных допустимы исключительно для заранее определенных целей. Использование информации для иных задач (например, применение контактных данных, полученных для бронирования номера, в маркетинговых рассылках) без отдельного разрешения субъекта является нарушением.

В целях минимизации потенциальных рисков утечек и несанкционированного доступа применяется принцип минимизации данных. Он требует ограничивать объем собираемой информации для достижения заявленных целей.

Принцип ограничения хранения предписывает сохранять персональные данные не дольше, чем это требуется для выполнения целей обработки. По истечении установленных сроков информация должна быть удалена или обезличена. Для практической реализации данного принципа организациям необходимо закреплять конкретные сроки хранения для каждого типа данных во внутренних регламентах.

Таким образом, персональные данные в российском и китайском законодательстве представляют собой любую информацию, позволяющую идентифицировать физическое лицо, при этом обе юрисдикции выделяют обычные и специальные категории данных, требующие различного уровня защиты. Обработка персональных данных в обеих странах основывается на универсальных принципах законности, минимизации, точности и безопасности, что отражает общемировую тенденцию к усилению защиты конфиденциальности граждан в цифровую эпоху.

⁷ Моросанова А. А. Усиление регулирования защиты персональных данных в России: экономические последствия и риски // Управленец. 2023. №5. URL: <https://cyberleninka.ru/article/n/usilenie-regulirovaniya-zaschity-personalnyh-dannyh-v-rossii-ekonomicheskie-posledstviya-i-riski> (дата обращения: 02.09.2025).

1.2. Нормативная база защиты персональных данных в гостиничном бизнесе России

Защита персональных данных в гостиничном бизнесе России регламентируется несколькими основными нормативно-правовыми актами, которые устанавливают требования к обработке, хранению и защите личной информации гостей. Важнейшими из них являются:⁸

В России основным документом, устанавливающим требования защиты персональных данных, является **Конституция РФ**, где декларируется право каждого человека на неприкосновенность частной жизни.

Трудовой кодекс РФ прописывает, что все персональные данные сотрудников, их объем, хранение и распространение используются только в целях исполнения законодательства и осуществления трудовых обязанностей.

Гражданский кодекс РФ посвящает охране частной жизни гражданина статью 152.2.

Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» устанавливает конкретные правила получения, обработки, использования и хранения персональных данных.⁹

Федеральный закон №152-ФЗ «О персональных данных», введенный в действие 26 января 2007 года, служит фундаментальным нормативно-правовым документом в области защиты приватной информации граждан Российской Федерации. Данный акт закрепляет ключевые понятия и принципы обращения с персональными данными, обозначает права лиц, чьи данные подвергаются обработке, а также фиксирует обязанности тех субъектов хозяйствования и государственных органов, которые занимаются обработкой указанной информации.

Документ раскрывает базовые концепции и подходы, представленные следующим образом.¹⁰

Во-первых, определяется само понятие персональных данных, включающее любую информацию, позволяющую прямо или косвенно установить личность физического лица. Примеры подобной информации охватывают ФИО, адреса проживания, контактные телефоны, электронные почтовые адреса и прочие идентификационные признаки.

Кроме того, выделяются важные принципы, регулирующие порядок обработки персональных данных:

– Любые действия с персональными данными должны совершаться в рамках существующего правового поля и с соблюдением интересов и прав самих владельцев данных.

– Цель сбора и последующей обработки данных должна быть установлена заранее и носить юридически обоснованный характер.

– Сбор и обработка данных ограничивается только теми случаями, когда такая информация действительно необходима для достижения заявленных целей.

– Операторы обязаны обеспечивать актуальность и точность персональных данных.

– Персональные данные должны защищаться от несанкционированного доступа.

Согласно закону, субъекты персональных данных обладают рядом прав, включая:

– Право на доступ к своим данным.

– Право на исправление недостоверных данных.

⁸ Крюкова Д. Ю., Мокрецов Ю. В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2017. №2 (38). URL: <https://cyberleninka.ru/article/n/aktualnye-problemy-pravovogo-regulirovaniya-oborota-i-zaschity-personalnyh-dannyh-v-rossii> (дата обращения: 02.09.2025).

⁹ Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (ред. от 24.06.2025) // СПС «КонсультантПлюс».

¹⁰ Сычева М. И. Проблемы правового регулирования защиты персональных данных в сети интернет // Международный журнал гуманитарных и естественных наук. 2022. №10—3. URL: <https://cyberleninka.ru/article/n/problemy-pravovogo-regulirovaniya-zaschity-personalnyh-dannyh-v-seti-internet> (дата обращения: 02.09.2025).

- Право на отзыв согласия на обработку данных.
- Право на уничтожение данных, обработка которых была осуществлена незаконно.

Операторы, обрабатывающие персональные данные, несут определенные обязательства, среди которых:

- Обеспечение безопасности обрабатываемых данных.
- Заключение с третьими лицами договоров на передачу персональных данных.

Для регламентации рассматриваемых общественных отношений помимо Федерального закона №152-ФЗ¹¹ применяются иные правовые акты:

Постановление Правительства РФ №1119 от 1 ноября 2012 года, которое вводит правила обработки персональных данных в информационных системах и предъявляет требования к их защите. Этот акт является значимым для операторов, использующих информационные технологии, так как предусматривает конкретные технические и организационные мероприятия по обеспечению безопасности данных.

Федеральный закон №126-ФЗ от 7 июля 2003 года «О связи», регулирующий процессы обработки данных, относящихся к телефонной и интернет-коммуникациям. Закон детально описывает права и обязанности операторов связи в части защиты персональных данных пользователей.

Все вышеперечисленные акты образуют комплексную нормативную базу, определяющую правила обработки персональных данных в России. Она требует от организаций не только соблюдения законных требований, но и внедрения эффективных систем защиты данных, что, в свою очередь, помогает обеспечить доверие пользователей и минимизировать правовые риски в процессе обработки информации.

Стоит отметить, что с учетом развития технологий и изменения подходов к проблемам защиты данных, в России обсуждаются и принимаются новые поправки в законодательство, что требует от компаний постоянного мониторинга актуальных изменений и своевременной корректировки своих процессов в соответствии с новыми требованиями.

Вторым важным документом можно считать Федеральный закон от 6 апреля 2011 года №63-ФЗ «Об электронной подписи»¹², который устанавливает правила использования электронной подписи. Указанное имеет значение в гостиничном бизнесе, особенно с учётом растущей популярности онлайн-бронирования и оплаты, что требует защиты данных клиентов. Применение законодательства о защите персональных данных в гостиничном бизнесе представляет собой значимую тему, требующую детального изучения как юридической, так и практической составляющей. С ростом технологических возможностей и расширением объемов обрабатываемой информации эта проблема приобрела особую актуальность в последние годы.

Гостиничные предприятия, оказывая услуги временного размещения гостей, осуществляют обработку значительных массивов персональных данных, включающих фамилии, имена, отчества, контакты, паспортные данные, информацию о платежах и иные сведения, способные однозначно идентифицировать конкретного клиента. Таким образом, гостиницы несут обязательство соблюдать требования законодательства, направленные на обеспечение сохранности и конфиденциальности предоставляемых ими данных.

Особое внимание следует уделить процессу получения согласия на обработку персональных данных. Гостиницам необходимо создавать и внедрять эффективные механизмы фиксации подобного согласия. Обычно это реализуется путем внесения соответствующей графы в регистрационную форму, где клиент ставит свою подпись или подтверждает свое согласие отметкой («галочкой»). Помимо этого, обязательным условием является предоставление возможности клиенту отозвать данное согласие в любое удобное для него время.

¹¹ Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (ред. от 24.06.2025) // СПС «КонсультантПлюс».

¹² Федеральный закон «Об электронной подписи» от 06.04.2011 №63-ФЗ (ред. от 21.04.2025) // СПС «КонсультантПлюс».

Значимым элементом выступает внутренняя организационная структура гостиниц в части обработки и защиты персональных данных. Для обеспечения необходимой степени безопасности необходимо разработать внутренние корпоративные правила и инструкции. Работников отелей следует систематически обучать вопросам правильного обращения с персональной информацией, минимизировать вероятность случаев её незаконного распространения. В случае возникновения нарушений конфиденциальности администрация заведения обязана оперативно сообщать об инциденте клиентам и соответствующим государственным органам, соблюдая предусмотренный законодательством порядок действий. Для усиления защитных механизмов целесообразно использовать новейшие криптографические инструменты, особенно при онлайн-заказах номеров, сопровождающихся обработкой платёжных реквизитов и иных высокочувствительных данных. Целесообразно также внедрить специализированные программы и методики, обеспечивающие контроль доступа к конфиденциальной информации, позволяющий пользоваться ею только уполномоченным сотрудникам, которым это необходимо для выполнения должностных обязанностей.¹³

При нарушении требований законодательства отель подвергается ряду серьёзных юридических рисков и негативных последствий, таких как штрафные санкции и ухудшение деловой репутации. Следует помнить, что потерпевший от неправомерного использования своих данных клиент вправе обратиться в судебные инстанции с требованием компенсации понесённого ущерба.

Гостиницы должны быть уверены, что эти организации также соблюдают нормы законодательства о защите персональных данных и имеют адекватные меры безопасности.

Практика применения законодательства о защите персональных данных в гостиницах показывает, что соблюдение этих норм не только является правовой необходимостью, но и повышает уровень доверия клиентов. Четкая политика конфиденциальности и надежная система защиты персональных данных способны стать весомым конкурентным фактором для отелей в современных рыночных условиях. Предприятия, обеспечивающие высокий уровень безопасности личных сведений клиентов, получают не только возможность избежать юридических санкций, но и формируют устойчивое доверие среди потребителей, что благоприятствует успешному развитию бизнеса в длительной перспективе.¹⁴

Роскомнадзор, официальное название которого звучит как Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, выступает важнейшим регулятором в области коммуникации и информации в России. Созданная для защиты прав граждан, обеспечения информационной безопасности и контроля над исполнением законов в областях связи, цифровых технологий и массовой информации, эта структура решает ключевые задачи, среди которых регулирование соблюдения законодательства о связи, защита прав потребителей информационных сервисов и гарантия свободного доступа населения к необходимой информации. Важнейшими функциями Роскомнадзора являются:

Осуществление мониторинга и контроля за содержанием интернет-ресурсов. Роскомнадзор следит за тем, чтобы информация, распространённая в интернете, соответствовала закону и не содержала запрещённых материалов, таких как детская порнография, экстремистские материалы и информация, угрожающая безопасности государства. Служба занимается регулированием деятельности операторов связи. Это включает в себя лицензирование операторов,

¹³ Жириков, И. К. Перспективы развития гостиниц, свободных от персонала / И. К. Жириков // Туристский сезон 2021: проблемы и перспективы: Материалы научно-практического on-line форума, Севастополь, 02 апреля 2021 года / Под научной редакцией И. С. Кусова, Н. В. Шабалиной, Р. Р. Тимиргалеевой. – Майкоп: ООО «Электронные издательские технологии», 2021. – С. 121—123. – EDN SBQFLE.

¹⁴ Жириков, И. К. Перспективы развития гостиниц, свободных от персонала / И. К. Жириков // Туристский сезон 2021: проблемы и перспективы: Материалы научно-практического on-line форума, Севастополь, 02 апреля 2021 года / Под научной редакцией И. С. Кусова, Н. В. Шабалиной, Р. Р. Тимиргалеевой. – Майкоп: ООО «Электронные издательские технологии», 2021. – С. 121—123. – EDN SBQFLE.

контроль за качеством предоставляемых ими услуг и защиту прав потребителей. По мере того, как телекоммуникации и интернет прочно вошли в повседневную жизнь общества, возрастает значимость роли Роскомнадзора в создании равных условий для провайдеров и пользователей.

Одно из приоритетных направлений работы службы – надзор за исполнением законодательства о защите персональных данных. Рост масштабов цифрового оборота информации, особенно в сегменте онлайн-платформ и соцсетей, обуславливает необходимость постоянного мониторинга соблюдения организациями требований по обеспечению безопасности личной информации граждан. Дополнительно Роскомнадзор осуществляет реализацию государственной стратегии в области технологического развития и коммуникации. Служба инициирует проекты и мероприятия, ориентированные на модернизацию инфраструктуры, внедрение передовых технических решений и развитие цифровой экономики страны.

Значимой частью деятельности службы является совершенствование информационных систем, содействующих реализации гражданских прав и повышению открытости органов власти.

Дополнительно Роскомнадзор осуществляет мероприятия по киберзащите, взаимодействуя с иными органами исполнительной власти для обороны жизненно важной информационной инфраструктуры страны от хакерских атак и иных видов цифрового вмешательства. Деятельность ведомства направлена на достижение баланса между прогрессом цифровых коммуникаций и обеспечением законных интересов граждан.

Таким образом, нормативная база защиты персональных данных в гостиничном бизнесе России представляет собой систему правовых актов, основу которой составляет Федеральный закон №152-ФЗ «О персональных данных», дополненный специализированными постановлениями и законами, регулирующими электронный документооборот и информационную безопасность. Реальное воплощение данного законодательства предполагает, что гостиничный сектор обязан официально соблюдать требования, касающиеся получения согласия на обработку данных и обеспечения их безопасности, а также организовывать внутренние системы защиты информации, находящиеся под надзором Роскомнадзора.

1.3. Особенности правового регулирования защиты персональных данных в гостиничном бизнесе Китая

«Закон о кибербезопасности», утвержденный Китаем в 2016 году, заложил основу для формирования правового фундамента, направленного на укрепление национальной безопасности и регулирование киберпространства. Документ охватывает разнообразные направления, начиная от информационной безопасности и сетевого администрирования, заканчивая защитой персональных данных граждан. Важнейшей целью закона является установление эффективного контроля над сетевыми инфраструктурами, включая введение обязательных требований к операторам критически важной информационной инфраструктуры (КИИ). Эти операторы обязаны предпринимать меры по повышению безопасности и осуществлять отчетность о состоянии сети.¹⁵

Данный закон затрагивает целый комплекс важнейших вопросов. Во-первых, он требует от организаций и компаний, работающих в Китае, устанавливать системы защиты данных и обеспечивать защиту сетевой инфраструктуры от киберугроз.¹⁶

Во-вторых, закон требует, чтобы данные, которые считаются «чувствительными» или «критическими», хранились на территории Китая и могли быть доступны для государственных органов при необходимости.

Наряду с Законом «О кибербезопасности», существуют и другие важные нормативные акты, затрагивающие рассматриваемую сферу. Одним из них является Закон о личных данных 2021 года, который закрепляет порядок сбора, хранения и обработки соответствующей информации.

Большое значение также имеет такой нормативный правовой акт, как Закон о противодействии кибершпионажу и киберпреступности, который предусматривает юридические основания для проведения расследований в сети Интернет, связанные с незаконным использованием данных.

Стоит упомянуть о различных инструкциях и предписаниях, которые издает министерство промышленности и информационных технологий Китая (МИИТ), регулируя более детализированные вопросы, касающиеся технологий и стандартов в сфере кибербезопасности.¹⁷

Все эти законодательные акты формируют комплексную правовую систему, которая значительно усиливает контроль со стороны государства в области кибербезопасности, устанавливает строгие стандарты для обработки личных данных и направлена на создание безопасного цифрового пространства. В то же время такие меры также вызывают предупреждения о возможности чрезмерного контроля и ограничения свободы слова, что стало предметом критики со стороны международных правозащитных организаций.

Система управления персональными данными в китайской гостиничной индустрии представляет значительный исследовательский интерес, поскольку изучается, каким образом отрасль собирает, сохраняет и обеспечивает защиту информации о гостях. В свете растущих

¹⁵ Попова Е. К. Правовая защита личной информации: опыт китайской народной республики // Наука. Общество. Государство. 2024. №2 (46). URL: <https://cyberleninka.ru/article/n/pravovaya-zaschita-lichnoy-informatsii-opyt-kitayskoy-narodnoy-respubliki> (дата обращения: 02.09.2025).

¹⁶ Линь До Правовое регулирование защиты персональных данных и их контроль со стороны государства в Китае // Политика и общество. 2020. №2. URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-zaschity-personalnyh-dannyh-i-ih-kontrol-so-storony-gosudarstva-v-kitae> (дата обращения: 02.09.2025).

¹⁷ Гун Н. Защита персональных данных в Китае: законодательство в цифровую эпоху // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14. №1. С. 159—172. URL: <https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-kitae-zakonodatelstvo-v-tsifrovuyu-epohu> (дата обращения: 02.09.2025).

регуляторных требований в сфере кибербезопасности и охраны частных данных китайские отели внедряют усовершенствованные процедуры и стандарты обработки информации.

Сначала отели получают необходимую информацию о посетителях на стадии бронирования, такую как имена, контактные данные, паспортные сведения, пожелания по проживанию и платежные реквизиты. Такая информация используется для оформления заказов и оказания качественных услуг. Одновременно с этим возникает потребность в защите этих данных от нелегального доступа и кражи, что достигается применением современных инструментов безопасности и шифрования.

Так, в 2022 году произошла крупная утечка примерно 1,5 млрд записей из платформ Weibo, DiDi и Компартии Шанхая.

В июне 2025 года специалисты портала Cybernews зафиксировали ещё одну крупную утечку данных объемом около 4 млрд финансовых записей, включая информацию из сервисов WeChat и Alipay, общий размер массива составил 631 ГБ.

Ещё одним ключевым моментом является соответствие Закону о защите персональных данных (PIPL), ставшему обязательным с ноября 2021 года. Согласно данному закону, отели обязаны заручиться согласием гостей на обработку их данных, предоставлять им доступ к собственным сведениям и возможность удалить их.

Сотрудники гостиничного сектора должны постоянно совершенствовать знания в сфере информационной безопасности, осознавая высокую ценность личной информации клиентов и методы предотвращения потенциальных угроз. Управление персональными данными в китайских отелях представляет собой сложную многоступенчатую систему, включающую выполнение законодательных норм, внедрение современных технологий и специализированное обучение работников, нацеленное на повышение надёжности и конфиденциальности информации о гостях.

На международном уровне, наиболее известным актом, регулирующим защиту данных, является Общий регламент по защите данных (GDPR) Европейского Союза. Данный нормативно-правовой акт вводит жесткие правила обработки персональных данных и значительные штрафы за их нарушение.¹⁸ Штрафы могут достигать до 20 миллионов евро или 4% от годового оборота компании, в зависимости от того, что больше. К тому же GDPR устанавливает права субъектов данных, позволяя им требовать доступ к своим данным, их исправление или даже удаление.

Несоблюдение правил обработки и защиты данных грозит юридическим лицам не только финансовыми потерями, но и серьезными репутационными рисками, способными нанести долгосрочный ущерб бизнесу. Утрата или несанкционированное использование информации способна подорвать доверие клиентов и партнёров, что приведет к значительным отрицательным последствиям для компании.

Помимо внешнего регулирования, многие организации вводят внутренние инструкции и процедуры по защите данных. Работодатели могут наказывать сотрудников, нарушивших правила обработки персональных данных, вплоть до расторжения трудового договора. Нарушения принципов защиты данных приводят не только к юридическим последствиям, но и вызывают значительные этические проблемы, связанные с нарушением прав и интересов клиентов.

В современной цифровой среде грамотное обращение с персональной информацией превращается из простого юридического обязательства в неотъемлемый элемент успешной деловой

¹⁸ Аджиева З. И., Ногайлиева М. Х., Кубанов М. Б. Актуальные аспекты правового регулирования защиты персональных данных // Этносоциум и межнациональная культура. 2023. №185. URL: <https://cyberleninka.ru/article/n/aktualnye-aspekty-pravovogo-regulirovaniya-zaschity-personalnyh-dannyh> (дата обращения: 02.09.2025).

вой практики, непосредственно связанный с поддержанием положительной репутации предприятия и стабильностью его развития.

Таким образом, правовое регулирование защиты персональных данных в гостиничном бизнесе Китая основывается на комплексной системе законодательных актов, включающей Закон о кибербезопасности 2016 года и Закон о личных данных 2021 года, которые устанавливают строгие требования к сбору, хранению и обработке клиентской информации с обязательным размещением критических данных на территории страны.

Практическая реализация данного законодательства в отелях требует внедрения современных CRM-систем, получения согласия клиентов на обработку данных, обучения персонала основам информационной безопасности и назначения ответственных за защиту данных сотрудников.

Выводы по первой главе

Первая глава посвящена изучению правовых основ защиты персональных данных в гостиничном бизнесе России и Китая.

Персональные данные определяются как любая информация, связанная с физическим лицом, которую можно прямо или косвенно идентифицировать.

В российском и китайском законодательстве выделяется две основные категории данных: обычные и специальные, каждая из которых требует разного уровня защиты.

Существуют сходства в определении персональных данных и подходов к их защите, но наблюдаются принципиальные различия в уровнях защиты и подходах к трансграничной передаче данных.

Основное нормативное регулирование обеспечивается Федеральным законом №152-ФЗ «О персональных данных», который распространяется на всю территорию России.

Отдельные законодательные акты регулируют обработку данных в области связи, труда и торговли.

Несмотря на существование общих правовых актов, гостиничный сегмент сталкивается с недостатком узконаправленных стандартов и подробного регулирования, что затрудняет эффективное обеспечение защиты данных.

Правовая база Китая представлена тремя основными законами: Законом о кибербезопасности, Законом о защите персональных данных и Законом о безопасности данных. Подход Китая характеризуется повышенной ориентацией на национальную безопасность и общественные интересы, выражающейся в строгих правилах локализации данных и усиленном государственном контроле. Особенности гостиничного дела заключаются в применении уникальных национальных документов и цифровых платформ, позволяющих отслеживать перемещение и активность туристов.

Ключевыми проблемами остаются отсутствие ясных стандартов обработки данных, низкая эффективность контролирующих механизмов и сложности в соблюдении прав субъектов данных. Перспективные пути улучшения ситуации включают создание специализированных отраслевых стандартов, усиление ответственности операторов и расширение международного взаимодействия.

Таким образом, первая глава обозначает ключевые аспекты правового регулирования защиты персональных данных в гостиничном бизнесе России и Китая, раскрывая сходства и различия в подходах, а также выделяя основные проблемы и направления совершенствования.

ГЛАВА 2. ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСТИНИЧНОМ БИЗНЕСЕ РОССИИ И КИТАЯ

2.1. Недостатки российского законодательства о защите персональных данных в контексте гостиничного сектора

В российском законодательстве о защите персональных данных существует серьезный пробел, связанный с отсутствием специализированных стандартов обработки персональных данных для гостиничной индустрии. Данный недостаток создает множественные проблемы как для операторов данных, так и для субъектов персональных данных.

Федеральный закон №152-ФЗ «О персональных данных» устанавливает общие принципы и требования к обработке персональных данных, однако не учитывает специфику различных отраслей экономики. Гостиничный сектор характеризуется особыми условиями сбора, хранения и использования персональных данных, которые не находят должного отражения в действующем правовом регулировании.¹⁹

Отсутствие отраслевых стандартов и недостаточная конкретизация требований к обработке персональных данных в гостиничной сфере находят свое отражение в статистике административных правонарушений. Анализ данных Роскомнадзора о выявленных нарушениях в сфере обработки персональных данных за период 2019—2024 гг. демонстрирует масштабы проблемы правоприменения действующего законодательства (см. приложение 1).

Представленные данные свидетельствуют о волнообразной динамике выявленных административных правонарушений в сфере защиты персональных данных. Несмотря на значительное снижение количества зафиксированных нарушений в период 2020—2022 гг. (что может быть связано с ограничениями контрольно-надзорной деятельности в период пандемии), с 2023 года наблюдается устойчивый рост числа выявленных правонарушений.

Динамика административных правонарушений в сфере обработки персональных данных в Российской Федерации в 2019—2024 гг. отражена в приложении 1.²⁰

Увеличение количества нарушений в 2023—2024 гг. на 76% по сравнению с минимальными показателями 2022 года указывает на системные проблемы в сфере обеспечения защиты персональных данных.

Согласно исследованию экспертно-аналитического центра ГК InfoWatch, в 2024 году наблюдалось существенное увеличение масштабов компрометации персональных данных в российских организациях. Общий объем скомпрометированных записей составил 1,581 млрд единиц, что на 30% превышает показатели 2023 года (1,202 млрд записей).

При этом количество зарегистрированных инцидентов возросло незначительно — с 569 до 592 случаев. Наибольшую долю утечек (29%) составляет аутентификационная информация, включающая пароли, логины и контактные данные пользователей. Ведущую позицию по количеству инцидентов занимает торговая сфера (35,1% случаев компрометации ПДн), за которой следуют государственные органы (18%) и телекоммуникационная отрасль (9,8%).

¹⁹ Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ (ред. от 24.06.2025) // СПС «КонсультантПлюс».

²⁰ Судебная статистика РФ. Административные правонарушения. Показатели по отдельным правонарушениям [Электронный ресурс]. — URL: <https://stat.xn--7sbqk8achja.xn--p1ai/stats/adm/t/31/s/1> (дата обращения: 02.09.2025)

Значительную угрозу представляют внутренние нарушители, на долю которых приходится 18,5% всех инцидентов, при этом 98% таких действий носят умышленный характер²¹.

Анализ судебной практики по защите персональных данных потребителей за 2019—2024 годы демонстрирует устойчивую тенденцию к усилению защиты прав субъектов персональных данных и формированию единообразной правоприменительной практики контролирующими и судебными органами.

В сфере финансовых услуг судебная практика выявила системные нарушения требований законодательства о персональных данных. Показательным является дело, рассмотренное Арбитражным судом города Санкт-Петербурга и Ленинградской области от 30.07.2020 по делу № А56—25130/2020²², подтвержденное Постановлением Тринадцатого арбитражного апелляционного суда от 25.11.2020 №13АП-21818/2020, 13АП-22245/2020. Суды установили, что включение в кредитный договор условий, при которых одна подпись заемщика одновременно подтверждает согласие с условиями договора и согласие на обработку персональных данных, является недопустимым и противоречит положениям Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных». Данная правовая позиция основывается на принципе осознанности и добровольности согласия субъекта персональных данных на их обработку.

Проблема избыточного срока хранения персональных данных получила развитие в постановлении Арбитражного суда Московского округа от 03.10.2022 по делу № А40—12838/2022²³. Судебная коллегия подтвердила законность привлечения кредитной организации к административной ответственности по части 2 статьи 14.8 КоАП РФ за установление в договоре 10-летнего срока обработки персональных данных после прекращения обязательств, что было признано завышенным и не подтвержденным конкретными целями обработки.

Транспортная сфера продемонстрировала особую проблематику в контексте передачи персональных данных неопределенному кругу третьих лиц. Решение Арбитражного суда Новосибирской области от 01.06.2021 по делу № А45—6560/2021²⁴, поддержанное постановлением Седьмого арбитражного апелляционного суда от 05.08.2021 и постановлением Арбитражного суда Западно-Сибирского округа от 26.10.2021 № Ф04—5462/2021, признало незаконным включение в договор с потребителем положений о возможности передачи персональных данных непоименованным третьим лицам.

Жилищно-коммунальная сфера характеризуется особой сложностью правоотношений по обработке персональных данных. Постановление Арбитражного суда Уральского округа от 23.01.2023 № Ф09—10171/22 по делу № А60—27757/2022²⁵ подтвердило нарушение

²¹ Количество слитых персональных данных в 2024 году выросло на треть [Электронный ресурс]. – URL: <https://www.infowatch.ru/company/presscenter/news/kolichestvo-slitikh-personalnykh-dannykh-v-dve-tysyachidvadtsat-chetvertom-godu-vyroslo-na-tret> (дата обращения: 02.09.2025).

²² Решение от 30 июля 2020 г. по делу № А56—25130/2020 [Электронный ресурс]. – URL: https://sudact.ru/arbitral/doc/3zswxVFepf5N/?arbitral-txt=&arbitral-case_doc=%D0%9056-25130%2F2020&arbitral-lawchunkinfo=&arbitral-date_from=&arbitral-date_to=&arbitral-region=&arbitral-court=&arbitral-judge=&_=1751395123695&snippet_pos=8#snippet (дата обращения: 02.09.2025).

²³ Постановление от 3 октября 2022 г. по делу № А40—12838/2022 [Электронный ресурс]. – URL: https://sudact.ru/arbitral/doc/5ZoVvZpRixNC/?arbitral-txt=&arbitral-case_doc=%D0%9040-12838%2F2022&arbitral-lawchunkinfo=&arbitral-date_from=&arbitral-date_to=&arbitral-region=&arbitral-court=&arbitral-judge=&_=1751394958321 (дата обращения: 02.09.2025).

²⁴ Решение от 1 июня 2021 г. по делу № А45—6560/2021 [Электронный ресурс]. – URL: https://sudact.ru/arbitral/doc/97MIujFdZoWz/?arbitral-txt=&arbitral-case_doc=%D0%9045-6560%2F2021&arbitral-lawchunkinfo=&arbitral-date_from=&arbitral-date_to=&arbitral-region=&arbitral-court=&arbitral-judge=&_=1751395441960 (дата обращения: 02.09.2025).

²⁵ Постановление от 23 января 2023 г. по делу № А60—27757/2022 [Электронный ресурс]. – URL: https://sudact.ru/arbitral/doc/qIashpmrgHVq/?arbitral-txt=&arbitral-case_doc=%D0%9060-27757%2F2022&arbitral-lawchunkinfo=&arbitral-date_from=&arbitral-date_to=&arbitral-region=&arbitral-

газоснабжающей организацией требований частей 3 статьи 6, частей 1, 4 статьи 9 Федерального закона «О персональных данных» при включении в акт сдачи-приемки работ положения об автоматическом согласии заказчика на обработку персональных данных. Постановление Второго кассационного суда общей юрисдикции от 02.06.2020 по делу №16—3231/2020 выявило нарушения в сфере водоснабжения, связанные с поручением обработки персональных данных третьим лицам без обеспечения должной защиты информации.

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.