Гавчук Д.В.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.80.72-83
УДК: 34.347

Доверие и добросовестность в обороте персональных данных в отельном бизнесе: юридический анализ и практические рекомендации

Аннотация: Сегодняшняя эпоха, характеризующаяся стремительным развитием информационных технологий и активным вовлечением общества в виртуальное пространство, создает особые вызовы в сфере оборота персональных данных. Особенно актуально данная проблема встаёт в контексте гостиничного бизнеса, где объемы обрабатываемой информации достигают значительных масштабов. Основной целью данной статьи является комплексное исследование механизмов защиты персональных данных, построение системы доверия и формирование добросовестного поведения участников рыночных отношений в гостиничном сегменте. Анализ проводится на стыке правовых, психологических и социально-экономических дисциплин, позволяя выявить недостатки существующей системы и предложить научно-обоснованные пути её модернизации.

Ключевые слова: персональные данные; информационная безопасность; доверие; добросовестность; отельный бизнес.

I. Историко-теоретические аспекты оборота персональных данных

1. История становления права на конфиденциальность

Главное в современном цифровом мире – доверие.
Нам нужен новый нормативно-правовой климат,
без которого невозможно применение инновационных технологий.
Сатья Наделла, генеральный директор Microsoft [23]

Исторически, право на тайну личной жизни зародилось ещё в Древних Афинах и Риме, где оно считалось важным элементом социальной справедливости. Позже в европейских странах идея права на частную жизнь получила свое выражение в Конституции Франции XVIII века и Билле о правах США XIX века. В XX веке появляется концепция права на человеческое достоинство, признанная международными конвенциями и декларациями, среди которых Всеобщая декларация прав человека 1948 года и Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 года.

2. Понятие персональных данных и принцип добросовестности

Термином «персональные данные» обозначается любая информация, связанная с физическим лицом, позволяющая однозначно установить его личность. Поскольку данные обладают особым статусом, необходима специальная защита, обеспечивающая неприкосновенность и сохранение личных сведений. Принцип добросовестности в данном контексте предполагает исполнение участниками оборота данных прав и обязанностей, основанных на принципе добропорядочного поведения и отсутствия корысти [9].

♦ **Гавчук Денис Васильевич** - PhD (экономика), магистр права и магистр международных отношений (Швейцария), профессор Региональной академии менеджмента, член Федерации рестораторов и отельеров (Российская Федерация). E-mail: midk@bk.ru

В теории гражданского права существуют разные подходы к принципу добросовестности, одни ученые считают его субстанциональным элементом гражданской добродетели, другие видят в нём инструмент борьбы с недобросовестными действиями. Исходя из нашего контекста, представляется верным считать, что принцип добросовестности выступает главным регулятором оборота персональных данных, гарантирующим баланс интересов сторон [16].

3. Субъекты оборота персональных данных

Основными субъектами оборота персональных данных являются: отель (оператор данных), сам гость (субъект данных) и государственные органы, выполняющие контрольные функции. Каждому участнику отводится своя роль в цепочке обработки данных, соответственно формируются индивидуальные обязанности и права. Особенностью отельного бизнеса является высокая интенсивность оборота данных, разнообразие источников их поступления и большой объем обрабатываемой информации.

II. Правовые рамки оборота персональных данных в России

1. Законодательство Российской Федерации

Система защиты персональных данных в России представлена множеством нормативных актов различного уровня. Основным документом является Федеральный закон № 152-ФЗ «О персональных данных», принятый в июле 2006 года. Данный закон установил четкий перечень объектов и субъектов права, перечислил основные принципы и предоставил органам исполнительной власти полномочия по контролю за исполнением норм [1].

Особое внимание заслуживает пункт 5 статьи 6 указанного Закона, согласно которому допускается обработка персональных данных без согласия субъекта, если это необходимо для исполнения договора, стороной которого является субъект данных. Таким образом, сбор данных о клиентах осуществляется автоматически при заключении договора на оказание гостиничных услуг.

Помимо федерального закона, большое значение имеют подзаконные акты, разработанные различными министерствами и ведомствами.

2. Механизм правового регулирования

Нормативные акты создают достаточно разветвленную систему правового регулирования, включающую прямые предписания и диспозитивные нормы. Центральным звеном этой системы является обязанность сообщать клиентам обо всех фактах обработки данных, разъяснять цель и пределы их использования, получать соответствующее согласие и предупреждать о последствиях отказа предоставить необходимые сведения.

Применяемый механизм санкционирования также эффективен. За нарушение норм предусмотрена административная ответственность в виде штрафных санкций, предусмотренных КоАП РФ, а также гражданско-правовая ответственность в форме возмещения убытков и компенсации морального вреда.

III. Международные стандарты защиты персональных данных

1. Европейский опыт

Европа известна своим высоким уровнем защиты персональных данных. Одним из значимых достижений стала разработка Общегосударственного регламента по защите данных (GDPR), вступившего в силу в мае 2018 года. Документ устанавливает строгие правила обработки данных, наделяет пользователей широкими полномочиями, включая право требовать

удаления собственных данных («право быть забытым»), и вводит серьезную финансовую ответственность за нарушение правил [2].

2. Азиатский опыт

Восточные страны, такие как Япония и Южная Корея, разработали собственные механизмы защиты данных, которые основаны на национальных культурных особенностях и местных обычаях (законы PIPA в Южной Корее и APPI в Японии). Например, японская модель строится на приоритете чести и доверия, в то время как корейская — подчёркивает технологичность и прогресс.

В Китае государство активно контролирует процесс оборота данных, стремясь ограничить иностранные компании в доступе к внутренним рынкам и поддерживать национальную компанию Huawei, ведущий разработчик коммуникационных технологий [11; 8; 13; 15].

3. Американская модель

США избрали путь минимальной регламентации и максимума возможностей для технологического прогресса. Здесь отсутствует единый федеральный закон, подобный европейскому GDPR, вместо этого существует множество локальных законов, часто противоречащих друг другу (федеральные: HIPAA, GLBA, COPPA, законы штатов: CCPA, VCDPA, CPA). Кроме законов, Национальный институт стандартов и технологий (NIST) публикует рекомендации по внедрению мер безопасности для защиты персональных данных. Например, руководство № SP 800-122, которое описывает системообразующие нормы и правила, касающиеся мер по защите персональных данных.

Судебная практика. В США существует доктрина третьей стороны, которая создаёт оговорку относительно защиты персональных данных. Согласно ей, человек, добровольно предоставляющий персональные данные третьим лицам (например, серверам электронной почты, банкам, интернет-провайдерам), не может рассчитывать на их защиту.

Подобная ситуация затрудняет принятие общих решений и препятствует формированию единого европейского подхода [21].

IV. Проблема недобросовестности в отельном бизнесе

1. Феномен недоверия

Недоверие со стороны клиентов вызвано многочисленными случаями утечек данных, неправомерного распространения информации и отсутствием достаточной прозрачности в процедурах обработки данных.

Одна из крупнейших утечек конфиденциальной информации среди заведений общественного питания произошла в Пакистане. Из-за проблем с безопасностью программного обеспечения злоумышленникам удалось похитить данные свыше 2 миллионов гостей ресторанов. Кража затронула 250 заведений, и преступники выложили похищенные сведения, содержащие имена, адреса, телефонные номера, платёжные данные и номер кредиток, в дарквебе за выкуп в размере 2 биткоинов.

Крупнейшая американская корпорация Yum! Brands, управляющая всемирно известными сетями быстрого питания KFC, Pizza Hut и Taco Bell по франшизе, подверглась крупной утечке данных в 2023 году. Причиной послужила кибератака с применением вымогательского ПО, результатом которой стало раскрытие персональных данных ряда сотрудников, включая номера водительских удостоверений. Атака временно вывела из строя около 300 ресторанов в Великобритании, хотя компания утверждала, что событие не окажет заметного отрицательного воздействия на финансовую устойчивость корпорации.

Ещё один крупный случай произошёл в Чили, где были похищены персональные данные свыше 10 миллионов клиентов сети кондитерских Pastelería Mozart. Украденные сведения содержали имена, электронные адреса, номера телефонов, даты рождения и даже пароли.

В марте 2024 года крупнейший оператор китайских кафе Panda Express столкнулся с масштабной кибератакой. Преступники получили доступ к внутренним системам компании и успели скопировать важные данные в течение нескольких дней. Утечка коснулась текущих и бывших сотрудников, чья конфиденциальная информация была раскрыта, включая ФИО, номера водительских удостоверений и паспорта.

Летом 2024 года компания Jolibee Foods Corporation, владелец известных брендов филиппинского фаст-фуда, объявила о краже данных приблизительно 11 миллионов клиентов. Это самая крупная утечка данных в истории Филиппин, ставшая возможной благодаря хакерской атаке. Сообщалось, что среди похищенных данных оказались имена, адресные и контактные сведения, а также email-адреса [19].

Наконец, летом 2025 года специалисты исследовательской группы Cybernews сообщили о крупнейшей в истории утечке данных: в открытом доступе оказалось почти 16 миллиардов записей с комбинациями логинов и паролей от популярных веб-сервисов [14].

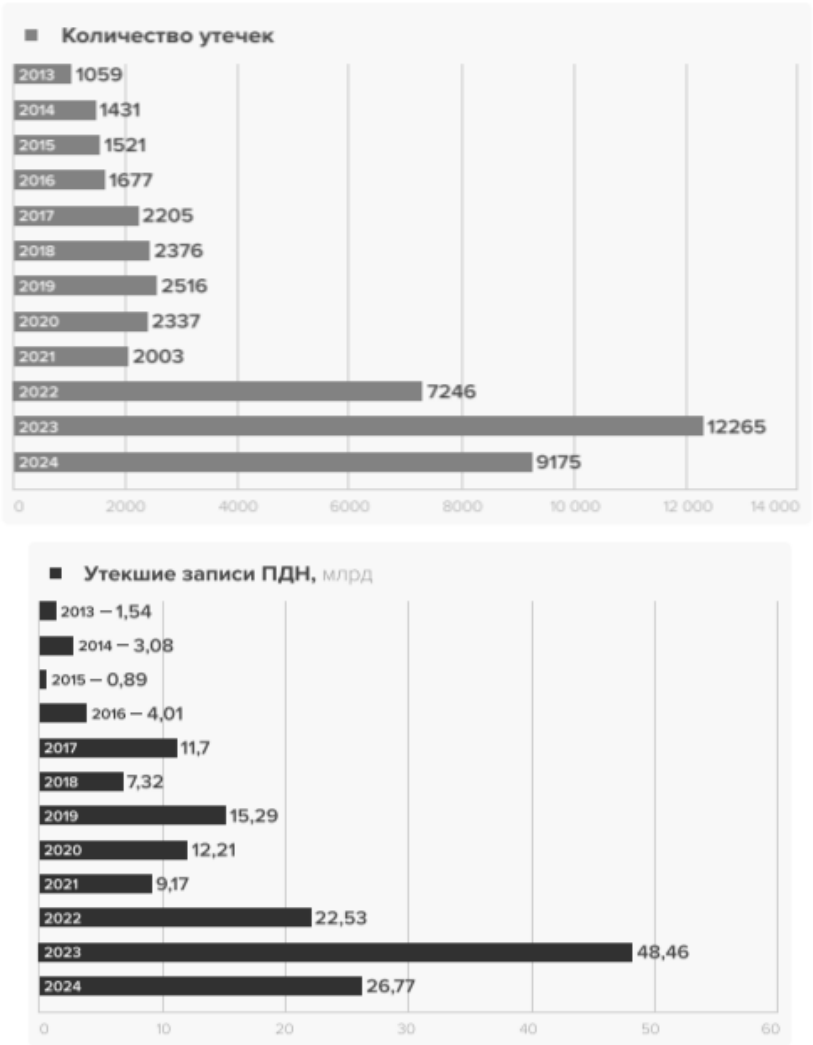

Рисунок 1. Количество утечек информации и количество утекших записей ПДн (млрд) в мире, 2013-2024 гг. [19]

По состоянию на июль 2025 года в России произошло 35 крупных инцидентов утечки персональных данных, суммарно затронувших более 39 миллионов пользователей. Более трети зафиксированных утечек пришлось на розничную торговлю. Одной из наиболее распространенных схем хищения информации стали незаконные выгрузки данных из корпоративных CRM-систем [18].

В общемировой картине Россия оказалась на втором месте по количеству инцидентов с утечками и поднялась на пятое место с седьмого в рейтинге по утечкам персональных данных. Согласно исследованию экспертно-аналитического центра InfoWatch, каждая 12-я мировая утечка информации происходила в России [19].

За первый квартал 2025 года крупнейшие утечки данных произошли следующим образом:

Самая крупная утечка произошла в Росреестре, когда в январе хакерам удалось извлечь более 2 млрд строк данных объемом около 1 Тб. Хотя публично доступен лишь небольшой фрагмент из 82 млн записей, сама утечка носит катастрофический характер.

Второй по величине инцидент случился в Департаменте информационных технологий Москвы. Группа хакеров опубликовала фрагменты базы данных, содержащих более 12,5 млн электронных почт и 11,7 млн телефонных номеров. Данные относятся к периоду лета-осени 2023 года [20].

Третья по размеру утечка связана с сайтом всероссийской муниципальной премии «Служение». Были опубликованы записи более 738 тыс. пользователей с их личными данными.

На четвертой позиции находится утечка данных покупателей сети Selgros Cash & Carry. Фрагмент содержал более 624 тыс. записей с подробной личной информацией и бонусными баллами.

Последнюю строчку занимает утечка данных сотрудников РЖД, опубликованная в январе. Было обнародовано около 573 тыс. записей с именами, должностями, рабочими номерами телефонов и служебными электронными адресами сотрудников [14].

В 2025 году российский суд впервые наложил взыскание на банковскую организацию за отправку персональных данных гражданина через иностранный мессенджер. Поводом для дела стало обращение москвички в Роскомнадзор, подтвердившей факты нарушения банковской тайны. Суд установил, что сотрудник банка использовал запрещённую платформу WhatsApp для отправки сообщения клиенту с корпоративного устройства. За данное нарушение учреждение признано виновным по ст. 13.11.2 Кодекса РФ об административных правонарушениях и оштрафовано на сумму 200 тысяч рублей [3].

Как показывает проведённый нами опрос в июле 2025 года (опрошено 234 россиянина старше 18 лет из разных регионов России) показал высокий уровень недоверия граждан к компаниям, обрабатывающим персональные данные: почти половина респондентов (47,4%) высказали полное недоверие. Наиболее высокую оценку респонденты дали компаниям, позволяющим удобно управлять собственными данными (36,3%).

Основная причина недоверия, по мнению большинства опрошенных, заключается в недостаточной осведомлённости о средствах защиты личной информации (42,7%). Треть участников опроса (36,3%) полагает, что проблему решит внедрение общепризнанных международных стандартов безопасности обработки данных. Ещё (40,2%) высказались за полный отказ от передачи личных данных компаниям.

Решить данную проблему возможно путем внедрения специализированных образовательных программ, направленных на повышение осведомленности сотрудников отелей о проблемах безопасности данных, а также применением современных технологий шифрования и аутентификации.

2. Формы недобросовестности

Нередко встречаются случаи откровенного злоупотребления данными, такие как продажа контактных данных третьим лицам, отправка спама и навязывание ненужных услуг. Наиболее распространёнными формами являются скрытые сборы дополнительной платы за якобы бесплатные услуги, завышение цен при бронировании номера и агрессивные маркетинговые кампании.

В последнее время отмечается рост количества мошеннических схем, использующих недостоверную информацию о скидках и акциях, вынуждая пользователей передавать свои персональные данные сомнительным ресурсам.

3. Способы устранения недостатков

Наиболее эффективным способом предупреждения нарушений является введение специального комитета по рассмотрению обращений граждан и установлению фактов недобросовестного поведения. Работа такого органа позволила бы быстро реагировать на жалобы клиентов и восстанавливать нарушенные права.

Ещё один важный элемент профилактики — техническое оснащение отелей современными системами мониторинга и контроля, способствующими оперативному обнаружению и пресечению подозрительных действий [7].

V. Психологический аспект доверия и добросовестности

1. Модель социального доверия

Психологи утверждают, что доверие формируется в ходе многократных повторений положительных впечатлений от общения с человеком или учреждением. В нашем случае доверие возникает у клиентов, которые ранее пользовались услугами отелей и остались довольны качеством обслуживания и надежностью защиты своих данных.[12]

Процесс формирования доверия зависит от ряда факторов, таких как профессионализм персонала, качество предоставляемых услуг, удобство интерфейса сайта и простота навигации. Немаловажную роль играет внешний вид здания гостиницы, чистота помещений и дружелюбие обслуживающего персонала.

2. Психологическое восприятие добросовестности

Восприятие добросовестности сотрудниками гостиницы складывается из личного убеждения в необходимости следовать правилам и нормам профессиональной этики. Высокий уровень самооценки, чувство принадлежности к профессии и вера в справедливость оказывают существенное влияние на поведение работника.

Формирование правильного восприятия добросовестности начинается с момента приема сотрудника на работу и продолжается на протяжении всей карьеры. Компания должна уделять особое внимание мотивации сотрудников, создавая комфортные условия труда и предоставляя карьерные перспективы [16].

VI. Практические рекомендации по обеспечению добросовестности и доверия

1. Оптимизация политики конфиденциальности

Политику конфиденциальности необходимо сделать доступной и простой для понимания каждым клиентом. Она должна содержать подробное описание типов собираемых дан-

ных, целей их обработки, срока хранения и методов защиты. Желательно разместить документ на сайте гостиницы и в открытых источниках, делая доступным каждому заинтересованному лицу.

2. Повышение квалификации сотрудников

Проведение курсов подготовки и переподготовки сотрудников, участие в тематических конференциях и симпозиумах способствуют росту профессионального мастерства персонала. Сотрудники должны понимать сущность добросовестности, осознавать ценность информации и уметь правильно обращаться с ней.

Организация регулярных тренировок и тестирования поможет закрепить полученные знания и умения, снизив риск ошибок и злоупотреблений.

3. Модернизация инфраструктуры

Использование современного технического оборудования и программного обеспечения, позволяющего надежно хранить и защищать данные, способно существенно уменьшить вероятность утечек и повреждений информации. Внедрение технологий облачного хранения и шифрования позволит организовать централизованное управление данными, сократить издержки и повысить эффективность работы персонала.

4. Сотрудничество с госорганами

Активное взаимодействие с правоохранительными структурами и контролирующими органами помогает своевременно выявлять факты нарушения законодательства и оперативно устранять возникшие проблемы. Своевременное информирование властей о любых изменениях в политике конфиденциальности позволяет избегать необоснованных обвинений и недопонимания.

5. Повышение уровня психологической устойчивости сотрудников

Создание комфортных условий труда, забота о здоровье и благополучии сотрудников, формирование положительного эмоционального климата в коллективе положительно сказываются на восприятии добросовестности и доверительности сотрудников. Необходимо вести профилактическую работу по снижению стрессовых нагрузок, оказывать поддержку работникам в кризисных ситуациях и поощрять достижения лучших профессионалов [22].

VII. Прогноз развития института защиты персональных данных

Согласно современным тенденциям, институт защиты персональных данных продолжит укрепляться, став одной из важнейших составляющих гражданского права. Рост популярности интернета и увеличение объемов цифровой информации приведут к появлению новых правовых институтов и нормативных актов, призванных регулировать данный сегмент.

Развитие технологий искусственного интеллекта и машинного обучения даст возможность создавать умные алгоритмы, способные самостоятельно анализировать данные и принимать взвешенные решения. Будущее принадлежит интеллектуальному праву, способному адаптироваться к изменениям внешней среды и обеспечивать надежную защиту персональных данных граждан.

Заключение

Представленная статья показала, насколько важны вопросы доверия и добросовестности в отельном бизнесе, особенно в контексте оборота персональных данных. Мы убедились, что современная действительность требует повышенного внимания к данному направлению, постоянного обновления методик и механизмов защиты данных, вовлечения профессиональных сообществ и органов власти в процесс выработки единых стандартов.

Реализация указанных рекомендаций позволит создать надежный защитный механизм, гарантирующий эффективное соблюдение принципов добросовестности и доверие клиентов к гостиничному бизнесу. Принимая во внимание сложность стоящих задач, предстоит дальнейшая исследовательская работа, нацеленная на выявление слабых мест и предложение путей их устранения.

Библиография

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция)
2. General Data Protection Regulation. [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
3. Банк оштрафован на 200 тыс. рублей за пересылку персональных данных в WhatsApp. [Электронный ресурс]. URL: https://rkn.gov.ru/press/news/news74922.htm
4. В защите персональных данных россияне все больше доверяют крупным операторам и все меньше уповают на себя. [Электронный ресурс]. URL: https://nafi.ru/analytics/v-zashchite-personalnykh-dannykh-rossiyane-vse-bolshe-doveryayut-krupnym-operatoram-i-vse-menshe-upo/
5. Ван Гуанлун Административно-правовая защита персональной информации в Китае: недостатки и пути решения // Вестник Университета имени О. Е. Кутафина (МГЮА). -2024. -№ 10. - С. 189-197. [Электронный ресурс]. URL: https://vestnik.msal.ru/jour/article/view/2541/2565
6. Ватолина Е. В. Сравнительно-правовой анализ правового регулирования защиты персональных данных в ЕС и Китае // Право и управление. -2024. -№ 8. - С. 403-405. [Электронный ресурс]. URL: https://law.law-books.ru/wp-content/uploads/2024/09/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE-%D0%B8-%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-8-2024.pdf#page=403
7. Гавчук Д.В. Экономика доверия в контексте устойчивого развития в индустрии гостеприимства. - Самара: Самарама, 2025. – 97 с.
8. Гун Нань Защита персональных данных в Китае: законодательство в цифровую эпоху // Вестник Санкт-Петербургского университета. Право. - 2023. - Т. 14. - № 1. - С. 159-172. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-kitae-zakonodatelstvo-v-tsifrovuyu-epohu
9. Добробаба М.Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О. Е. Кутафина. - 2023. - № 2 (102). - С. 42-52. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/ponyatie-personalnyh-dannyh-problema-pravovoy-opredelennosti.
10. Заклязьминская Е.О. Туристическая отрасль в стратегии развития Китая: монография. – М.: ИМЭМО РАН, 2021. – 234 с.
11. Законодательное регулирование цифровой экономики: опыт России и Китая: монография / под ред. Л.В. Санниковой, А.П. Алексеенко. – Москва: Проспект, 2025. – 528 с.
12. Кокотов А.Н. Доверие. Недоверие. Право:монография. - М.: Норма, 2020. - 192 с.

13. Коломойцев В. С., Хмелевский К. А. Сравнительный анализ защиты и обработки персональных данных в странах БРИКС // Международная научно-практическая конференция по компьютерной и информационной безопасности (INFSEC 2023): сб. Екатеринбург: ООО «Институт цифровой экономики и права», 2023. - С. 25-33.

14. Крупнейшие утечки информации за первый квартал 2025 года. [Электронный ресурс]. URL: https://cloudnetworks.ru/analitika/krupnejshie-utechki-informatsii-za-pervyj-kvartal-2025-goda/

15. Линь До Правовое регулирование защиты персональных данных и их контроль со стороны государства в Китае // Политика и общество. - 2020. - №2. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-zaschity-personalnyh-dannyh-i-ih-kontrol-so-storony-gosudarstva-v-kitae

16. Нам К.В. Принцип добросовестности: развитие, система, проблемы теории и практики. – 2-е изд., перераб. доп. – М.: Статут, 2022. – 388 с.

17. Основы коммерческого права Китайской Народной Республики: учебное пособие / отв. ред. В.Ф. Попондопуло, О.А. Макарова. – М.: Проспект, 2024. – 208 с.

18. Сливы подросли на CRM: увеличилось количество утечек данных из систем взаимодействия с заказчиками. [Электронный ресурс]. URL: https://www.f6.ru/media-center/press-releases/leaks-h1-2025/

19. Утечки информации в мире: статистика и анализ за 2024 год. [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-2023-2024-gody.pdf

20. Утечки данных: самые опасные хакерские группировки: Мир-Россия, 2024 г. [Электронный ресурс].URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki - dannykh-samyye-opasnyye-khakerskiye-gruppirovki-mir-rossiya_0.pdf

21. Файзуллина Л. Особенности регулирования вопросов, связанных с защитой персональных данных в сети «Интернет» в Российской Федерации и в США. Сравнительно-правовой анализ. [Электронный ресурс]. URL:https://zakon.ru/blog/2024/03/26/osobennosti_regulirovaniya_voprosov_svyazannyh_s_zaschitoj_personalnyh_dannyh_v_seti_internet_v_ross

22. Филипенко В.А. Специфика проявления принципа добросовестности в корпоративном праве : [монография]. – М.: Статут, 2025. – 501 с.

23. Шваб К. Технологии Четвертой промышленной революции: [перевод с английского]/ Клаус Шваб, Николас Дэвис. – М.: Эксмо, 2022. – 320 с.

Дата поступления: *22 августа 2025 г.*
Дата принятия в печать: *25 сентября 2025 г.*

Gavchuk D.V.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.80.72-83
UDC: 34.347

Trust and Integrity in the Handling of Personal Data in the Hotel Industry: Legal Analysis and Practical Recommendations

Abstract: Today's era, characterized by the rapid development of information technology and the active involvement of society in the virtual space, creates unique challenges in the handling of personal data. This issue is particularly relevant in the context of the hotel industry, where the volumes of information processed reach significant proportions. The main objective of this article is to comprehensively study the mechanisms for protecting personal data, building a system of trust, and fostering good faith behavior among market participants in the hotel sector. The analysis is conducted at the intersection of legal, psychological, and socioeconomic disciplines, allowing us to identify the shortcomings of the existing system and propose scientifically based approaches to its modernization.

Key words: personal data, information security, trust, integrity.

References

1. Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ (latest revision) (in Russian).

2. General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

3. A bank was fined 200,000 rubles for sending personal data via WhatsApp. Available at: https://rkn.gov.ru/press/news/news74922.htm (in Russian).

4. In terms of personal data protection, Russians increasingly trust large operators and rely less and less on themselves. Available at: https://nafi.ru/analytics/v-zashchite-personalnykh-dannykh-rossiyane-vse-bolshe-doveryayut-krupnym-operatoram-i-vse-menshe-upo/ (in Russian).

5. Wang Guanglong, Administrative and legal protection of personal information in China: shortcomings and solutions // Bulletin of O. E. Kutafin Moscow State Law University (MSAL). - 2024. - No. 10. - P. 189-197. Available at: https://vestnik.msal.ru/jour/article/view/2541/2565 (in Russian).

6. Vatolina E. V. Comparative legal analysis of legal regulation of personal data protection in the EU and China // Law and Management. -2024. - No. 8. - P. 403-405. Available at: https://law.law-books.ru/wp-content/uploads/2024/09-2024.pdf#page=403 (in Russian).

7. Gavchuk D. V. Economy of trust in the context of sustainable development in the hospitality industry. - Samara: Samara Publ., 2025. – 97 p. (in Russian).

8. Gong Nan. Personal Data Protection in China: Legislation in the Digital Age // Bulletin of St. Petersburg University. Law. - 2023. - Vol. 14. - No. 1. - Pp. 159-172. Available at:

♦ **Gavchuk Denis Vasilevich** - PhD in Economics, Master of Laws and Master of International Relations (Switzerland), Professor at the Regional Academy of Management, Member of the Federation of Restaurateurs and Hoteliers (Russian federation). E-mail: midk@bk.ru

https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-kitae-zakonodatelstvo-v-tsifrovuyu-epohu (in Russian).

9. Dobrobaba M.B. The Concept of Personal Data: The Problem of Legal Certainty // Bulletin of O.E. Kutafin University. - 2023. - No. 2 (102). - Pp. 42-52. Available at: https://cyberleninka.ru/article/n/ponyatie-personalnyh-dannyh-problema-pravovoy-opredelennosti. (in Russian).

10. Zaklyazminskaya E.O. Tourism Industry in China's Development Strategy: Monograph. Moscow: IMEMO RAS Publ., 2021. 234 p. (in Russian).

11. Legislative Regulation of the Digital Economy: The Experience of Russia and China: Monograph / edited by L.V. Sannikova, A.P. Alekseenko. Moscow: Prospect Publ., 2025. 528 p. (in Russian).

12. Kokotov A.N. Trust. Mistrust. Law: Monograph. Moscow: Norma Publ., 2020. 192 p. (in Russian).

13. Kolomoitsev V.S., Khmelevsky K.A. Comparative Analysis of Personal Data Protection and Processing in the BRICS Countries // International Scientific and Practical Conference on Computer and Information Security (INFSEC 2023): Coll. Yekaterinburg: Institute of Digital Economy and Law, 2023, pp. 25-33. (in Russian).

14. The Largest Information Leaks in the First Quarter of 2025. Available at: https://cloudnetworks.ru/analitika/krupnejshie-utechki-informatsii-za-pervyj-kvartal-2025-goda/ (in Russian).

15. Lin Do, Legal Regulation of Personal Data Protection and State Control in China // Politics and Society. - 2020. - No. 2. Available at: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-zaschity-personalnyh-dannyh-i-ih-kontrol-so-storony-gosudarstva-v-kitae (in Russian).

16. Nam K.V. The Good Faith Principle: Development, System, Theory and Practice. 2nd ed., revised and enlarged. Moscow: Statut Publ., 2022. – 388 p. (in Russian)

17. Fundamentals of Commercial Law of the People's Republic of China: Study Guide / eds. V.F. Popondopulo, O.A. Makarova. Moscow: Prospect Publ., 2024. – 208 p. (in Russian)

18. CRM Leaks Have Increased: the Number of Data Leaks from Customer Interaction Systems Has Increased. Available at: https://www.f6.ru/media-center/press-releases/leaks-h1-2025/ (in Russian)

19. Information Leaks Around the World: Statistics and Analysis for 2024. Available at: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-2023-2024-gody.pdf (in Russian)

20. Data Leaks: The Most Dangerous Hacker Groups: Mir-Russia, 2024. Available at: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-dannykh-samyye-opasnye-khakerskiye-gruppirovki-mir-rossiya_0.pdf (in Russian).

21. Fayzullina L. Features of regulation of issues related to the protection of personal data on the Internet in the Russian Federation and in the USA. Comparative legal analysis. Available at: https://zakon.ru/blog/2024/03/26/osobennosti_regulirovaniya_voprosov_svyazannyh_s_zaschitoj_personalnyh_dannyh_v_seti_internet_v_ross (in Russian).

22. Filipenko V.A. Specifics of the manifestation of the principle of good faith in corporate law: [monograph]. - Moscow: Statut Publ., 2025. - 501 p. (in Russian).

23. Schwab K. Technologies of the Fourth Industrial Revolution: [translated from English] / Klaus Schwab, Nicholas Davis. - Moscow: Eksmo Publ., 2022. - 320 p. (in Russian).

The article was submitted: *2025 August 22*
Accepted for publication: *2025 September 25*

Qavçuk D.V.♦

DOI: 10.25108/2304-1730-1749.iolr.2025.80.72-83
UOT: 34.347

Otel sənayesində şəxsi məlumatların idarə edilməsində etimad və dürüstlük: hüquqi təhlil və praktiki tövsiyələr

Xülasə: İnformasiya texnologiyalarının sürətli inkişafı və cəmiyyətin virtual məkana fəal cəlb olunması ilə səciyyələnən müasir dövr fərdi məlumatların dövriyyəsi sahəsində xüsusi problemlər yaradır. Bu problem, işlənmiş məlumatların həcminin əhəmiyyətli nisbətlərə çatdığı otel biznesi kontekstində xüsusilə aktualdır. Bu məqalənin əsas məqsədi şəxsi məlumatların qorunması, inam sisteminin qurulması və otel seqmentində bazar münasibətləri iştirakçılarının vicdanlı davranışının formalaşdırılması mexanizmlərinin hərtərəfli öyrənilməsidir. Təhlil hüquqi, psixoloji və sosial-iqtisadi fənlərin kəsişməsində aparılır və mövcud sistemin çatışmazlıqlarını aşkar etməyə və onun müasirləşdirilməsinin elmi əsaslı yollarını təklif etməyə imkan verir.

Açar sözlər: şəxsi məlumatlar; informasiya təhlükəsizliyi; etimad; vicdan; otel işi.

Məqalə daxil olmuşdur: *22 avqust 2025-ci il*
Çapa qəbul edilmişdir: *25 sentyabr 2025-ci il*

♦ **Gavchuk Denis Vasilyeviç** - PhD (iqtisad), hüquq üzrə magistri və beynəlxalq münasibətlər magistri (İsveçrə), Regional Menecment Akademiyasının professoru, Restorançılar və Otelçilər Federasiyasının üzvü (Rusiya Federasiyası). E-poçt: midk@bk.ru