Утверждено

Приказом от 23 января 2017 № ПД-16

ПОЛИТИКА

ООО «Отель» в отношении обработки персональных данных

1. Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и правовая основа документа

Политика ООО «Отель» определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется ООО «Отель» в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных ООО «Отель» позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

3. Основными объектами системы безопасности персональных данных в ООО «Отель» являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные;
- процессы обработки персональных данных в информационных системах персональных данных ООО «Отель», информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

4. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных ООО «Отель» являются:

- ООО «Отель», как собственник информационных ресурсов;
- руководство и сотрудники ООО «Отель», в соответствии с возложенными на них функциями;
- физические лица, не являющиеся сотрудниками ООО «Отель», но имеющими с ней отношения.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

4.1. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений ООО «Отель» от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем ООО «Отель», при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах ООО «Отель» и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

4.2. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности ООО «Отель» должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем ООО «Отель»;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационных систем ООО «Отель» посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам ООО «Отель» (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в информационных системах ООО «Отель» программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

4.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационных систем ООО «Отель» (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов ООО «Отель» по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам ООО «Отель»;

– четким знанием и строгим соблюдением всеми пользователями информационных систем ООО «Отель» требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам ООО «Отель»;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды ООО «Отель»;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением пользователями информационных ресурсов ООО «Отель» требований по обеспечению безопасности информации;

– юридической защитой интересов ООО «Отель» при взаимодействии с внешними организациями (связанными с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

5. Построение системы, обеспечения безопасности персональных данных ООО «Отель», и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;
– системность;
– комплексность;
– непрерывность;
– своевременность;
– преемственность и непрерывность совершенствования;
– разумная достаточность (экономическая целесообразность);
– персональная ответственность;
– минимизация полномочий;
– исключение конфликта интересов;
– взаимодействие и сотрудничество;
– гибкость системы защиты;
– открытость алгоритмов и механизмов защиты;
– простота применения средств защиты;
– обоснованность и техническая реализуемость;
– специализация и профессионализм;
– обязательность контроля.

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных ООО «Отель» в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем ООО «Отель» должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

5.2. Системность

Системный подход к построению системы защиты информации в ООО «Отель» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем ООО «Отель», а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты

Обеспечение безопасности персональных данных - процесс, осуществляемый руководством ООО «Отель», ответственными за организацию обработки персональных данных и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри ООО «Отель» и каждый сотрудник ООО «Отель» принимает участие в этом процессе. Деятельность по

обеспечению информационной безопасности является составной частью повседневной деятельности ООО «Отель». Физическим и техническим средствам защиты для эффективного выполнения своих функций оказываеися постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.).

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

5.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем ООО «Отель» и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите.

5.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным предоставляется только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов.

5.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе ООО «Отель». В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственного за обработку персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в ООО «Отель» является высокая культура работы с информацией. Руководство ООО «Отель» несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности ООО «Отель

5.11. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Организации своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Организации;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

5.12. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

5.13. Простота применения средств защиты.

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

5.14. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Организации. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения

безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

5.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных реализованы в ООО «Отель» на современном уровне, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности персональных данных.

5.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

5.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

6. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационных систем ООО «Отель» подразделяются на:

- правовые (законодательные);
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

6.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и постоянно разъясняются с пользователям и обслуживающему персоналу информационных систем ООО «Отель».

6.2. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты - меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

6.4. Формирование политики безопасности

Главная цель административных мер - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Политика в области обеспечения безопасности персональных данных в ООО «Отель» обеспечивает приемлемый уровень безопасности и обладает функциональностью.

6.5. Регламентация доступа в помещения

Компоненты информационных систем ООО «Отель» размещаются в помещениях, находящихся под охраной и наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников ООО «Отель».

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем ООО «Отель», запираются на ключ.

6.6. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами ООО «Отель» и доступ к их ресурсам строго регламентирован. Любые изменения состава и полномочий пользователей подсистем производятся установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально:

- каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, согласовывается с ответственным за организацию обработки персональных данных;

– директор ООО «Отель» имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники ООО «Отель» несут персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) подписывает обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных ООО «Отель».

Обработка персональных данных в компонентах информационных систем ООО «Отель» производится в соответствии с утвержденными технологическими инструкциями.

6.7. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников ООО «Отель», с которых возможен доступ к ресурсам информационной системы, соответствует кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей устанавливается и использовается лицензионные программные средства.

6.8. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам закрывается.

6.9. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем ООО «Отель», а также руководящий и обслуживающий персонал ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в ООО «Отель».

Все пользователи информационных систем ООО «Отель» ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных ООО «Отель». Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, осуществляется под роспись.

6.10. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы ООО «Отель».

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, определяется нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства ООО «Отель».

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов;
– проверка подлинности пользователей (аутентификация) на основе паролей;
– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

6.11. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности ООО «Отель» используются следующие средства защиты:

– физические средства;
– технические средства;
– средства идентификации и аутентификации пользователей;
– средства разграничения доступа;
– средства обеспечения и контроля целостности;
– средства оперативного контроля и регистрации событий безопасности.

Средства защиты применяются ко всем ресурсам информационных систем ООО «Отель», независимо от их вида и формы представления информации в них.

6.11.1. Физические средства защиты

Физические меры защиты основаны на применении механических и электронных устройств, ограничивающих доступ к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационной системы ООО «Отель» применяется:

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных;
– оборудование систем информатизации устройствами защиты от сбоев электропитания.

6.11.2. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и функции .

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства идентификации пользователей при помощи имен или пароля;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

6.11.3. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем ООО «Отель» посторонних лиц применяется распознавание каждого легального пользователя: магнитные карточки, ключи.

6.11.4. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

6.11.5. Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

6.12. Контроль эффективности системы защиты

Контроль эффективности защиты персональных данных осуществляется ответственным лицом для выявления и предотвращения утечки персональных данных за счет несанкционированного доступа,

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.