УТВЕРЖДАЮ
Генеральный директор
АО «Гостиничная компания»

_____/Карелов А.Б.

Приказ № 2023-07-14-1 от 14.07.2023

ПОЛОЖЕНИЕ

об организации и обеспечении защиты персональных данных в АО «Гостиничная компания»

г. Москва 2023

Содержание

1. Назначение и область применения ... 3
2. Термины и сокращения ... 3
3. Общие положения ... 5
4. Нормативные ссылки ... 5
5. Персональные данные, подлежащие защите ... 5
6. Организационная система обеспечения безопасности персональных данных ... 6
7. Защита персональных данных при их обработке без использования средств автоматизации ... 7
8. Защита персональных данных при их обработке в информационных системах персональных данных ... 7
9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных ... 14
10. Принятие мер в случае обнаружения фактов нарушения требований (несанкционированного доступа к персональным данным), разбирательство и составление заключений по фактам нарушения требований безопасности ... 14
11. Требования к персоналу по обеспечению защиты персональных данных ... 15
12. Порядок внесения изменений ... 15
Приложение № 1. Форма Журнала учета средств защиты информации, эксплуатационной и технической документации к ним ... 16
Приложение № 2. Форма Журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов ... 17
Приложение № 3. Форма Журнала периодического тестирования средств защиты информации ... 18
Приложение № 4. Форма Журнала учета мероприятий по защите информации ... 19
Лист изменений ... 20
Лист ознакомления ... 21

1. Назначение и область применения

1.1. Положение об организации и обеспечении защиты персональных данных (далее - Положение) предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных в соответствии с требованиями Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных в АО «Гостиничная компания» (далее – Общество).

1.3. Положение является локальным нормативным актом Общества. Требования Положения обязательны для выполнения всеми работниками, которые допущены к обработке персональных данных.

2. Термины и сокращения

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

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с ранее присвоенным идентификатором.

Информация — сведения (сообщения, данные) независимо от формы их представления.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Материальный носитель персональных данных (далее материальный носитель) – материальный объект, используемый для закрепления и хранения информации. В целях настоящего Положения под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т.п.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием

штатных средств, предоставляемых информационными системами персональных данных.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы информационной системы, осуществляемое с использованием вредоносных программ.

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

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

Ресурс информационной системы – именованный элемент системного прикладного или аппаратного обеспечения функционирования информационной системы.

Средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СЗПДн	Система (подсистема) защиты персональных данных
ФЗ	Федеральный закон

3. Общие положения

3.1. Необходимость проведения мероприятий по защите ПДн определяется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.2. Целью защиты ПДн является предотвращение возможной утечки информации, несанкционированного или непреднамеренного изменения или разрушения ПДн.

3.3. Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его ПДн, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

3.4. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением СЗИ НСД в процессе ее обработки, передачи и хранения.

3.5. Все работники, обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под роспись.

4. Нормативные ссылки

Настоящее Положение разработано в соответствии с законодательством РФ:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее также – Закон о персональных данных);

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 21.07.2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;

– Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15.02.2008;

– «Методическими рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденными руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144.

5. Персональные данные, подлежащие защите

5.1. Персональные данные, подлежащие защите в Обществе, обрабатываются как без использования средств автоматизации, так и в ИСПДн.

5.2. Персональные данные, подлежащие обработке и защите, утверждаются приказом Генерального директора Общества в виде Перечня обрабатываемых персональных данных.

5.3. Изменения, дополнения Перечня обрабатываемых персональных данных осуществляются на основании информации, предоставляемой работниками и руководителями подразделений, которые обрабатывают ПДн.

6. Организационная система обеспечения безопасности персональных данных

6.1. В состав организационной системы обеспечения безопасности ПДн Общества входят:

- Генеральный директор Общества;
- Заместитель генерального директора по безопасности;
- Работник, отвечающий за кадровое производство в Обществе;
- Работники подразделения ИТ;
- Руководители подразделений, работникам которых предоставлен доступ к ПДн;
- Работники, которым предоставлен доступ к ПДн.

6.2. Общее руководство организацией работ по защите ПДн осуществляет Генеральный директор Общества и осуществляет:

- общую организацию работы в Обществе согласно Закону о персональных данных;
- утверждение должностных лиц, положений, приказов и прочих локальных нормативных актов Общества.

6.3. Заместитель генерального директора по безопасности Общества в рамках обеспечения безопасности ПДн участвует в комиссиях по оценке соответствия систем и процедур обработки персональных данных и осуществляет:

- контроль обеспечения безопасности ПДн;
- полноту и объективность предлагаемых Генеральному директору Общества заключениях по результатам проведённой проверки;

6.4. Начальник отдела информационной безопасности Общества в рамках обеспечения безопасности ПДн осуществляет:

- контроль за организацией работ по разработке документации по ПДн;
- контроль за разработкой СЗПДн;
- контроль проведения организационных и технических мероприятий по защите ПДн;
- контроль и проведение проверок в Обществе в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе.

6.5. Работник, отвечающий за кадровое производство в Обществе, отвечает за организацию обработки персональных данных в Обществе и осуществляет:

- внутренний контроль за соблюдением Обществом и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- контроль за доведением до работников Общества положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- контроль приема и обработки обращений и запросов субъектов персональных данных и/или их представителей.

6.6. Работники подразделения ИТ Общества осуществляют системное администрирование ИСПДн и осуществляют:

- осуществление системного администрирования серверов, АРМ ИСПДн, администрирование прикладных систем ИСПДн Общества;
- настройки общесистемного и прикладного ПО ИСПДн, обеспечивают функционирование ИСПДн Общества, а также обеспечивают реализацию мероприятий по обеспечению безопасности ПДн в ИСПДн;
- обеспечение технической и организационной защиты персональных данных при их

обработке в ИСПДн, участие в классификации информационных систем персональных данных, разработку систем защиты персональных данных и при должной квалификации - настройку средств защиты.

6.7. Из состава работников Отдела информационной безопасности СБ Общества назначается лицо (лица), в обязанности которого (которых) входит обеспечение безопасности ПДн при их обработке в ИСПДн (администратор безопасности).

6.8. Руководители подразделений Общества, работникам которых предоставлен доступ к ПДн, действуют в рамках возложенных на них полномочий и осуществляют:

- контроль за наличием в подразделении актуального комплекта документации по ПДн;
- организацию и контроль хранения ПДн в подразделении;
- проведение проверок в подразделении в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе;
- контроль за соблюдением работниками подразделения законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доведение до работников подразделения положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей.

6.9. Работники Общества, которым предоставлен доступ к ПДн, непосредственно реализуют требования к обработке и безопасности ПДн, а также требований локальных нормативных актов Общества по обработке и безопасности ПДн.

7. Защита персональных данных при их обработке без использования средств автоматизации

7.1. Требования к обеспечению безопасности ПДн при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.2. Состав ПДн и перечень лиц, допущенных к обработке ПДн без использования средств автоматизации, указывается в Перечне обрабатываемых персональных данных и Перечне подразделений, в которых осуществляется обработка персональных данных.

7.3. Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

- определением мест хранения ПДн (материальных носителей ПДн) и перечня должностей, осуществляющих обработку ПДн либо имеющих к ним доступ;
- обеспечением раздельного хранения ПДн (материальных носителей ПДн), обработка которых осуществляется в различных целях;
- соблюдением условий, обеспечивающих сохранность материальных носителей ПДн и исключающих несанкционированный доступ к ним;
- установлением порядка прекращения обработки и уничтожения или обезличивания ПДн.

7.4. Порядок хранения, уничтожения ПДн без использования средств автоматизации устанавливается Положением об обработке персональных данных АО «Гостиничная компания».

8. Защита персональных данных при их обработке в информационных системах персональных данных

8.1. Состав ПДн и перечень лиц, допущенных к обработке ПДн при их обработке в ИСПДн указывается в Перечне обрабатываемых персональных данных и Перечне подразделений, в которых осуществляется обработка персональных данных.

8.2. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

– определение актуальных угроз безопасности ПДн при их обработке в ИСПДн, формирование на их основе частной модели нарушителя и угроз;

– определение уровня защищенности ПДн при их обработке в ИСПДн с учетом категории обрабатываемых ПДн, категории субъектов ПДн, объема обрабатываемых ПДн в ИСПДн и типа актуальных безопасности ПДн;

– выбор мер по обеспечению безопасности ПДн для установленного уровня защищенности ПДн, подлежащих реализации в системе защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию актуальных угроз безопасности ПДн;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (СЗИ), когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн;

– описание состава и содержания мер по обеспечению безопасности ПДн, реализуемых СЗПДн;

– установку и ввод в эксплуатацию СЗИ в соответствии с эксплуатационной и технической документацией;

– ознакомление работников с требованиями к защите ПДн, правилами обработки ПДн, обучение работников правилам работы с СЗИ в ИСПДн;

– установление правил доступа к ПДн и ИСПДн;

– учет применяемых СЗИ, эксплуатационной и технической документации к ним, электронных носителей (съемных носителей) ПДн;

– учет лиц, допущенных к работе с ПДн в ИСПДн;

– контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн, включая контроль над соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения электронных носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– принятие мер в случае обнаружения фактов НСД к ПДн;

– восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8.3. Меры по защите персональных данных, реализуемые СЗПДн, включают в себя:

– идентификацию и аутентификацию пользователей, являющихся работниками Общества, а также внешних пользователей;

– управление доступом работников Общества и внешних пользователей ИСПДн;

– регистрацию событий безопасности;

– ограничение программной среды ИСПДн;

– учет и хранение электронных носителей (съемных носителей) ПДн, исключающее несанкционированное использование, хищение, подмену и уничтожение;

– обеспечение целостности и доступности ПДн, ИСПДн и СЗИ (резервирование технических средств, дублирование массивов и носителей информации);

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок с использованием средств антивирусной защиты.

– управление конфигурацией и изменениями ИСПДн и СЗИ;

– защита среды виртуализации;

– защита периметра ИСПДн, средств и систем связи и передачи данных;

– обнаружение (предотвращение) вторжений, направленных на ИСПДн;

– анализ защищенности ИСПДн и тестирование работоспособности СЗПДн;

– защита технических средств (АРМ, серверы, коммутационное оборудование, сетевые принтеры), позволяющих осуществлять обработку ПДн;

– выявление инцидентов и реагирование на них.

8.4. Моделирование угроз безопасности и выбор уровня защищенности

8.4.1. Модель нарушителя и угроз безопасности персональных данных разрабатывается с использованием методических документов ФСТЭК России и (или) ФСБ России. Результаты определения и оценки актуальных угроз безопасности ПДн при их обработке в ИСПДн утверждаются приказом Генерального директора Общества.

8.4.2. Выявление типа и состава актуальных угроз безопасности ПДн осуществляется на основе экспертного метода, в том числе путем опроса специалистов по информационным технологиям, пользователей ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

8.4.3. На основе определенного типа актуальных угроз безопасности ПДн и характеристик ИСПДн (категории обрабатываемых ПД, категории субъектов ПДн, объем обрабатываемых ПДн в ИСПДн) в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности ПДн при их обработке в ИСПДн.

8.4.4. Модель нарушителя и угроз безопасности персональных данных должна периодически пересматриваться в соответствии с Планом внутренних проверок состояния защиты персональных данных в Обществе.

8.4.5. Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется в случаях:

– изменения процессов обработки (хранения, предоставления, передачи) ПДн в ИСПДн;

– использования в ИСПДн новых информационных технологий.

– изменения характеристик ИСПДн, влияющих на уровень защищенности (категории обрабатываемых ПД, категории субъектов ПДн, объем обрабатываемых ПДн в ИСПДн).

8.4.6. При необходимости применения (в случае передачи ПДн по незащищенным каналам связи) шифровальных (криптографических) средства (СКЗИ) для ИСПДн на основе «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных» ФСБ России и Модели нарушителя и угроз безопасности персональных данных определяется уровень криптографической защиты ПДн, которому должны соответствовать применяемые СКЗИ.

8.5. Порядок разработки, ввода в действие и эксплуатации системы защиты персональных данных

8.5.1. Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью СЗПДн, включающей организационные меры и СЗИ, а также используемые в информационной системе информационные технологии.

8.5.1.1. Требования по защите ПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

8.5.1.2. Требования к СЗПДн должны формироваться на основании положений руководящих документов ФСТЭК России и ФСБ России, перечень которых приведен в п. 4.

8.5.2. Требования к СЗПДн разрабатываются на основе Частной модели нарушителя и угроз безопасности персональных данных и должны обеспечивать нейтрализацию актуальных угроз.

8.5.2.1. Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн проводятся следующие мероприятия:

– обследование ИСПДн и определение необходимого уровня защищенности ПДн;

– разработка технического (частного технического) задания на создание СЗПДн;

– проектирование и реализация ИСПДн и СЗПДн в её составе;

– ввод в действие СЗПДн, включающее опытную эксплуатацию и приемо-сдаточные испытания СЗИ, а также оценку эффективности реализованных мер по обеспечению безопасности ИСПДн.

8.5.2.2. Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав и категория обрабатываемых ПДн, объем обрабатываемых ПДн;

– изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;

– изменился состав актуальных угроз безопасности ПДн в ИСПДн.

8.5.2.3. Все имеющиеся и вводимые в эксплуатацию ИСПДн вносятся в Перечень информационных систем персональных данных АО «Гостиничная компания».

8.6. Управление доступом пользователей к ИСПДн

8.6.1. Права доступа работника в ИСПДн Общества должны указываться в заявке руководителя подразделения.

8.6.2. Заявка передается администратору безопасности ИСПДн для согласования заведения учетной записи и назначения полномочий доступа работника в ИСПДн.

8.6.3. Права доступа к ИСПДн фиксируются администратором безопасности ИСПДн в матрице доступа ИСПДн.

8.6.4. На периодической основе или после каждого изменения в ИСПДн должна проводиться проверка матрицы доступа ИСПДн и действующих прав доступа в ИСПДн.

8.6.5. Доступ работника к ИСПДн с использованием мобильных технических средств должен предоставляться на основании заявки руководителя подразделения.

8.6.6. Администратор безопасности ИСПДн осуществляет настройку учетной записи пользователя ИСПДн в соответствии с установленными правилами разграничения доступа.

8.7. Регистрация событий безопасности информационных систем персональных данных

8.7.1. Регистрация событий безопасности должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

8.7.2. Подлежат обязательной регистрации и анализу следующие события в ИСПДн:

– регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

– регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

– регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа.

8.8. Ограничение программной среды ИСПДн

8.8.1. Контроль за установкой (инсталляцией) компонентов ИСПДн, обновлений программного обеспечения ИСПДн должен осуществляться администратором безопасности ИСПДн.

8.9. Обеспечение безопасности персональных данных при хранении носителей информации

8.9.1. Подлежат учету следующие защищаемые носители ПДн:

– накопители на жестких магнитных дисках, установленные в серверы ИСПДн;

– накопители на жестких магнитных дисках, установленные в АРМ, на которых предусмотрено хранение ПДн;

– накопители для хранения резервных копий;

– внешние носители ПДн (дискеты, компакт-диски, flash-накопители), на которых технологией обработки ПДн разрешается хранение или передача ПДн.

8.9.2. Учет защищаемых носителей информации должен осуществляться в Журналах учета внешних машинных носителей ПДн в соответствии с порядком, предусмотренным Положением об обработке персональных данных Общества.

8.9.3. Обязанность по ведению учета защищаемых носителей ПДн возлагается на администратора безопасности ИСПДн.

8.9.4. В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых носителей информации необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с носителей информации должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя.

8.9.5. По факту уничтожения носителя ПДн должен составляться соответствующий Акт в порядке, предусмотренном Регламентом уничтожения персональных данных в Обществе.

8.10. Обеспечение целостности и доступности персональных данных

8.10.1. Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при их случайной или намеренной модификации, должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

8.10.2. Для обеспечения целостности и доступности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие механических повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

8.10.3. Контроль целостности программного обеспечения СЗИ должен осуществляться с помощью встроенных механизмов проверки целостности программного обеспечения резервных копий СЗИ по контрольным суммам.

8.11. Использование средств антивирусной защиты

8.11.1. Подсистема антивирусной защиты реализуется путем внедрения специального антивирусного программного обеспечения на всех элементах ИСПДн.

8.11.2. Средства антивирусной защиты предназначены для реализации следующих функций:

– антивирусное сканирование;

– блокирование вредоносных программ;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

8.11.3. Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять администратора безопасности ИСПДн.

8.12. Защита среды виртуализации

8.12.1. Защита ПДн в виртуальной среде должна обеспечиваться выполнением мер, предусмотренных настоящим Положением:

– управление доступом пользователей и администраторов виртуальной среды;

– регистрация событий безопасности в виртуальной среде;

– ограничение программной среды виртуальных машин ИСПДн;

– контроль целостности конфигурации виртуальной инфраструктуры и резервное копирование данных;

– антивирусная защита.

8.13. Использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия

8.13.1. В качестве СЗИ, прошедших процедуру оценки соответствия, используются СЗИ, сертифицированные в системах сертификации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации в пределах их полномочий.

8.13.2. При использовании СЗИ, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию СЗИ осуществляется в соответствии с эксплуатационной и технической документацией;

– проведение обучения работников, использующих СЗИ, правилам работы с ними;

– учет применяемых СЗИ, эксплуатационной и технической документации к ним. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним приведена в приложении № 1. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним приведена в приложении № 2;

– контроль за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

– периодическое тестирование средств защиты в соответствии с эксплуатационной документацией на СЗИ. Форма журнала проведения периодического тестирования СЗИ приведена в приложении № 3;

– разбирательство и составление заключений по фактам несоблюдения условий использования СЗИ, которые могут привести к нарушению целостности, конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

8.14. Защита периметра ИСПДн, систем и средств связи и передачи данных

8.14.1. При взаимодействии ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от НСД являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи, в том числе беспроводным каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты;

– централизованное управление СЗПДн.

8.14.2. Для обеспечения безопасности ПДн при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена дополнительно должны применяться следующие основные методы и способы защиты информации от НСД:

– проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена данных;

– управление доступом к защищаемым ПДн информационной сети;

– использование атрибутов безопасности.

8.14.3. Для обеспечения безопасности ПДн при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от НСД:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

8.14.4.Защита каналов связи реализуется следующими организационно-техническими способами:

– размещение линий связи и сетевого оборудования в пределах КЗ;

– использование волоконно-оптических линий связи, затрудняющих или исключающих возможность перехвата передаваемой информации;

– использование шифровальных (криптографических) средств.

8.15. Защита технических средств

8.15.1.Размещение ИСПДн и охрана помещений, в которых ведется работа с ПДн, должны обеспечивать сохранность материальных носителей ПДн, СВТ ИСПДн и СЗИ, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.15.2.Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию КЗ Общества.

8.15.3.Границами КЗ могут являться:

– периметр охраняемой территории;

– ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;

– стены помещений.

8.15.4.В состав КЗ должны входить:

– помещения, в которых размещены АРМ, серверы, сетевое оборудование, входящие в состав ИСПДн;

– помещения, в которых проходят кабельные линии связи ИСПДн;

– помещения, в которых хранятся съемные носители ПДн (резервные копии), материальные носители ПДн.

8.15.5.Размещение СВТ ИСПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

8.15.6.Доступ посторонних лиц (посетителей, клиентов, контрагентов) в КЗ в рабочее время осуществляется только в сопровождении работников Общества.

8.15.7.Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8.15.8.Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

8.15.9.В нерабочее время доступ в КЗ должен быть исключен следующими мерами:

– Заключением договора с арендодателем (охранным предприятием), обязательными условиями которого являются следующие обязанности арендодателя (охранного предприятия):

– организация и обеспечение контроля доступа в арендуемые помещения работников и посетителей в рабочее время.

– организация и обеспечение охраны помещений в нерабочее время, а также в выходные и праздничные дни.

– не допускать проникновения и пребывания посторонних лиц в помещениях в нерабочее время, а также в выходные и праздничные дни. При необходимости использования помещений в

указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом.

– внос и вынос материальных ценностей в помещения и из помещений осуществляется только в присутствии ответственного лица.

8.16. Порядок оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн

8.16.1. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн при их обработке в ИСПДн проводится в виде внутренней оценки или добровольной аттестации на соответствие требованиям безопасности информации.

8.16.2. Для ИСПДн, оценка эффективности принимаемых мер которых проводится в виде внутренней оценки, необходимо выполнять следующие требования:

– оценка эффективности принимаемых мер осуществляется на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии;

– в случае проведения оценки на основе собственных доказательств самостоятельно формирует комплект документов, содержащих результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия ИСПДн всем необходимым требованиям по защите ПДн в ИСПДн;

– результаты оценки эффективности принимаемых мер должны содержать:

– наименование и местонахождение ИСПДн;

– информацию об объекте подтверждения соответствия (описание организационных и технических мер обеспечения безопасности ПДн в ИСПДн);

– наименование документов, на соответствие требованиям которых оценивается ИСПДн;

– сведения о принятых мерах по обеспечению соответствия ИСПДн необходимым требованиям;

– сведения о документах, послуживших основанием для подтверждения соответствия ИСПДн требованиям;

– срок действия оценки и условия повторной оценки.

8.16.3. Добровольная аттестация ИСПДн на соответствие требованиям безопасности информации проводится в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденным председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.

9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных

9.1. Целью контроля состояния защиты ПДн является своевременное выявление и предотвращение утечки информации.

9.2. Контроль состояния защиты ПДн должен осуществляться в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных Общества. Форма журнала учета проведения мероприятий приведена в приложении № 4.

9.3. Проведение контроля состояния защиты включает в себя мероприятия по оценке:

– актуальности локальных актов Общества по вопросам обработки и защиты ПДн;

– соблюдения работниками требований законодательства РФ по вопросам обработки и защиты ПДн;

– работоспособности применяемых СЗИ в соответствии с их эксплуатационной документацией.

9.4. Проверка проводится дополнительно при изменении конфигурации ИСПДн и СЗИ, состава технических средств и систем, условий обработки ПДн.

10. Принятие мер в случае обнаружения фактов нарушения требований (несанкционированного доступа к персональным данным), разбирательство и

составление заключений по фактам нарушения требований безопасности

10.1. Работник Общества, обнаруживший факт нарушения требований, незамедлительно уведомляет руководителя подразделения и подразделение (или лицо), осуществляющее функции по организации и обеспечению безопасности ПДн в Обществе.

10.2. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения, и принять меры к их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

– возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

10.3. В случае, если вследствие НСД ПДн были модифицированы или уничтожены, осуществляется восстановление ПДн из резервной копии.

11. Требования к персоналу по обеспечению защиты персональных данных

11.1. При вступлении в должность нового работника лицо, Руководитель подразделения работника, обязан провести ознакомление работника с должностной инструкцией и необходимыми документами, регламентирующими требования по обработке и защите ПДн (Положением об обработке персональных данных, настоящим Положением).

Подразделение (или лицо), осуществляющее функции по организации и обеспечению защиты ПДн в Обществе, проводит обучение работника навыкам выполнения процедур, необходимых для работы с СЗИ в ИСПДн, знакомит под роспись с Инструкцией по обеспечению безопасности при работе с персональными данными и прочими локальными нормативными актами Общества по организации защиты информационных систем Общества.

11.2. Работники Общества должны соблюдать установленные локальными нормативными актами Общества требования по режиму обработки ПДн, учету, хранению, передаче съемных и материальных носителей ПДн и обеспечению защиты ПДн.

11.3. Работники Общества должны быть проинформированы об ответственности за нарушение требований по обеспечению защиты ПДн в момент заключения трудового договора.

12. Порядок внесения изменений

12.1. Настоящее Положение пересматривается подразделением, осуществляющем функции по организации защиты персональных данных раз в год и в случае изменения законодательства в области защиты ПДн.

12.2. Все изменения отражаются в Листе изменений.

12.3. Измененное Положение утверждается Генеральным директором Общества.

Приложение № 1 к положению об организации и обеспечению защиты ПДн в АО «Гостиничная компания»

**Журнал учета средств защиты информации,
эксплуатационной и технической документации к ним**

Журнал начат «___» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование СЗИ	Серийный (заводской) номер СЗИ	Организация, выполнявшая установку СЗИ	Место установки СЗИ	Примечание
1					
2					
3					
4					
5					

Приложение № 2 к положению об организации и обеспечению защиты ПДн в АО «Гостиничная компания»

Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	ФИО работника, проводившего установку	Дата установки и подписи лиц, произведших установку	Номера аппаратных средств, в которые установлены СКЗИ	
1	2	3	4	5	6	8	9	10	11	12	13
1.											
2.											
3.											
4.											

Приложение № 3 к положению об организации и обеспечению защиты ПДн в АО «Гостиничная компания»

Журнал периодического тестирования средств защиты информации

Журнал начат «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование СЗИ/СКЗИ	Регистрационные номера СЗИ/СКЗИ	Дата проведения тестирования	ФИО и подпись проводившего тестирование	Вид теста и используемые средства для его проведения	Результат тестирования (успешный/неуспешный), примечания	Дата проведения следующего тестирования
1							
2							
3							
4							
5							

Приложение № 4 к положению об организации и обеспечению защиты ПДн в АО «Гостиничная компания»

Журнал учета мероприятий по защите информации

Журнал начат «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование мероприятия	Краткое описание мероприятия	**Дата проведения** мероприятия	**ФИО проводившего** мероприятие	**Подпись проводившего** мероприятие	Примечание
1						
2						
3						
4						
5						

Лист изменений

№ версии	Приказ/ дата	Название документа	Лист / Статья	Содержание изменения	Характер изменения	Изменения произвел