RADISSON COLLECTION
HOTEL MOSCOW

Политика Информационной Безопасности

RADISSON COLLECTION
HOTEL MOSCOW

Оглавление:

RADISSON COLLECTION
HOTEL MOSCOW

Основные термины и определения

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
Администратор АС (системный администратор АС) – лицо, ответственное за функционирование АС в установленном штатном режиме работы;
Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах: библиотеках, архивах, фондах, банках данных, других видах ИС;
Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
Клиент – субъект, ПДн которого обрабатываются в организации;
Информация конфиденциального характера (конфиденциальная информация) - информация, к которой нет свободного доступа на законном основании и, по отношению к которой установлен режим конфиденциальности;
Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
Локальная вычислительная сеть (ЛВС) – совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС;
Несанкционированный доступ (НСД) к информации (ресурсам ИС) - доступ к информации (ресурсам информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам ИС) с применением штатных средств ИС или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам;
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;
Служебные сведения ограниченного распространения – сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Перечень Сокращений

АРМ – автоматизированное рабочее место

ИБ – информационная безопасность

КСЗ – комплекс средств защиты

ЛВС – локальная вычислительная сеть

НДВ – недекларированные возможности

НСД – несанкционированный доступ

ПДн – персональные данные

ПО – программное обеспечение

РД – руководящий документ

СВТ – средства вычислительной техники

СЗИ – система защиты информации

СКЗИ – средства криптографической защиты информации

СрЗИ – средства защиты информации

ФСБ – Федеральная служба безопасности

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ЭВМ – электронно-вычислительная машина

ЭЦП – электронно-цифровая подпись

1 Общие положения

1.1 Назначение

Настоящее Положение по организации и проведению работ по обеспечению безопасности ПДн (далее – Положение) в ООО «ВЫСОТКА» (далее – предприятие) представляет собой совокупность правил, процедур, практических приемов и руководящих принципов в области информационной безопасности.
Положение определяет:
- порядок отнесения информации к ПДн и порядок обращения с ней;
- правовые и организационные меры обеспечения безопасности персональных данных на предприятии в соответствии с законодательством РФ
- отношения с другими организациями, возникающие при формировании и использовании персональных данных.

Положение предназначено для формирования комплексной системы организационных, технических и правовых процедур, обеспечивающих формирование и исполнение мероприятий по защите информационных ресурсов предприятия.
Требования настоящего Положения распространяются на все структурные подразделения предприятия, субъекты информационных отношений и привлекаемые организации, имеющие доступ к персональным данным на предприятии.
Положение разработано в соответствии с действующими нормативно-правовыми актами Российской Федерации, стандартами и рекомендациями в области защиты ПДн.
Настоящее Положение может уточняться, дополняться или изменяться в установленном на предприятии порядком, в случае изменения:
- состава обрабатываемой информации в ИСПДн предприятия;
- организационной структуры предприятия и (или) структуры ИСПДн;
- нормативно-правовых актов Российской Федерации в области обеспечения информационной безопасности.

1.2 Цели и задачи Положения

Цели Положения:

Основной целью настоящего документа является регламентация работ в области обеспечения защиты информационных ресурсов предприятия, в том числе:
- предотвращение материального, морального или иного ущерба за счет разглашения, утечки информации ограниченного распространения вследствие несанкционированного доступа к информационным ресурсам предприятия;
- обеспечение функционирования информационных ресурсов предприятия в соответствии с установленными режимами и регламентами;
- поддержание требуемого уровня защищенности информационных ресурсов предприятия.

Для достижения вышеуказанных целей, Положение решает следующие основные задачи:

- формирование организационных, правовых и технических процедур защиты информационных ресурсов предприятия;
- формирование организационных, правовых и технических процедур контроля реализации механизмов защиты информации;
- формирование базовых принципов построения комплексной системы защиты информации предприятия;
- обеспечение соответствия и адекватности механизмов защиты информации угрозам безопасности информационным и техническим;
- определение ответственности работников предприятия за нарушение установленных процедур защиты информационных ресурсов;

2 Принципы построения комплексной системы защиты информации

2.1 Общие принципы

Комплексная система обеспечения безопасности информации на предприятии должна обеспечивать сохранность ПДн, а также информации о структуре ИСПДн, используемых технических и программных средствах, о структуре, принципах и алгоритмах работы средств защиты информации.
Комплексная система обеспечения безопасности ПДн на предприятии включает в свой состав следующие группы мер и мероприятий по защите информации:
- правовые и законодательные;
- организационные и административные;
- режимно-объектовые;
- технические и технологические.

Правовые и законодательные меры защиты

К правовым мерам защиты относятся действующие законы и иные правовые нормативные акты, регламентирующие правила обращения с информацией, устанавливающие права и обязанности участников процессов обработки и использования информации и определяющие ответственность и санкции за нарушения этих правил. Важным условием использования данных мер защиты, является обеспечение осведомленности пользователей ИСПДн о действующих требованиях.

Организационные и административные меры защиты

Организационные и административные меры защиты регламентируют процессы функционирования ИСПДн, использование ещё ресурсов, деятельность обслуживающего персонала. Организационные методы защиты информации включают:
- формирование политики информационной безопасности и формулировку перспектив дальнейшего развития и совершенствования системы защиты информации;
- определение регламента и процедуры предоставления доступа к ресурсам ИСПДн;
- определение порядка взаимодействия и координация действий всех подразделений предприятия с целью обеспечения требуемого уровня защищённости информационных ресурсов;

- определение обязанностей пользователей и степень ответственности за нарушения процедур обработки данных и защиты информации;
- осуществление контроля над выполнением положений нормативных документов и проведение проверок;
- подбор и проверку персонала при зачислении в штат организации и предоставлении доступа к информационным ресурсам;
- проведение мероприятий по доведению порядка эксплуатации компонент АС до пользователей (проведение инструктажа);

Режимно-объектовые меры защиты

Режимно-объектовые меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, предназначенных для предотвращения физического проникновения потенциальных нарушителей к компонентам системы и защищаемым информационным ресурсам, а также технических средств наблюдения, связи, охранной и пожарной сигнализации. Для обеспечения физической безопасности компонентов ИСПДн выполняются следующие организационные и технические мероприятия:
- введение ограничений по доступу в помещения, предназначенные для хранения и обработки ПДн;
- оборудование системы устройствами от сбоев электропитания и помех в линиях связи;
- противопожарная сигнализация и охрана;
- охрана периметра защищаемых территорий;
- контроль доступа сотрудников и посторонних лиц в помещения предприятия.

Технические средства защиты

В соответствии с общими принципами создания комплексной системы безопасности информации, в состав системы технических и технологических средств защиты ИСПДн входят следующие подсистемы:
- подсистема защиты информации от НСД;
- подсистема антивирусной защиты;
- подсистема обнаружения вторжений;
- подсистема анализа защищенности;
- подсистема межсетевого экранирования.

Технические меры защиты информации конфиденциального характера, при ее передаче и обработке техническими средствами устанавливаются в соответствии с требованиями действующего законодательства РФ и внутренними нормативными документами, регламентирующими организацию технической защиты информации конфиденциального характера на предприятии.

2.2 Построение комплексной системы защиты информации

Для построения комплексной системы защиты информации необходимо разработать на каждую ИСПДн Модель угроз и модель нарушителя, на ее основании разработать систему защиты информации, обеспечивающую противодействие актуальным угрозам безопасности, при этом необходимо учесть следующие требования:

- применяемые средства и технологии защиты должны обладать свойствами модульности, масштабируемости, открытости и возможности адаптации системы к различным организационным и техническим условиям;
- подсистемы и компоненты СЗИ должны обеспечивать безопасное функционирование всех элементов ИСПДн (АРМ, серверного и системного программного обеспечения, прикладных систем, систем связи);
- должен быть предусмотрен комплекс организационно-технических мер и мер технологической защиты информации.

Комплексная система защиты информации по своей структуре подразделяется на ряд составляющих ее подсистем, основывающихся на различных механизмах защиты и объединенных единой идеологией построения и управления. Только совокупность защитных механизмов всех подсистем позволяет осуществить комплексное обеспечение информационной безопасности ИСПДн.

3 Организация работ по защите информации

3.1 Порядок обработки информации конфиденциального характера

При сборе, обработке, хранении, использовании и передаче ПДн на предприятии обеспечивается следующее:
- доступ к ПДн только для специально уполномоченных лиц, при этом указанные лица должны получать только те данные, которые необходимы для выполнения конкретных функций;
- проведение мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи ее лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки информации, в результате которого может быть нарушено их функционирование;
- постоянный контроль обеспечения защищенности информации.

3.2 Порядок организации работ по защите информации

Выполнение обязанностей по защите ПДн, по обеспечению функционирования комплексной системы безопасности информации возлагается на структурное подразделение или организацию, обеспечивающую функционирование ИСПДн.
Задачи по обеспечению физической безопасности территорий и контролю доступа лиц на территории предприятия возлагаются на Административный департамент.
На структурное подразделение или должностное лицо, ответственное за обеспечение информационной безопасности предприятия возлагаются следующие задачи:
- методологический контроль в области безопасности информации,
- взаимодействие с ФСТЭК – в части защиты информационных ресурсов от НСД, сертификации используемых технических средств и аттестации объектов информатизации по требованиям безопасности информации;
- взаимодействие с МВД – в части расследования компьютерных инцидентов и преступлений в области информационных технологий.

В структурных подразделениях разрабатывается перечень должностных обязанностей работников, ответственных за обеспечение безопасности конфиденциальной информации.

3.3 Порядок обработки ПДн

Обеспечение защиты ПДн, предоставляемых субъектам, при их обработке в ИСПДн осуществляется в соответствии с приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн» и постановлением Правительства от 01.11.2013г. №1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».
Контроль эффективности принятых мер защиты ПДн возлагается на оператора ПДн – ООО «ВЫСОТКА».
Оператор ПДн вправе обрабатывать ПДн пользователей (субъектов персональных данных) только с их согласия.
Работники предприятия (в пределах полномочий, приведенных в Уставе и законодательства РФ) вправе проверять предоставляемые пользователями ПДн, с целью корректного выполнения возложенных на них функций.
Работники предприятия имеют право получать и обобщать ПДн, необходимые для выполнения административных функций.
Меры по обеспечению целостности, конфиденциальности и доступности персональных данных, признаются разумно достаточными, если выполняются требования по обработке ПДн без нарушения режима защиты ПДн.
Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.
Право Клиента на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

Порядок обработки ПДн работников

Персональные данные (ПДн) работника – информация, необходимая работодателю в связи с установлением трудовых отношений и касающаяся конкретного работника.
К категории ПДн относятся следующие сведения, обрабатываемые в ИСПДн: опознавательные данные (ФИО, дата и место рождения, трудовая биография работника, факты биографии); личные характеристики работника (гражданство, наличие научных трудов, изобретений и т.д.); сведения о семейном положении; составе семьи; социальном положении; служебном положении; навыках; о финансовом положении; информацию, содержащаяся в трудовой книжке, в страховом свидетельстве государственного пенсионного страхования; информацию об образовании, квалификации и в других документах, которые содержат данные, необходимые работодателю в связи с трудовыми отношениями.
Обработка ПДн работника осуществляется в целях обеспечения соблюдения законов и других нормативно-правовых актов.
Работодатель получает и обрабатывает ПДн работника без его письменного согласия, т.к. это делается во исполнение трудового кодекса.
Все ПДн работника работодатель получает непосредственно от самого работника путем анкетирования и сбора официальных документов, необходимых для обеспечения трудовой деятельности работника.

Работодатель вправе проверять ПДн работников с целью формирования кадрового резерва.
При приеме на работу (заключении трудового договора), заполнении анкетных данных работодатель не имеет право получать и обобщать информацию о религиозных, политических и других убеждениях работника.
Работодатель сообщает работнику цели, предположительные источники, способы получения ПДн, характер ПДн и последствия отказа работника дать письменное согласие на их получение (в случаях, предусмотренных ФЗ 152).
Работодатель имеет право передавать ПДн работников в налоговые органы, Пенсионный фонд РФ, Фонд социального страхования РФ, Государственную инспекцию труда. Использование ПДн работника допустимо только в соответствии с целями, определившими их получение. Передача ПДн работника возможна только с согласия работника, если иное не предусмотрено законодательством, при передаче ПДн работника в банк необходимо получить согласие на передачу, если договор на выпуск банковской карты заключен напрямую с работником, либо у работодателя имеется доверенность на представление интересов работника при заключении договора с банком на выпуск карты, то согласие не требуется.
Работодатель производит расчет и выплату налогов за работника путем удержания их из заработной платы, работодатель имеет право собирать предусмотренные Налоговым Кодексом РФ сведения о налогоплательщике.
При обработке ПДн работодатель обеспечивает право работников предприятия на:
- получение полной информации об их ПДн и обработке этих данных;
- свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных федеральным законом;
- требование об исключении или исправлении неверных, или неполных ПДн, а также данных, обработанных с нарушением требований действующего законодательства. При отказе работодателя исключить или исправить ПДн работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия; ПДн оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым раннее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его ПДн.

ПДн работников вместе с необходимыми документами остаются у работодателя в лице ответственного за оформление приема и хранения личных папок работников. Хранение ПДн должно исключать их утрату или неправомерное использование.

Порядок обработки ПДн клиентов

Персональные данные Клиента могут обрабатываться только с согласия Клиента для целей, непосредственно связанных с деятельностью предприятия.
Клиент предоставляет предприятию ПДн только в объеме, необходимом для достижения названных целей. На предприятии ведется автоматизированная и неавтоматизированная обработка ПДн Клиента.

Сбор, хранение, использование и распространение, в том числе передача третьим лицам, ПДн Клиента без письменного его согласия на предприятии запрещена, если иное не предусмотрено Законодательством РФ.
Передача ПДн третьим лицам возможна, без письменного согласия Клиента, в случаях обезличивания, если иное не определено Законодательством РФ. На предприятии не ведется сбор и обработка ПДн Клиента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

Все ПДн Клиента, обработка которых ведется на предприятии, получены у него самого, после предоставления им письменного Согласия на обработку переданных им в ООО «ВЫСОТКА» его персональных данных, с возможностью передачи третьим лицам и должно соответствовать требованиям 152 - ФЗ и содержит следующие сведения:
– фамилию, имя, отчество, адрес Клиента, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
– цель обработки ПДн;
– перечень ПДн, на обработку которых дается согласие Клиента;
– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПДн;
– срок, в течение которого действует согласие, а также порядок его отзыва;
– по достижению целей обработки и хранения, удаление ПДн Клиента происходит без дополнительного уведомления Клиента.

Согласно пункту 5 части 1 статьи 6 Федерального закона «О персональных данных» согласие субъекта персональных данных на обработку персональных данных не требуется, если обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных.

3.4 Общий порядок обеспечения безопасности персональных данных

Меры по охране ПДн, признаются разумно достаточными, если:
- исключается доступ к ПДн любых лиц без согласия ее обладателя;
- выполняется требование обработки ПДн и передачи их контрагентам без нарушения режима конфиденциальности.

Порядок допуска работников к ПДн

В трудовой договор, вне зависимости от наличия у работника права доступа к ПДн, включается пункт о неразглашении ПДн, ставших известными работнику в процессе трудовой деятельности, а также пункт об ответственности за их разглашение.
Если доступ работника к ПДн не предусмотрен его должностными обязанностями, то право доступа к подобной информации предоставляется работнику только с его письменного согласия.
При принятии решения о допуске работника к ПДн, с ним заключается Соглашение о неразглашении ПДн. Одновременно с подписанием Соглашения осуществляется ознакомление работника с:
- утвержденным перечнем ПДн;

- установленным режимом конфиденциальности и мерами ответственности за его нарушение.

В структурных подразделениях предприятия должен вестись учет работников, получивших доступ к ПДн.
Доступ работника к ПДн, обрабатываемых на предприятии, прекращается по решению работодателя, в случаях:
- нарушения работником установленного режима конфиденциальности;
- прекращения трудовых отношений;
- предоставления работником подложных документов или заведомо ложных сведений при заключении трудового договора;
- привлечения работника к уголовной ответственности.

Прекращение доступа к ПДн, обрабатываемым в ИСПДн предприятия, не освобождает работника от взятых им обязательств по неразглашению указанных сведений.
Руководитель подразделения несет персональную ответственность за соблюдение режима конфиденциальности в подразделении и выполнение работниками требований внутренних нормативных документов предприятия, регламентирующих вопросы защиты информации.
Руководитель структурного подразделения обязан создать своим работникам, допущенным к ПДн, следующие условия, обеспечивающие соблюдение ими установленного на предприятии режима конфиденциальности:
- предоставить рабочее место в помещении, отвечающем требованиям обеспечения сохранности ПДн;
- обеспечить сейфами (шкафами) для хранения материальных носителей информации конфиденциального характера;
- установить на АРМ необходимые средства защиты информации;
- ознакомить под роспись с правилами работы с ПДн, обрабатываемыми в ИСПДн.

Руководители структурных подразделений должны обеспечивать поддержание соответствующего режима доступа в помещения, в которых расположены технические средства АС, исключающего несанкционированное нахождение в них посторонних лиц и использование ими технических средств АС.
Требования настоящего документа обязательны для всех работников предприятия, допущенных к работе с ПДн.
Работники, ознакомленные в установленном порядке с положениями настоящего документа, а также иных документов (политики, руководства, инструкции), разработанных в дополнение к данному документу и регламентирующих вопросы информационной безопасности, в случае допущений нарушения в работе с ПДн несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
Работники структурного подразделения, ответственного за обеспечение безопасности информации предприятия несут ответственность за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ, в соответствие с внутренними документами предприятия и условиями трудового соглашения (контракта), вплоть до увольнения.

Порядок обеспечения безопасности информации, в том числе порядок проведения анализа защищенности определяется инструкциями администратора безопасности, пользователя, и другими внутренними документами предприятия.
Порядок учета сторонних лиц и организаций, которым ПДн были предоставлены или переданы, определяется внутренними документами предприятия.

3.5 Порядок разработки и модернизации СЗИ

Разработка СЗИ может осуществляться как ответственным подразделением (уполномоченным лицом), так и другими специализированными, организациями, имеющими лицензии ФСТЭК России и (или) ФСБ на соответствующий вид деятельности.
В случае разработки СЗИ или ее отдельных компонентов специализированными организациями, должны быть назначены ответственные за организацию и проведение мероприятий по защите информации. Привлечение специализированных компаний допускается к решению задач по проектированию, созданию, внедрению и/или обслуживанию СЗИ предприятия. Задачи, функции и требования к проведению работ данными организациями определяются в ТЗ на данные работы (либо в ЧТЗ на спецработы).
Разработка и внедрение СЗИ осуществляется во взаимодействии разработчика со структурным подразделением или организацией, обеспечивающей функционирование ИСПДн, которая осуществляет методическое руководство и участвует в разработке, конкретных требований по защите информации, аналитическом обосновании необходимости создания СЗИ, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможных каналов утечки информации или воздействий на нее и предупреждению утечки и нарушения целостности защищаемой информации, в аттестации объектов информатизации.
В случае привлечения специализированной компании к выполнению либо организации работ по проектированию, созданию, внедрению и/или обслуживанию ИС, необходимо обеспечить защиту ПДн, доступ к которым был получен при проведении работ с информационными ресурсами предприятия.

Порядок разработки, ввода в действие и эксплуатации СЗИ

При обеспечении защиты информации ИСПДн должны быть выполнены следующие этапы работ:
- этап предпроектных изысканий;
- этап проектирования и разработки
- этап ввода в действие СЗИ
- этап эксплуатации.

На этапе предпроектных изысканий выполняются следующие работы:
- проведение обследования ИСПДн;
- исследование и категорирование информации, циркулирующей в ИСПДн;
- определение класса защищенности ИСПДн;
- разработка и анализ моделей угроз, уязвимостей, способов их реализации;
- разработка технических требований к защите информации.

На этапе проектирования и разработки выполняются следующие работы:
- разработка (эскизное, техническое и рабочее проектирование) и реализация системы мероприятий по обнаружению, локализации, нейтрализации воздействия угроз безопасности информации и устранению уязвимостей;
- определение подразделений и лиц, ответственных за эксплуатацию СрЗИ, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;
- разработка эксплуатационной документации, а также организационно-распорядительной документации по защите информации.

На этапе ввода в эксплуатацию выполняются следующие работы
- опытная эксплуатация СрЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания СрЗИ;
- декларирование на соответствие требованиям безопасности.

На этапе эксплуатации ИСПДн выполняется проведение мероприятий по контролю состояния защищенности.