ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«МЕЖРЕГИОНАЛЬНЫЙ СПЕЦИАЛИЗИРОВАННЫЙ
ФИНАНСОВО-ПРОМЫШЛЕННЫЙ РЕГИСТРАТОР
«СИБИРСКИЙ РЕЕСТР»

УТВЕРЖДЕНО
Приказом Генерального директора
ОАО «Сибирский реестр»
от 30 июня 2011 г. № 74/1

И.В. Казакова

Положение по обработке персональных данных

г. Новосибирск
2011 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящее Положение по обработке персональных данных (далее по тексту – Положение) определяет общий порядок получения, обработки, хранения, передачи и иного использования персональных данных Открытым акционерным обществом «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр» (далее по тексту - Регистратор), осуществляющего деятельность по ведению реестра владельцев именных ценных бумаг.

1.2.Настоящее Положение разработано на основании нормативно-правовых актов:

Федерального закона от 22.04.1996 г. № 39-ФЗ «О рынке ценных бумаг»;

Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Конвенции о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28 января 1981 г.;

Федерального закона от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 08.08.2001 г. № 128 «О лицензировании отдельных видов деятельности»;

Федерального закона от 07.07.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем»;

Трудового кодекса Российской Федерации (ТК РФ), от 30.12.2001 г. № 197-ФЗ (гл. 14);

Постановления Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

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

Постановления ФКЦБ России от 02.10.1997 г. № 27 «Об утверждении Положения о ведении реестра владельцев именных ценных бумаг»;

Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 г. № 58 г. Москва «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

иными нормативными актами в области защиты персональных данных.

1.3. Обработка, хранение, передача и иное использование персональных данных должна осуществляться на основе следующих принципов:

1)законности целей и способов обработки персональных данных и добросовестности;

2)соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям персональных данных;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных.

1.4.Требования настоящего Положения распространяются на всех работников Регистратора, допущенных к информации персональных данных.

Работники Регистратора, допущенные к информации персональных данных, несут персональную ответственность (дисциплинарную, административную. уголовную) за нарушение требований настоящего Положения и действующего законодательства о персональных данных.

1.5.В настоящем Положении используются следующие основные понятия:

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу: клиенту Регистратора (зарегистрированному лицу, а также его уполномоченным представителям); работнику Регистратора (далее - субъектам персональных данных);

трансфер-агент – юридическое лицо, которое на основании договора с Регистратором имеет право принимать от зарегистрированных лиц документы на совершение операций в реестре, передавать Регистратору подлинники документов на совершение операций в реестре, передавать зарегистрированным лицам, а также их уполномоченным представителям выписки из реестра, полученные от Регистратора;

обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу) персональных данных;

распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно - телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

конфиденциальность персональных данных – обязательное для соблюдения Регистратором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных и/или в виде файлов, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования;

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

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

модель угроз – документ, содержащий перечень возможных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и характеризующий наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации угроз безопасности персональных данных;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам;

правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

система защиты персональных данных – совокупность организационных мер и программно-технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технических мероприятия, обеспечивающие безопасность персональных данных;

специальные информационные системы персональных данных – информационные системы персональных данных, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищённость от уничтожения, изменения, блокирования, а также иных несанкционированных действий);

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

уполномоченное лицо по обработке персональных данных – работник Регистратора, осуществляющий на основании трудового договора с Регистратором и должностной инструкции функции по обработке и обеспечению безопасности персональных данных в процессе их обработки;

частная модель угроз – модель угроз применительно к конкретным условиям функционирования ИСПДн.

2. ПОРЯДОК ДЕЙСТВИЙ РЕГИСТРАТОРА, ТРАНСФЕР - АГЕНТОВ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1.Цели и обработка персональных данных и их структура

2.1.1.Обработка персональных данных осуществляется Регистратором:

а)в процессе профессиональной деятельности на рынке ценных бумаг;

б)в процессе взаимодействия с работниками Регистратора при осуществлении ими своей трудовой деятельности.

2.1.2.Обработка персональных данных клиентов Регистратора при осуществлении своей профессиональной деятельности на рынке ценных бумаг осуществляется в целях реализации функций Регистратора по ведению реестра владельцев именных ценных бумаг.

Указанная деятельность, являясь профессиональной и лицензируемой, осуществляется в порядке, предусмотренном Федеральным законом «О рынке ценных бумаг», а также иными правовыми актами, регламентирующими профессиональную деятельность организаций на рынке ценных бумаг.

2.1.3.Трансфер-агент осуществляет обработку персональных данных на основании заключенного договора с Регистратором в целях реализации своих функций по приему от зарегистрированных лиц документов на совершение операций в реестре, передаче Регистратору подлинников документов на совершение операций в реестре, передаче зарегистрированным лицам выписок из реестра, полученных от Регистратора.

2.1.4.Обработка персональных данных, сопряженная с выполнением указанных функций Регистратора и Трансфер-агента, не требует согласия субъектов персональных данных и осуществляется на основе заключенных с эмитентами договоров на ведение реестра владельцев именных ценных бумаг.

2.1.5.Регистратор и Трансфер-агент осуществляет обработку следующей информации, относящейся к персональным данным клиентов:

- фамилия, имя, отчество (если иное не вытекает из закона или национального обычая);
- дата и место рождения;
- адреса места жительства (регистрации) и места пребывания;
- гражданство;
- сведения о документе, удостоверяющем личность (вид, серия и номер документа, дата выдачи и орган, его выдавший);
- данные миграционной карты (при наличии) (серия и номер карты, дата начала срока пребывания и дата окончания срока пребывания);

- данные документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации (серия (при наличии) и номер документа, дата начала срока действия права пребывания (проживания), дата окончания срока действия права пребывания (проживания));
- индивидуальный номер налогоплательщика (ИНН) (при наличии);
- номер телефона;
- адрес электронной почты;
- сведения о принадлежащих клиентам правах на ценные бумаги;
- банковские реквизиты;
- почтовый адрес.

2.1.6.Обработка персональных данных работников Регистратора при осуществлении ими своей трудовой деятельности производится в целях обеспечения соблюдения трудового законодательства Российской Федерации, обучения, обеспечения личной безопасности сотрудника, а также учета результатов исполнения им должностных обязанностей.

Уполномоченное лицо Регистратора истребует персональные данные у работника. В случае возникновения необходимости получения персональных данных работника Регистратора у третьей стороны следует известить об этом работника заранее, получить его письменное согласие и сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных.

2.1.7.Регистратор осуществляет обработку следующей информации, относящейся к персональным данным работника:

- фамилия, имя и отчество;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства и регистрации;
- контактный телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, аттестации, служебным расследованиям;
- другие сведения, предусмотренные законодательством.

2.1.8.При обработке персональных данных Регистратору и Трансфер-агенту запрещается получать, обрабатывать персональные данные о политических, религиозных и иных убеждениях, частной жизни субъекта персональных данных, его членстве в общественных объединениях, в том числе в профессиональных союзах.

2.1.9.При обработке персональных данных Регистратором и Трансфер-агентом обеспечивается конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

2.1.10.Регистратор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 7 рабочих дней с даты получения запроса.

2.2.Взаимодействие Регистратора с субъектами персональных данных

2.2.1.Взаимодействие Регистратора с клиентами осуществляется в порядке, предусмотренном Федеральным законом «О рынке ценных бумаг», нормативными актами Федерального органа исполнительной власти на рынке ценных бумаг, а также иными правовыми актами, регламентирующими профессиональную деятельность организаций на рынках ценных бумаг.

2.2.2.Взаимодействие Трансфер-агентов с клиентами осуществляется в порядке, предусмотренном Федеральным законом «О рынке ценных бумаг», нормативными актами Федерального органа исполнительной власти на рынке ценных бумаг и условиями заключенного договора с Регистратором.

2.2.3.При получении персональных данных клиентов от Трансфер-агентов Регистратор не обязан информировать об этом указанных субъектов персональных данных.

2.2.4.Взаимодействие Регистратора с работниками осуществляется в порядке, предусмотренном Трудовым кодексом Российской Федерации, заключенными трудовыми договорами, должностными инструкциями, а также внутренними документами Регистратора.

2.2.5.Передача персональных данных третьим лицам не допускается без письменного согласия клиентов и работников Регистратора, за исключением случаев, установленных действующим законодательством, в том числе законодательством о рынке ценных бумаг, трудовым законодательством.

2.2.6.В случае выявления неправомерных действий с персональными данными Регистратор в срок, не превышающий трех рабочих дней с момента выявления, обязан устранить допущенные нарушения. Об устранении допущенных нарушений обработки персональных данных Регистратор обязан уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

2.2.7.В случае выявления факта недостоверности персональных данных клиента Регистратор на основании документов, представленных субъектом персональных данных, обязан уточнить персональные данные.

2.2.8.В случае изменения своих персональных данных клиент должен вновь предоставить Регистратору документ, содержащий необходимые сведения о субъекте в полном объеме (анкета зарегистрированного лица и иные документы, предусмотренные Правилами ведения реестра владельцев именных ценных бумаг Регистратора).

2.2.9.Обработка персональных данных клиента должна быть прекращена Регистратором, а сами персональные данные клиента должны быть уничтожены по истечении срока, установленного нормативными актами Российской Федерации.

2.2.10.Обработка персональных данных работника Регистратора должна быть прекращена, а сами персональные данные работника по истечении 1 года после прекращения с ним трудовых отношений переданы в архив для хранения в соответствии с требованиями законодательства об архивном деле и кадровом делопроизводстве.

2.2.11.Субъект персональных данных имеет право:

1)на получение следующей информации:

-о Регистраторе;

-о месте нахождения Регистратора;

-о наличии у Регистратора персональных данных субъекта;

2)на ознакомление со своими персональными данными.

2.2.12.Доступ к своим персональным данным предоставляется Регистратором субъекту персональных данных или его законному представителю при обращении либо при получении запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных (законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

2.2.13.Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1)подтверждение факта обработки персональных данных Регистратором и цель такой обработки;

2)способы обработки персональных данных, применяемых Регистратором;

3)сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4)перечень обрабатываемых персональных данных и источник их получения;

5)сроки обработки персональных данных, в том числе сроки их хранения;

6)сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

2.2.14.Регистратор обязан предоставить субъекту персональных данных информацию в соответствии с пунктами 2.2.11 и 2.2.13 настоящего Положения в течение 10 рабочих дней с момента обращения (получения запроса) субъекта персональных данных или его законного представителя.

2.3.Риски, возникающие при обработке Регистратором персональных данных

2.3.1.Обработка Регистратором персональных данных влечет за собой определенные риски для субъекта персональных данных, связанные с искажением или уничтожением персональных данных в результате недобросовестных действий третьих лиц, а также ошибочных и/или противоправных действий работников Регистратора в процессе обработки персональных данных, в том числе с использованием электронного документооборота.

В случае реализации названных рисков клиент вправе требовать исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства в области персональных данных, с учетом требований законодательства на финансовом рынке.

2.3.2.Виды рисков, возникающих при обработке Регистратором персональных данных:

1)технологические риски – риски необеспечения (ненадлежащего обеспечения) порядка обработки персональных данных с использованием информационной системы персональных данных вследствие неэффективности и/или неадекватности технологий, порядка и способов использования информационной системы персональных данных;

2)операционные риски – риски возникновения нарушений при обработке персональных данных вследствие ненадлежащих действий работников Регистратора, ненадлежащего функционирования аппаратно-программного обеспечения информационной системы персональных данных;

3)криминальные риски – риски совершения работниками Регистратора, иными лицами, умышленных действий в целях неправомерного получения и использования персональных данных;

4)форс-мажорные риски – риски нарушения деятельности Регистратора при обработке персональных данных, целостности информационной системы персональных данных, вследствие возникновения непредотвратимых (форс-мажорных) чрезвычайных ситуаций техногенного, природного и социального характера.

2.3.3.Меры снижения технологических рисков Регистратора при обработке персональных данных:

1)обеспечение идентификации уполномоченного лица по обработке персональных данных с использованием информационной системы персональных данных;

2)обеспечение целостности информационной системы персональных данных;

3)установление требований к порядку осуществления документооборота, в т.ч. электронного;

4)обеспечение исполнения требований к форматам и реквизитам электронного документа.

2.3.4.Меры снижения операционных рисков Регистратора при обработке персональных данных:

1)разделение полномочий и служебных обязанностей уполномоченных работников Регистратора, осуществляющих обработку персональных данных;

2)осуществление контроля за надлежащим исполнением работниками Регистратора своих служебных обязанностей, связанных обработкой персональных данных;

3)определение порядка выявления ошибок (ошибочных действий), совершенных работниками Регистратора, осуществляющими обработку персональных данных, и порядка их устранения;

4)установление Регистратором и исполнение им требований по надежности и отказоустойчивости системы персональных данных.

2.3.5.Меры снижения криминальных рисков Регистратора при обработке персональных данных:

1)установление защиты персональных данных от несанкционированного доступа (в т.ч. с использованием вредоносных программ);

2)обеспечение владельцами сертификатов ключей сохранность в тайне ключей электронной цифровой подписи (в случае использования электронного документооборота при обработке персональных данных);

3)осуществление расследования случаев неправомерного предоставления и/или использования персональных данных, неисполнения (ненадлежащего исполнения) своих служебных обязанностей работниками Регистратора.

2.3.6.Меры снижения форс-мажорных рисков Регистратора при обработке персональных данных:

1)осуществление защиты персональных данных, в случае возникновения чрезвычайных ситуаций, в т.ч. с использованием систем и средств резервного копирования;

2)применение Регистратором резервных источников питания, систем бесперебойного питания, средств безаварийного завершения работы при использовании информационной системы персональных данных для обработки персональных данных;

3)применение Регистратором средств защиты от поражения вредоносными программами (вирусы, «трояны», сетевые «черви» и т.п.) при использовании информационной системы персональных данных для обработки персональных данных.

2.3.7.Компенсационные инструменты, применяемые Регистратором при обработке персональных данных:

1)собственные средства Регистратора;

2)страхование профессиональной деятельности Регистратора.

2.4.Методика классификации информационных систем персональных данных

2.4.1.Классификация информационных систем Регистратора является обязательной процедурой, осуществляемой с учетом категорий и объема обрабатываемых персональных данных, а также в соответствии с нормативно – правовыми актами уполномоченных органов.

2.4.2.Регистратор определяет порядок действий при классификации информационных систем персональных данных, включающий:

1)назначение ответственных лиц;

2)определение границ контролируемых зон в виде доступа к информационным системам персональных данных;

3)утверждение генеральным директором Регистратора перечня защищаемой информации, составляющей коммерческую тайну и служебную информацию, в которую входят персональные данные клиентов и работников Регистратора;

4)утверждение генеральным директором Регистратора разграничения прав доступа к защищаемым ресурсам в информационной системе персональных данных в соответствии с Приложением № 1 настоящего Положения.

2.4.3.Регистратор проводит анализ информационных систем персональных данных, включающий классификацию и описание операций, связанных с обработкой персональных данных и определение программных и/или аппаратно – программных средств, с помощью которых реализуются указанные процедуры.

2.4.4.Порядок действий должностных лиц Регистратора при классификации информационных систем персональных данных:

1)генеральный директор Регистратора назначает уполномоченных лиц для проведения классификации информационных систем персональных данных. В состав уполномоченных лиц, ответственных за классификацию информационных систем персональных данных, включаются представители подразделений, осуществляющих обработку персональных данных, работники подразделений информационных технологий и информационной безопасности;

2)уполномоченные лица Регистратора, ответственные за классификацию информационных систем персональных данных, должны изучить классификационные признаки информационных систем персональных данных, влияющие на определение их класса.

2.4.5.Уполномоченные лица Регистратора при проведении классификации информационной системы должны учитывать следующие характеристики информационной системы:

1)категорию обрабатываемых в информационной системе персональных данных – $X_{ПД}$;

2)объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – $X_{НПД}$;

3)характеристики безопасности персональных данных, обрабатываемых в информационной системе;

4)структуру информационной системы (автономная, локальная или распределённая);

5)наличие подключений информационной системы к сетям общего пользования и (или) сетям международного информационного обмена;

6)режим обработки персональных данных (однопользовательский или многопользовательский);

7)режим разграничения прав доступа пользователей информационной системы (Приложение № 1 к настоящему Положению);

8)местонахождение программно-технических средств информационной системы (внутри контролируемой зоны или за ее пределами);

9)наличие зарегистрированного в саморегулируемой организации договора страхования деятельности Регистратора, покрывающего риски, связанные с электронными и компьютерными преступлениями, утратой персональных данных, техническими ошибками или сбоями программно - аппаратных средств при обработке персональных данных.

2.4.6.Существуют следующие категории обрабатываемых в информационной системе персональных данных ($X_{ПД}$):

1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

4 – обезличенные и (или) общедоступные персональные данные.

2.4.7.В зависимости от объема обрабатываемых персональных данных $X_{НПД}$ принимает одно из следующих значений:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

2.4.8.Уполномоченные лица Регистратора, ответственные за классификацию информационных систем персональных данных, разрабатывают акт классификации информационных систем персональных данных, учитывающий требования раздела 2.4.5 настоящего Положения по форме Приложения № 2.

2.4.9.Акт классификации информационной системы персональных данных должен быть подписан и утвержден генеральным директором Регистратора.

2.4.10.Итогом классификации информационной системы персональных данных является присвоение ей класса информационной безопасности (К1, К2, К3, К4), соответствующего ее индивидуальным признакам и учитывающего модель угроз безопасности информационной системы персональных данных:

1)класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

2)класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

3)класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

4)класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

2.4.11.Класс информационной системы может быть пересмотрен по решению генерального директора Регистратора на основе проведенного им анализа и оценки угроз безопасности персональных данных с учетом особенностей и/или изменений конкретной информационной системы или по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

2.5.Организационные меры по защите персональных данных

2.5.1.Регистратор при обработке персональных данных принимает необходимые организационные меры, направленные на защиту персональных данных клиентов и работников, а также соблюдает требования нормативных актов, регулирующих профессиональную деятельность Регистратора на рынке ценных бумаг.

2.5.2.Организационные меры по защите персональных данных регламентированы порядком, устанавливающим:

1)требования к помещению, в котором осуществляется обработка персональных данных;

2)требования к работникам, осуществляющих обработку персональных данных.

2.5.3.Требования, предъявляемые к помещению, в котором осуществляется обработка персональных данных:

2.5.3.1.Регистратор при осуществлении профессиональной деятельности на рынке ценных бумаг использует следующие специальные помещения: операционный зал, архив и серверная комната.

2.5.3.2.Регистратором определен порядок доступа работников в помещения, в которых ведется обработка персональных данных.

2.5.3.3. Доступ в помещения, в которых ведется обработка персональных данных, ограничен, а помещение защищено от внешних воздействий и других причин, которые могут повлечь утрату или искажение персональных данных.

2.5.4.Требования, предъявляемые к работникам Регистратора, осуществляющим обработку персональных данных:

2.5.4.1.Доступ к персональным данным имеют работники Регистратора, которые в соответствии со своими должностными инструкциями имеют доступ к системам ведения реестра владельцев именных ценных бумаг и персональным данным работников Регистратора.

2.5.4.2.Регистратор включает в должностные инструкции работников положения об ответственности за разглашение служебной тайны, которая включает в себя информацию о персональных данных.

2.5.4.3.Регистратор включает в трудовые договора, которые заключаются с работниками Регистратора, положения о неразглашении служебной и конфиденциальной информации.

2.5.4.4.Работники Регистратора, осуществляющие обработку персональных данных, должны быть ознакомлены под роспись с настоящим Положением.

2.5.4.5.Регистратор определяет порядок контроля за выполнением работниками требований по обеспечению безопасности персональных данных в информационных системах персональных данных в соответствии со своими внутренними документами.

2.6.Технические меры по защите персональных данных

2.6.1.Размещение технических средств (серверов, активного сетевого и телекоммуникационного оборудования) осуществляется в выделенных серверных помещениях. Остальные технические средства размещены в рабочих помещениях Регистратора, закрытых для постороннего доступа.

2.6.2.Серверное помещение Регистратора оборудовано системой контроля доступа. Идентификационные средства доступа в серверное помещение выдаются только уполномоченным работникам.

2.6.3.Используемые электрические сети и электрооборудование должны отвечать требованиям действующих «Правил устройства электроустановок» и «Правил технической эксплуатации электроустановок потребителей».

2.6.4.Серверы и телекоммуникационное оборудование подключаются к источникам бесперебойного питания, обеспечивающих их работу в течение времени, достаточного для корректного завершения работы после прекращения основного электроснабжения. Технические средства, эксплуатируемые на рабочих местах работников Регистратора, также оборудуются источниками бесперебойного питания.

2.6.5.Серверное помещение оборудуется средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

2.6.6.Серверное помещение оборудовано пожарной сигнализацией.

2.6.7.Хранение документированной информации осуществляется в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу, внутренними документами Регистратора.

2.6.8.Регистратор осуществляет резервное копирование информационной системы персональных данных в соответствии с политикой информационной безопасности.

3. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ И РАЗРАБОТКИ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.Угрозами безопасности персональных данных при их обработке в информационных системах является совокупность условий и факторов, создающих опасность несанкционированного доступа к персональным данным, результатом которых может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные действия при их обработке.

3.2.Угрозы безопасности персональных данных могут быть реализованы за счет их утечки по техническим каналам или вследствие несанкционированного доступа, в том числе с использованием соответствующего программного обеспечения.

3.3.Источниками угроз несанкционированного доступа к персональным данным с использованием программного обеспечения являются лица, действия которых нарушают правила разграничения доступа к информации в информационных системах.

3.4.Возможности нарушителя зависят от установленного порядка допуска физических лиц к информационным ресурсам и мер по контролю порядка проведения работ.

3.5.Выявление угроз, реализуемых с применением программных и аппаратно - программных средств, осуществляется как с помощью специальных средств для подтверждения наличия и выявления недостатков программного и аппаратного обеспечения (сетевых сканеров), так и путем опроса работников и должностных лиц Регистратора, а также изучение публикуемых обзоров уязвимостей.

3.6.Детальное описание угроз, связанных с утечкой персональных данных по техническим каналам и несанкционированным доступом к ним, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Приложение № 5 настоящего Положения).

3.7.На основе сетевого сканирования, опроса работников и должностных лиц, а также данных обследования информационной системы персональных данных составляется модель угроз безопасности информационной системы персональных данных (Приложение № 5 настоящего Положения).

3.8.Возможность реализации той или иной угрозы оценивается по уровню исходной защищенности информационной системы персональных данных и вероятности ее реализации. Показатели исходной защищенности приведены в Приложении № 3 настоящего Положения.

3.9.Исходная степень защищенности определяется следующим образом:

3.9.1.Информационная система имеет **высокий** уровень исходной защищенности, если не менее 70 % ее характеристик соответствуют уровню «высокий», а остальные – среднему уровню защищенности.

3.9.2.Информационная система имеет **средний** уровень исходной защищенности, если не выполняются условия по пункту 3.9.1. и не менее 70 % ее характеристик соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности.

3.9.3.Информационная система имеет **низкую** степень исходной защищенности, если не выполняются условия по пунктам 3.9.1. и 3.9.2 настоящего Положения.

3.10.При разработке модели угроз безопасности информационной системы персональных данных каждой степени исходной защищенности присваивается числовой коэффициент Y_1 (0 – для высокой степени исходной защищенности; 5 – для средней степени исходной защищенности; 10 – для низкой степени исходной защищенности).

3.11.Для показателя «вероятность реализации угрозы» вводятся следующие градации:

маловероятно – отсутствуют предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где хранятся персональные данные);

низкая вероятность – предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности персональных данных недостаточны;

высокая вероятность - предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности персональных данных не приняты.

3.12.При разработке модели угроз безопасности информационной системы персональных данных каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2 (0 – для маловероятной угрозы; 2 – для низкой вероятности угрозы; 5 – для средней вероятности угрозы; 10 – для высокой вероятности угрозы).

3.13.Далее определяется коэффициент реализуемости угрозы Y соотношением $Y = (Y_1 + Y_2) / 20$.

3.14.По значению коэффициента реализуемости угрозы Y формируется следующая интерпретация реализуемости угрозы:

если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается **низкой**;

если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается **средней**;

если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается **высокой**;

если $Y > 0{,}8$, то возможность реализации угрозы признается **очень высокой**.

3.15.Далее оценивается показатель опасности каждой угрозы, который может принимать следующие значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

3.16.Затем осуществляется выбор актуальных для данной информационной системы угроз безопасности, в соответствии с правилами, приведенными в Приложении № 4 настоящего Положения.

3.17.На заключительном этапе разработки модели угроз формулируются конкретные технические и организационные меры по противодействию выявленным актуальным угрозам, с использованием данных о классе информационной системы персональных данных и на основе рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

3.18.Примерный результат разработки модели угроз безопасности информационной системы персональных данных Регистратора приведен в Приложении № 5 настоящего Положения.

Приложение № 1
к Положению об обработке персональных данных

УТВЕРЖДАЮ
Генеральный директор ОАО «Сибирский реестр»
_____ И.В. Казакова

«___» _____20__ г.

Таблица разграничения прав доступа
к защищаемым ресурсам в информационной системе

п/п	ЗАЩИЩАЕМЫЕ РЕСУРСЫ					Допуск к ресурсу	Виды доступа в соответствии с возможностями системы
	Наименование ресурса, АРМа	Здание, № помещения	Условное имя группы пользователей	Путь доступа к ресурсу	Гриф секретности		
1	2	3	4	5	6	7	8
Задача:							
АППАРАТНО-ПРОГРАММНЫЕ КОМПЛЕКСЫ							

Приложение № 2
к Положению об обработке персональных данных

УТВЕРЖДАЮ
Генеральный директор ОАО «Сибирский реестр»
_____ И.В. Казакова

«___» _____20__ г.

Акт классификации
информационной системы персональных данных
«Система ведения реестра владельцев ценных бумаг»
Открытого акционерного общества «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр»

Классификация информационной системы персональных данных проводится на основании «Порядка проведения классификации информационных систем персональных данных», утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва.

Открытое акционерное общество «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр» ведет свою деятельность по ведению реестра владельцев именных ценных бумаг на основании лицензии № 10-000-1-00311, выданной 19.03.2004 г. ФКЦБ РФ, и осуществляет сбор идентификационных данных клиентов (зарегистрированных лиц) и учет их прав в отношении ценных бумаг эмитентов, с которыми заключены договора на ведение реестра владельцев именных ценных бумаг.

Исходные данные:
Категория обрабатываемых персональных данных;
Объем обрабатываемых персональных данных;
Характеристики безопасности персональных данных;
Структура информационной системы;
Режим обработки персональных данных;
Режим разграничения прав доступа пользователей;
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена;
Место нахождение технических средств информационной системы;
Наличие зарегистрированного в саморегулируемой организации договора страхования учетного института, покрывающие риски, связанные с электронными и компьютерными преступлениями, утратой, техническими ошибками или сбоями программно – аппаратных средств, при обработке персональных данных.

Основные виды деятельности:

1) Ведение реестра владельцев именных ценных бумаг.

В идентификационные данные включены персональные данные, которые позволяют идентифицировать клиентов (зарегистрированных лиц), учитываемых в реестрах владельцев именных ценных бумаг эмитентом, с которыми заключены договора. Необходимый и достаточный перечень персональных данных включает в себя:

фамилия, имя, отчество;
гражданство;

вид, номер, серия, дата и место выдачи документа, удостоверяющего личность, а также наименование органа, выдавшего документ;
год и дата рождения;
место проживания (регистрации);
адрес для направления корреспонденции (почтовый адрес);
права в отношении ценных бумаг.
другое.

Открытое акционерное общество «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр» имеет информационную систему – «Система ведения реестра владельцев ценных бумаг», которая позволяет обрабатывать персональные данные клиентов с использованием средств автоматизации - программным обеспечением «ЗЕНИТ-Р» («ЗЕНИТ-Р.ОФИС», «ЗЕНИТ-Р.ФИЛИАЛ», ЗЕНИТ-Р.АГЕНТ») (далее по тексту – информационная система).

Персональные данные, обрабатываемые информационной системой согласно классификатору, определяются, как персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1 (категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни) ($X_{пд}$ = категория 2).

Информационная система обрабатывает персональные данные более 100 000 ($X_{нпд}$ = 1).

Информационная система является специальной информационной системой.

По структуре информационная система является распределенной информационной системой (комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа), так как Открытое акционерное общество «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр» имеет территориально распределенные филиалы:

Ангарский филиал (г. Ангарск, ул. К.Маркса, 25);

Барнаульский филиал (г. Барнаул, ул. Пионеров, 5);

Бийский филиал (г. Бийск, ул. Социалистическая, 1);

Новосибирский филиал «Независимый регистратор» (Новосибирская область, пос. Краснообск, 5-й микрорайон, д. 2, корп. 4);

Приморский филиал (г. Владивосток, ул. Березовая, 25);

Славгородский филиал (с. Славгород, ул. Титова, 167);

Филиал «Амурреестр» г. Благовещенск (г. Благовещенск, ул. Зейская, 156/2);

Филиал «Находка» (г. Находка, ул. Пограничная, 6).

Информационная система подключена к сетям связи общего пользования. Информационная система не подключена к сетям международного информационного обмена.

Информационная система является многопользовательской. При этом в информационной системе присутствует разграничение прав доступа пользователей.

Все технические средства информационной системы находятся внутри контролируемой зоны.

Открытое акционерное общество «Межрегиональный специализированный финансово-промышленный регистратор «Сибирский реестр» имеет зарегистрированный в саморегулируемой организации договор страхования, покрывающий риски, связанные с электронными и компьютерными преступлениями, утратой, техническими ошибками или сбоями программно – аппаратных средств, при обработке персональных данных.

Результаты анализа.

На основании исходных данных $X_{пд}$ = категория 2 и $X_{нпд}$ = 1 (более 100 000)

$X_{пд}$ \ $X_{нпд}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Информационной системе присваивается класс - класс К1.

По результатам анализа информационная система является многопользовательской, специальной, распределенной, информационной системой класса К1 с разграничением доступа и подключением к сетям связи общего пользования, находящейся на территории Российской Федерации.

Приложение № 3
к Положению об обработке персональных данных

**Показатели исходной защищенности
информационной системы персональных данных**

Технические и эксплуатационные характеристики информационной системы персональных данных	Уровень защищенности		
	Высокий	Средний	Низкий
По территориальному размещению			
распределенная, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная, развернутая в пределах одного здания.	+	–	–
По наличию соединения с сетями общего пользования:			
имеющая многоточечный выход в сеть общего пользования;	–	–	+
имеющая одноточечный выход в сеть общего пользования;	–	+	–
физически отделенная от сети общего пользования.	+	–	–
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача.	–	–	+
По разграничению доступа к персональным данным			

к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем информационной системы, либо субъект персональных данных;	–	+	–
к которой имеют доступ все сотрудники организации, являющейся владельцем информационной системы;	–	–	+
с открытым доступом.	–	–	+
По наличию соединений с другими базами персональных данных иных информационных систем			
интегрированная информационная система (организация использует несколько баз персональных данных, при этом организация не является владельцем всех используемых баз);	–	–	+
в которой используется одна база персональных данных, принадлежащая организации – владельцу данной информационной системы.	+	–	–
По уровню обобщения (обезличивания) персональных данных			
в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных).	–	–	+
По объему персональных данных, которые предоставляются сторонним пользователям информационной системы без предварительной обработки			
предоставляющая всю базу данных с персональными данными;	–	–	+
предоставляющая часть персональных данных;	–	+	–
не предоставляющая никакой информации.	+	–	–

Приложение № 4
к Положению об обработке персональных данных

Правила отнесения угроз безопасности персональных данных к актуальным

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Приложение № 5
к Положению об обработке персональных данных

УТВЕРЖДАЮ
Генеральный директор ОАО «Сибирский реестр»

_____ И.В. Казакова

«___» _____20__ г.

Базовая Модель угроз безопасности
информационной системы персональных данных
Открытого акционерного общества
«Межрегиональный специализированный финансово-промышленный регистратор
«Сибирский реестр»

Исходная степень защищенности информационной системы персональных данных: _____

Показатель защищенности Y_1 = _____(0 – для высокой степени исходной защищенности, 5 – для средней, 10 – для низкой)

Справочно:

Вероятность реализации Y_2 =
0 для малой вероятности угрозы;
2 для низкой вероятности угрозы;
5 для средней вероятности угрозы;
10 для высокой вероятности угрозы.

Коэффициент реализуемости угрозы
Y = (Y1 + Y2)/20.

Возможность реализации угрозы
$0 < Y < 0,3$, - низкая;
$0,3 < Y < 0,6$, - средняя;
$0,6 < Y < 0,8$, - высокая;
$Y > 0,8$, - очень высокая.

Наименование угрозы	**Вероятность реализации угрозы (Y_2)**	**Возможность реализации угрозы (Y)**	**Опасность угрозы**	**Актуальность угрозы**	**Меры по противодействию угрозе**	
					Технические	**Организационные**
Угрозы от утечки по техническим каналам						

Угрозы утечки акустической информации	Малая вероятность	Средняя	Низкая	Неактуальная		✓ Должностные инструкции работников ✓ Технологический процесс
Угрозы утечки видовой информации						
Просмотр информации на дисплее работниками, не допущенными к обработке персональных данных	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Система учета доступа в помещения ✓ Перегородки	✓ Должностные инструкции работников ✓ Порядок пропускного режима
Просмотр информации на дисплее посторонними лицами, находящимися в помещении в котором ведется обработка персональных данных	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Система учета доступа в помещения ✓ Перегородки	✓ Должностные инструкции работников ✓ Порядок пропускного режима ✓ Порядок расположения мониторов работников ✓ Проведение обслуживания клиентов и переговоров в специально отведенном помещении
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором ведется обработка персональных данных	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Жалюзи на окна ✓ Расположение офиса	✓ Порядок расположения мониторов работников
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	Низкая вероятность	Высокая	Средняя	Актуальная	✓ Система учета доступа в помещения.	✓ Порядок пропускного режима
Угрозы утечки информации по каналам ПЭМИН						

Утечка информации по сетям электропитания	Малая вероятность	Средняя	Низкая	Неактуальная		✓ Должностная инструкция системного администратора ✓ Технологический процесс обработки ✓ Установка средств защиты
Угрозы несанкционированного доступа к информации						
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
Кража ПК	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Охранная сигнализация ✓ Система контроля доступа в помещения ✓ Кодовый замок	✓ Порядок учета средств вычислительной техники ✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностные инструкции работников
Кража носителей информации	Низкая вероятность	Высокая	Средняя	Актуальная	✓ Система контроля доступа в помещения ✓ Кодовый замок ✓ Контроль вскрытия ПК и серверов	✓ Порядок учета средств вычислительной техники ✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностная инструкция системного администратора ✓ Должностные инструкции работников
Кража ключей доступа	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Хранение у круглосуточной охраны	✓ Должностные инструкции работников

Кражи, модификации, уничтожения информации.	Средняя вероятность	Высокая	Средняя	Актуальная	✓ Система разграничения прав доступа ✓ Охранная сигнализация ✓ Система контроля доступа в помещения ✓ Кодовый замок ✓ Введение журналов доступа к информации ✓ Система резервного копирования	✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора
Вывод из строя узлов ПК, каналов связи	Низкая вероятность	Средняя	Средняя	Актуальная	✓ Охранная сигнализация ✓ Система контроля доступа в помещения ✓ Кодовый замок ✓ Наличие резервных узлов ✓ Наличие резервных каналов связи	✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностная инструкция системного администратора
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПК	Низкая вероятность	Средняя	Средняя	Актуальная	✓ Система защиты от НСД ✓ Шифрование данных	✓ Ремонт силами работниками, имеющих доступ к ПДн
Несанкционированное отключение средств защиты	Средняя вероятность	Высокая	Средняя	Актуальная	✓ Настройка средств защиты	✓ Должностная инструкция системного администратора ✓ Должностные инструкции работников ✓ Технологический процесс обработки ПДн ✓ Установка средств защиты
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						

Компьютерные вирусы	Средняя вероятность	Высокая	Средняя	Актуальная	✓ Антивирусное ПО	✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора ✓ Технологический процесс обработки ПДн ✓ Установка средств защиты
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая вероятность	Средняя	Низкая	Неактуальная	✓ Ведение журналов учета работы ПО	✓ Сертификация используемого ПО
Установка ПО, не связанного с исполнением служебных обязанностей	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Настройка средств защиты ✓ Права пользователя на компьютере	✓ Должностная инструкция системного администратора
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Система контроля доступа в помещения	✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностная инструкция системного администратора ✓ Ввод в эксплуатацию средств вычислительной техники
Внедрение аппаратных закладок работниками Регистратора	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Настройка средств защиты	✓ Должностная инструкция системного администратора ✓ Должностные инструкции работников
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	Малая вероятность	Средняя	Низкая	Неактуальная		✓ Должностная инструкция системного администратора

Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
Утрата ключей доступа	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Централизованное хранение ключей доступа	✓ Порядок хранения, учета и использования ключей доступа ✓ Должностная инструкция системного администратора ✓ Должностные инструкции работников
Непреднамеренная модификация (уничтожение) информации работниками	Средняя вероятность	Высокая	Высокая	Актуальная	✓ Разграничение прав доступа к информации ✓ Настройка средств защиты ✓ Настройка системы резервного копирования	✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора ✓ Резервное копирование
Непреднамеренное отключение средств защиты	Средняя вероятность	Высокая	Низкая	Актуальная	✓ Доступ к установлению режимов работы средств защиты предоставляется только системному администратору ✓ Настройка средств защиты информации	✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора
Выход из строя аппаратно - программных средств	Средняя вероятность	Высокая	Средняя	Актуальная	✓ Наличие резервных узлов ✓ Наличие резервных каналов связи	✓ Резервирование
Сбой системы электроснабжения	Средняя вероятность	Высокая	Средняя	Актуальная	✓ Использование источника бесперебойного электропитания	✓ Резервное копирование
Стихийное бедствие	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Пожарная сигнализация	✓ Система оповещения
Угрозы преднамеренных действий внутренних нарушителей						

Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Малая вероятность	Средняя	низкая	Неактуальная	✓ Система защиты от НСД ✓ Охранная сигнализация ✓ Система контроля доступа в помещения ✓ Шифрование данных	✓ Порядок пропускного режима ✓ Круглосуточная охрана ✓ Должностная инструкция системного администратора ✓ Должностные инструкции работников
Разглашение информации, модификация, уничтожение работниками, допущенными к ее обработке	Высокая вероятность	Очень высокая	Высокая	Актуальная		✓ Положение в трудовых договорах с работниками о не разглашении конфиденциальной и служебной информации ✓ Должностные инструкции работников
Угрозы несанкционированного доступа по каналам связи						
Несанкционированный доступ через ЛВС организации	Низкая вероятность	Высокая	Средняя	Актуальная	✓ Система контроля доступа в помещения	✓ Технологический процесс ✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора ✓ Установка средств защиты
Утечка атрибутов доступа	Высокая вероятность	Высокая	Средняя	Актуальная		✓ Технологический процесс ✓ Должностные инструкции работников ✓ Должностная инструкция системного администратора ✓ Установка средств защиты
Угрозы перехвата при передаче по проводным (кабельным) линиям связи						

Перехват в пределах контролируемой зоны внешними нарушителями	Низкая	Высокая	Низкая	Актуальная	✓ Система контроля доступа в помещения ✓ Шифрование данных	✓ Пропускной режим ✓ Технологический процесс
Перехват в пределах контролируемой зоны внутренними нарушителями	Малая вероятность	Средняя	Низкая	Неактуальная	✓ Система контроля доступа в помещения ✓ Шифрование данных	✓ Технологический процесс