УТВЕРЖДАЮ

Генеральный директор
ЗАО «ИК «Питер Траст»

_____ А.В. Мамаев
(*подпись*) (*ФИО*)

«20» июня 2011г.

ПОЛИТИКА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ИНВЕСТИЦИОННАЯ КОМПАНИЯ «ПИТЕР ТРАСТ»

г. 2011г.

ВВЕДЕНИЕ

«Политика безопасности персональных данных» (далее – Политика) определяет стратегию защиты персональных данных, обрабатываемых в ИСПДн Закрытого акционерного общества «Инвестиционная компания «Питер Траст» (далее Организация) и формулирует основные принципы и механизмы защиты ПДн.

Политика является основным руководящим документом *Организации*, определяющим требования, предъявляемые к обеспечению безопасности ПДн.

Безопасность персональных данных достигается путем исключения 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.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Настоящий документ разработан в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и на основании положений Стандарта НАУФОР «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг».

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цель и область применения политики

Целью Политики является обеспечение безопасности персональных данных, а также реализация положений нормативных правовых актов и иных документов по защите персональных данных.

Основными целями обеспечения безопасности персональных данных являются:

- предотвращение нарушений прав субъекта персональных данных (физического лица) на сохранение конфиденциальности информации, обрабатываемой в ИСПДн *Организации*;
- предотвращение искажения или несанкционированной модификации информации, содержащей персональные данные, обрабатываемой в ИСПДн *Организации*;
- предотвращение несанкционированных действий по блокированию информации, содержащей персональные данные.

Требования настоящей Политики обязательны для всех структурных подразделений *Организации* и распространяются на:

- автоматизированные системы *Организации*;
- средства телекоммуникаций;
- информационные ресурсы и носители информации;
- помещения;

▪ работников *Организации*.

Внутренние документы *Организации*, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Политики и не противоречить им.

1.2. Состав персональных данных

В информационных системах *Организации* происходит обработка, передача, накопление и хранение информации, содержащей персональные данные и в соответствии с действующим законодательством Российской Федерации подлежащей защите.

В *Организации* определены следующие основания для обработки информации, содержащей персональные данные:

- Федеральный закон РФ от 27.07.06 № 152-ФЗ «О персональных данных».

Цель обработки информации, содержащей персональные данные:

осуществление Организацией своей основной деятельности в соответствии с Уставом.

Определен следующий перечень персональных данных, обрабатываемых в ИСПДн *Организации*, утвержденный Генеральным директором:

а) Касающиеся работников Организации

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- паспортные данные;
- ИНН
- данные страхового свидетельства государственного пенсионного страхования;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства, регистрации;
- домашний телефон;
- содержание трудового договора;
- 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;
- *иные персональные данные*.

Б) Касающиеся клиента Организации, его представителя и/или выгодоприобретателя:

- дата и место рождения;
- гражданство;
- адрес регистрации и адрес места жительства;
- почтовый адрес;
- сведения о документе, удостоверяющем личность;
- занимаемая должность;
- ИНН;
- домашний, рабочий, мобильный телефон, адрес электронной почты;
- сведения о банковских счетах, в том числе за рубежом;
- информация о ходе исполнения договора (соглашения), в т.ч. данные о совершенных операциях, денежных средствах и ином имуществе клиента;
- сведения о доходах;
- иные персональные данные, связанные с оказанием услуг клиенту.

1.3. Субъекты персональных данных:

▪ сотрудник Организации – субъект ПДн, являющийся работником Организации на основании ТК РФ;

▪ клиенты Организации – субъекты ПДн, являющиеся клиентами по договорам на брокерское обслуживание, доверительное управление ценными бумагами, договорам биржевого посредничества и иным договорам, связанным с деятельностью Организации - профессионального участника рынка ценных бумаг, в том числе представители клиентов, и их выгодоприобретатели.

1.4. Период хранения и обработки персональных данных

Период хранения и обработки персональных данных *определяется*[1] в соответствии со ст.21 Закона «О персональных данных», Федеральным Законом о бухгалтерском учете № 129-ФЗ от 21.11.1996г., Налоговым кодексом, Приказ Министерства культуры РФ от 25 августа 2010 г. N 558 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», Федеральным законом «Об акционерных Обществах», Постановление Федеральной комиссии по рынку ценных бумаг от 16 июля 2003 г. N 03-33/пс "Об утверждении Положения о порядке и сроках хранения документов акционерных обществ".

Обработка ПДн начинается с момента поступления персональных данных в ИСПДн и прекращается:

▪ в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, *Организация* устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений *Организация* в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных *Организация* уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, *Организация* уведомляет также указанный орган;

▪ в случае достижения цели обработки персональных данных *Организация* незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, *Организация* уведомляет также указанный орган;

▪ в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных *Организация* прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных *Организация* уведомляет субъекта персональных данных.

▪ в случае прекращения деятельности *Организации.*

[1] Приводятся конкретные статьи и наименования нормативно-правовых актов, которые определяют сроки хранения информации, содержащей ПДн, отличающиеся от требований 152-ФЗ, например: статьи 115-ФЗ, Трудового кодекса и т.п., с указанием максимальной продолжительности периода хранения и обработки ПДН.

2. ОБЩИЕ ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Организационная структура по обеспечению безопасности персональных данных

Структуру, обеспечивающую безопасность персональных данных, составляют лица, занимающие следующие должности:

- Уполномоченное лицо по обеспечению безопасности персональных данных в Организации (назначается приказом Генерального директора)
- Системный администратор;

Права, обязанности и ответственность вышеуказанных лиц в части обеспечение безопасности ПДн. определены должностными инструкциями.

Общее руководство системой обеспечения безопасности персональных данных осуществляет Уполномоченное лицо по обеспечению безопасности персональных данных (далее по тексту – Уполномоченное лицо).

Уполномоченное лицо отвечает за:

- методологическое обеспечение безопасности ПДн;
- формирование системы технической защиты ПДн;
- контроль выполнения мер и мероприятий по защите информации.
- проведение мероприятий по обеспечению безопасности ПДн;
- эксплуатацию технических и программных средств защиты ПДн;

Уполномоченное лицо обязано:

- проводить мониторинг защищённости всех компонентов ИСПДн;
- расследовать случаи как успешных, так и предотвращенных попыток НСД;
- вырабатывать рекомендации по повышению уровня защищённости ресурсов ИСПДн;
- контролировать действия администраторов ИСПДн;

Настройку и поддержку функционирования ИСПДн *Организации* осуществляет Системный администратор.

Системный администратор отвечает за:

- обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных;
- безотказное функционирование технических средств ИСПДн
- обеспечение штатного режима функционирования программного обеспечения серверов и рабочих станций ИСПДн.

Системный администратор обязан:

- осуществлять мониторинг состояния ресурсов и компонентов ИСПДн;
- осуществлять резервное копирование информации и обеспечивать оперативное восстановление систем при сбоях;
- своевременно принимать меры по модернизации программного и аппаратного обеспечения;
- устанавливать, настраивать и поддерживать работоспособность баз данных;
- вести учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных (*ИСПДн);*

▪ осуществлять администрирование информационных систем персональных данных;

▪ осуществлять администрирование средств антивирусной защиты информационных систем персональных данных;

▪ администрирование средств и систем защиты персональных данных в информационных системах персональных данных.

Внутренний контроль соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Организации в отношении обработки персональных данных осуществляет Уполномоченное лицо.

Уполномоченное лицо обязано:

▪ осуществлять внутренний контроль за соблюдением Организацией и его работниками законодательства РФ о персональных данных, в том числе требований к защите ПДн;

▪ доводить до сведения работников организации положения законодательства РФ о персональных данных, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

Обработка персональных данных должна осуществляться работниками, имеющими допуск к ПДн. Данные работники обязаны соблюдать положения настоящей Политики, а также своих должностных инструкций и других документов *Организации* в области защиты персональных данных.

2.2. Требования к организационным мерам по обеспечению безопасности персональных данных

2.2.1. Основные положения

Основой организационных мероприятий по обеспечению безопасности ПДн являются нормативные правовые акты и иные документы по защите ПДн, в частности Политика. Данные документы определяют стратегию и требования по защите ПДн. Положения данных документов доводятся до всех работников, ответственных за безопасность ПДн.

Мероприятия по обеспечению безопасности ПДн организуются и проводятся в соответствии с требованиями нормативных правовых актов:

▪ Федерального закона РФ от 27.07.06 № 152-ФЗ «О персональных данных»;

▪ Положения, утвержденного Постановлением Правительства РФ от 17 ноября 2007 г. «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

▪ Положения, утвержденного Постановлением Правительства РФ от 15 сентября 2008 г. «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

При обработке персональных данных субъектов ПДн допущенные к ним работники *Организации* обязаны соблюдать следующие требования:

соблюдать принципы и правила обработки персональных данных, предусмотренные настоящей Политикой безопасности;

соблюдать соответствие перечня действий при обработке персональных данных целям обработки персональных данных;

соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

соблюдать требования по защите обрабатываемых персональных данных.

2.2.1.1. *Организация* не вправе обрабатывать персональные данные субъекта ПДн без его письменного согласия, за исключением случаев, приведенных в п.2 ст.6 Федерального закона №152-ФЗ «О персональных данных». Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес *Организации*;
- цель передачи персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых *Организацией* способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Типовая форма согласия приведена в (*Приложении №26*).

2.2.1.2. В *Организации* запрещается обрабатывать специальные категории персональных данных, в том числе данные субъекта о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах.

2.2.1.3. Передача персональных данных субъектов третьей стороне не допускается без письменного согласия субъектов ПДн, за исключением случаев, установленных законодательством Российской Федерации.

2.2.1.4. В случае выявления недостоверных персональных данных субъекта ПДн или неправомерных действий с ними работников *Организации* при обращении или по запросу субъекта ПДн или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки.

2.2.1.5. В случае подтверждения факта недостоверности персональных данных субъекта ПДн на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

2.2.1.6. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с момента выявления, Уполномоченное лицо обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с момента выявления неправомерности действий с персональными данными, Уполномоченное лицо обязано уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Уполномоченное лицо обязано уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомляется указанный орган.

2.2.2. Анализ угроз

Обеспечение безопасности персональных данных, а также разработка и внедрение СЗПДн основывается на анализе угроз безопасности ПДн.

Уполномоченное лицо является ответственным за разработку и поддержку Частной модели угроз безопасности персональных данных при их обработке в ИСПДн (далее – Частная модель угроз).

В качестве исходных данных для разработки Частной модели угроз в *Организации* используется Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных, введённая Стандартом НАУФОР «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг» (далее – Базовая модель угроз).

Частная модель угроз должна отражать актуальное состояние защищенности ИСПДн и актуальные угрозы безопасности ПДн. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой ИСПДн.

2.3. Порядок уничтожения персональных данных

Ответственным за уничтожение персональных данных является Уполномоченное лицо.

Уполномоченное лицо является председателем комиссии *Организации* по уничтожению персональных данных. Назначение комиссии по уничтожению персональных данных производится приказом Генерального директора *Организации*.

При наступлении любого из событий, указанных в разделе 1.4. и повлекших необходимость уничтожения персональных данных, Уполномоченное лицо обязано обязано:

- уведомить членов комиссии о проведении работ по уничтожению персональных данных; определить (назначить) время, место работы комиссии (время и место уничтожения ПДн);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся ПДн, подлежащие уничтожению (и/или материальные носители ПДн);
- определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей ПДн); определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение ПДн;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей ПДн);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей ПДн) и представить Акт об уничтожении персональных данных (и/или материальных носителей ПДн) на утверждение Генерал ьному директору *Организации*;
- в случае необходимости уведомить об уничтожении ПДн субъекта персональных данных и/или уполномоченный орган.

2.4. Порядок обработки обращений субъектов персональных данных

Ответственным за обработку обращений субъектов персональных данных является Уполномоченное лицо.

При поступлении обращения от субъекта персональных данных Уполномоченное лицо обязано:

- убедиться, что обращение субъекта ПДн зарегистрировано согласно процедурам, установленным в *Организации*;
- действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;
- уведомить Генерального директора о поступлении обращения субъекта персональных данных;
- убедиться в отсутствии в обращении требования, нарушающего конституционные права и свободы других лиц;
- подготовить ответ, удовлетворяющий запрос субъекта ПДн, или мотивированный отказ (в случае если исполнение запроса может повлечь нарушение конституционных прав и свобод других лиц);
- сделать соответствующую запись в «Журнале учета обращений субъектов персональных данных при обработке персональных данных в ИСПДн *Организации*»;
- направить соответствующий ответ в адрес субъекта персональных данных.

2.5. Порядок действий в случае запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных

Ответственным за обработку запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, является Уполномоченное лицо.

При поступлении запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, Уполномоченное лицо обязано:

- убедиться, что запрос зарегистрирован согласно процедурам, установленным в *Организации*;
- действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;
- уведомить Генерального директора Организации о поступлении обращения субъекта персональных данных;
- подготовить ответ в соответствии с запросом уполномоченного органа по защите прав субъектов персональных данных или запросом иных надзорных органов, осуществляющих контроль и надзор в области персональных данных;
- зарегистрировать и направить соответствующий ответ в адрес уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

2.6. Порядок хранения отдельных материальных носителей персональных данных

2.6.1. Основные принципы хранения отдельных материальных носителей персональных данных:

- при фиксации персональных данных на материальных носителях не допускать фиксацию на одном материальном носителе персональных данных, цели обработки которых различны;
- для каждой категории персональных данных использовать отдельный материальный носитель;

▪ материальные носители, содержащие персональные данные, обработка которых осуществляется в различных целях, хранить раздельно (в отдельных шкафах (сейфах) или на отдельных полках);

▪ при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.6.2. Хранение отдельных материальных носителей персональных данных осуществляется на основании соответствующего приказа Генерального директора *Организации*.

В приказе Генерального директора определяются:

▪ места (номера комнат, шкафы (сейфы)), предназначенные для хранения материальных носителей персональных данных;

▪ перечень работников (ФИО, должность), ответственных за реализацию принципов и требований по обеспечению безопасности носителей персональных данных;

▪ требования по обеспечению безопасности персональных данных при хранении материальных носителей:

- порядок учёта материальных носителей;
- порядок доступа к носителям, получения носителей, работы с ними и порядок сдачи носителей на хранение;
- лицо (ФИО, должность), ответственное за хранение материальных носителей;
- лицо (ФИО, должность), ответственное за учёт материальных носителей;

▪ порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных:

- лицо (ФИО, должность), ответственное за контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных;
- обязанности лица (ФИО, должность), ответственного за контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

2.7. Доступ в помещения, в которых ведётся обработка персональных данных, и/или размещаются средства обработки ПДн, и/или хранятся носители персональных данных

2.7.1. Доступ в помещения, в которых ведётся обработка персональных данных, разрешён только работникам, непосредственно занятым обработкой персональных данных.

Перечень работников, непосредственно занятых обработкой персональных данных и имеющих право входа в названные помещения, устанавливается приказом Генерального директора.

Другие работники *Организации*, непосредственно не занятые в обработке персональных данных допускаются в помещения, в которых ведётся обработка персональных данных, только в сопровождении работников, уполномоченных приказом Генерального директора на обработку персональных данных и непосредственно имеющих рабочее место в помещении, в котором ведётся обработка персональных данных. При этом ознакомление работников *Организации*, которые прибыли в помещения с сопровождающим, с обрабатываемыми ПДн не допускается.

2.7.2. Доступ в помещения, в которых ведётся обработка персональных данных, лицам, не являющимися работниками *Организации,* запрещён. Исключение составляют только работниками государственных органов, организаций, доступ в помещения которым разрешается в соответствии с нормативными правовыми актами.

Доступ названных лиц осуществляется с разрешения Генерального директора и по разовым пропускам. При этом сотрудники государственных органов и организаций допускаются в помещения, в которых ведётся обработка персональных данных, только в сопровождении работников *Организации*, уполномоченных распоряжением (*устным или письменным*) Генерального директора для сопровождения конкретных лиц. При этом ознакомление сотрудников государственных органов, организаций, которые прибыли в помещения с сопровождающим, с обрабатываемыми ПДн не допускается.

2.7.3. Доступ в помещения, в которых размещаются средства обработки и/или защиты ПДн, разрешён только работникам, непосредственно занятым обработкой персональных данных или обслуживанием ИСПДн (СЗПДн).

Перечень работников, непосредственно занятых обработкой персональных данных или обслуживанием ИСПДн (СЗПДн) и имеющих право входа в названные помещения, устанавливается приказом Генерального директора.

Другие работники *Организации*, непосредственно не занятые в обработке персональных данных или обслуживании ИСПДн (СЗПДн), а так же работники других организаций (в т.ч. сотрудники государственных органов) допускаются в помещения, в которых размещаются средства обработки и/или защиты ПДн, только в сопровождении работников, уполномоченных приказом Генерального директора на обработку персональных данных или обслуживание ИСПДн (СЗПДн). При этом ознакомление лиц, которые прибыли в помещения с сопровождающим, с обрабатываемыми ПДн не допускается.

2.7.4. Доступ в помещения, в которых хранятся носители персональных данных, разрешён только работникам, непосредственно занятым работами с носителями персональных данных или ответственным за хранение носителей ПДн.

Перечень работников, непосредственно занятых работами с носителями персональных данных или ответственных за хранение носителей ПДн, устанавливается приказом Генерального директор. Другие работники *Организации*, а так же сотрудники других организаций (в т.ч. и сотрудники государственных органов) допускаются в помещения, в которых хранятся носители персональных данных, только в сопровождении работников, уполномоченных приказом Генерального директора

на хранение носителей персональных данных. При этом ознакомление лиц, которые прибыли в помещения с сопровождающим, с обрабатываемыми ПДн не допускается.

2.7.5. Общие требования к доступу в помещения, в которых ведётся обработка персональных данных, и/или размещаются средства обработки ПДн, и/или хранятся носители персональных данных

Требования настоящего раздела являются обязательными на всех стадиях проектирования, строительства, оснащения и эксплуатации помещений, в которых ведётся обработка персональных данных, и/или размещаются средства обработки ПДн, и/или хранятся носители персональных данных (далее - Помещения).

Помещения должны размещаться в пределах контролируемой зоны. При этом рекомендуется размещать их на максимальном удалении от границ контролируемой зоны (КЗ), чтобы ограждающие конструкции (стены, полы, потолки) не являлись смежными с помещениями, расположенными на неохраняемой территории.

Целесообразно, чтобы окна выходили на закрытую для несанкционированного доступа территорию, имели шторы (жалюзи).

Около окон Помещений, как правило, не должно быть пожарных лестниц, водосточных труб, пристроек и т.п.

Эффективность защиты Помещений должна соответствовать требованиям нормативных правовых актов и иных документов по обеспечению безопасности ПДн.

Достаточность предпринятых мер защиты Помещений, а также необходимость дополнительных мер защиты определяются при периодических проверках Помещений.

На каждое Помещение должен быть составлен технический паспорт, в котором необходимо отразить:

- план помещения с отображением размещенного оборудования и мебели;
- перечень оборудования и мебели, установленных в Помещении, с указанием типа, учетного или инвентарного номера и даты установки и замены;
- перечень реализованных в помещении мероприятий по защите ПДн;
- даты и результаты периодических проверок, выводы о соответствии Помещения предъявляемым требованиям.

2.7.6. Организационно-режимные требования к помещениям, в которых ведётся обработка персональных данных, и/или размещаются средства обработки ПДн, и/или хранятся носители персональных данных

2.7.6.1. Для Помещений, в которых ведётся обработка персональных данных, необходимо выполнять следующие требования:

- двери Помещений необходимо оборудовать замками повышенной надежности;
- выдача ключей от Помещений должна производиться лицам, работающим в нем или ответственным за это помещение;
- уборка этих Помещений должна производиться в присутствии лиц, ответственных за эти помещения, или специально выделенными уборщицами;
- в случае ухода из этих Помещений в рабочее время необходимо их закрывать на ключ или оставлять под ответственность доверенных лиц (например, секретаря).

2.7.6.2. Для Помещений, в которых размещаются средства обработки ПДн и/или хранятся носители персональных данных, кроме перечисленных в разделе 2.7.6.1. мер, необходимо выполнять следующие требования:

- двери Помещений должны быть оборудованы электроконтактными или магнитными датчиками охранной сигнализации;
- установка и замена оборудования, мебели в Помещении должны производиться только по согласованию с Генеральным директором*;*
- ремонт Помещения должен проводиться под наблюдением специально назначенного лица.

2.7.6.3. В случае обнаружения факта несанкционированного проникновения в Помещения должно производится расследование.

3. ПРЕСЕЧЕНИЕ (УСТРАНЕНИЕ) НАРУШЕНИЙ УСТАНОВЛЕННЫХ НОРМ И ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Своевременное и оперативное пресечение (устранение) нарушений норм и требований по обеспечению безопасности персональных данных является важнейшим требованием сохранения конфиденциальности персональных данных.

Невыполнение предписанных мер по обеспечению безопасности персональных данных считается предпосылкой к нарушению конфиденциальности ПДн (далее - предпосылка).

По каждой предпосылке немедленно докладывается Генеральному директору; для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование.

Для проведения расследования по приказу Генерального директора назначается комиссия из компетентных лиц. Комиссия обязана установить, имелось ли нарушение конфиденциальности персональных данных. После окончания расследования принимаются меры по устранению нарушений.

Работники, организующие и осуществляющие обработку и/или защиту ПДн, обязаны строго соблюдать требования по защите персональных данных и несут ответственность за нарушения, приводящие к нарушению конфиденциальности ПДн.

Нарушения норм и требований по обеспечению безопасности персональных данных делятся на три категории:

нарушение первой категории:

невыполнение норм и требований по обеспечению безопасности персональных данных, в результате которого произошло нарушение конфиденциальности ПДн;

По всем случаям нарушений первой категории немедленно докладывается Генеральному директору.

нарушение второй категории:

невыполнение норм и требований по обеспечению безопасности ПДн, в результате которого имелась или имеется реальная возможность нарушения конфиденциальности ПДн;

нарушение третьей категории:

невыполнение других требований по обеспечению безопасности ПДн, не приводящих к нарушениям первой и второй категорий.

О нарушениях второй и третьей категорий докладывается Уполномоченному лицу. По указанию Уполномоченного лица немедленно организуется пресечение нарушения, выявляется причина допущенного нарушения, оценивается степень возможного ущерба и принимаются меры к его устранению.

4. РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Регулирование деятельности по обеспечению безопасности персональных данных осуществляется посредством разработки и ввода в действие документов:

№	Наименование документа
1.	Приказ (распоряжение) об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
2.	Журнал учета лиц, допущенных к работе с персональными данными в информационных системах
3.	План по приведению деятельности Организации в соответствие с требованиями Федерального закона «О персональных данных»
4.	Перечень персональных данных, обрабатываемых в информационных системах персональных данных
5.	Перечень информационных систем персональных данных (ИСПДн), в которых должна быть обеспечена безопасность информации
6.	Акт обследования информационной системы персональных данных
7.	Описание технологического процесса обработки персональных данных в ИСПДн
8.	Перечень защищаемых ресурсов ИСПДн
9.	Описание настроек системы разграничения доступа системы защиты информации от несанкционированного доступа в ИСПДн
10.	Матрица доступа пользователей к информационным ресурсам ИСПДн
11.	Акт классификации информационной системы персональных данных
12.	Частная модель угроз безопасности персональных данных при их обработке в ИСПДн
13.	Журнал учета машинных носителей персональных данных в ИСПДн
14.	Акт об уничтожении персональных данных
15.	Границы контролируемой зоны ИСПДн
16.	Акт установки системы защиты информации от несанкционированного доступа
17.	Заключение о возможности эксплуатации средств (а)/системы защиты информации в информационной системе персональных данных
18.	Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним
19.	Журнал учета средств защиты информации, эксплуатационной и технической документации к ним
20.	Требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных
21.	План внутренних проверок состояния защиты персональных данных
22.	Журнал учета мероприятий по контролю обеспечения защиты персональных данных в ИСПДн
23.	Журнал учета обращений субъектов персональных данных при обработке персональных данных в ИСПДн
24.	Соглашение о неразглашении персональных данных работника
25.	Типовой раздел по конфиденциальности в трудовом, гражданско-правовом договоре
26.	Согласие на обработку персональных данных
27.	Инструкция администратора информационной системы персональных данных
28.	Инструкция пользователя информационной системы персональных данных
29.	Инструкция администратора безопасности при использовании ресурсов объекта вычислительной техники
30.	Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных
31.	Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов
32.	Технический (аппаратный) журнал криптосредства
33.	Схема документов
34.	Политика безопасности персональных данных

5. ТЕХНИЧЕСКАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Общие положения

Для защиты ПДн, обрабатываемых в *Организации,* внедрена СЗПДн – комплексная система, позволяющая обеспечить конфиденциальность (*целостность, доступность и др.*) ПДн, хранящихся и обрабатываемых в *Организации*.

Внедрение или модернизация СЗПДн представляет собой поэтапный процесс, учитывающий особенности имеющейся ИСПДн, и включает в себя следующие этапы:

- предпроектное обследование ИСПДн;
- определение требований к СЗПДн;
- проектирование СЗПДн;
- создание СЗПДн.

Обоснование комплекса мероприятий по обеспечению безопасности ПДн в ИСПДн Организации производится с учетом результатов оценки опасности угроз и определения класса ИСПДн на основе Приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Защита ПДн обеспечивается на всех технологических этапах передачи, обработки и хранения ПДн и при всех режимах работы ИСПДн, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе меры (механизмы) защиты от НСД не должны ухудшать основные функциональные характеристики ИСПДн.

5.2. Состав системы защиты персональных данных

СЗПДн *Организации* включает в себя следующие подсистемы:

- подсистема управления доступом;
- подсистема межсетевого экранирования;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема анализа защищенности;
- подсистема антивирусной защиты.

5.3. Требования к СЗПДн

Учитывая специфику деятельности Организации ИСПДн и СЗПДн должны выполнять требования:

- направленные на обеспечение непрерывного функционирования подсистем защиты ПДн с установленными параметрами, позволяющими обеспечивать безопасность ПДн в соответствии с заданными требованиями;
- к защищенной среде хранения и обработки ПДн, позволяющей предоставлять доступ к ПДн только авторизованным для этого работникам;
- по защите ПДн от разглашения или утечки, а так же по защите ПДн от подмены или модификации;
- к системе резервного копирования данных, позволяющей восстановить утерянную информацию сроком давности до … (2)-х лет;
- по защищенности от сбоев;

▪ и др.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, должны в установленном порядке проходить процедуру оценки соответствия (или иметь разрешение Генерального директора.

Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

▪ изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

▪ изменился состав угроз безопасности ПДн, обрабатываемых в ИСПДн;

▪ изменился класс ИСПДн.

6. ИНСТРУКТАЖ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

Работники, осуществляющие обработку ПДн и ответственные за обеспечение её безопасности, должны иметь квалификацию, достаточную для поддержания требуемого режима безопасности персональных данных.

В этих целях вводится система обеспечения требуемого уровня квалификации:

▪ для всех работников, обрабатывающих персональные данные, проводятся инструктажи по обеспечению безопасности ПДн: вводный - при приёме на работу; квалификационный – при допуске к работе с персональными данными; периодический (контрольный) - регулярно, раз год;

▪ для работников, являющихся администраторами ИСПДн, или администраторами СЗПДн, или ответственными за хранение носителей ПДн, проводится обучение по курсу обеспечения безопасности ПДн.

Обязанность по реализации системы обеспечения требуемого уровня квалификации возлагается на Генерального директора, а также на Уполномоченное лицо по обеспечению безопасности персональных данных, в том числе:

▪ организовывать инструктирование и обучение работников;

▪ вести персональный учёт работников, прошедших инструктирование и обучение;

▪ вести реестр свидетельств об обучении;

▪ и др.

7. ОТВЕТСТВЕННОСТЬ

Работники *Организации*, разгласившие персональные данные субъектов ПДн, а также работники, по вине которых произошло нарушение конфиденциальности ПДн, и работники, создавшие предпосылки к нарушению конфиденциальности персональных данных, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами *Организации* и условиями трудового договора (контракта, соглашения).

8. ПЕРЕСМОТР ПОЛИТИКИ

Развитие системы информационной безопасности и совершенствование методов и средств защиты является непрерывным процессом, в связи с чем возникает необходимость пересмотра положений настоящей Политики.

Внесение изменений в Политику может быть вызвано изменениями в ИСПДн, системе защиты ПДн, изменениями нормативных правовых актов и иных документов.

Внесению изменений в Политику предшествуют:

- обследование и анализ изменений в ИСПДн и СЗПДн и/или;
- анализ изменений нормативных правовых актов и иных документов.

По завершении вышеназванных процедур анализа и обследования вносятся изменения (дополнения, исключения, новые редакции):

- в Политику обеспечения безопасности персональных данных;
- в документы, указанные в разделе «4» - «Регулирование направлений, областей и частных действий по обеспечению безопасности персональных данных».

Введение в действие новых редакций Политики и документов из раздела «4» осуществляется согласно процедурам документооборота, установленным в Организации.

Лист изменений

Версия	Дата	Номер раздела	Тип изменений	Автор	Аннотация изменения
			дополнение		
			исключение		
			и т.д.		