

**Приложение 4**  
к приказу ЗАО «Система АКСЕКО»  
от «10» ноября 2014г. №1-10-05  
«Об обработке персональных данных  
в информационных системах ЗАО  
«Система АКСЕКО»

**Закрытое акционерное общество  
«Система АКСЕКО»**

**ПОЛОЖЕНИЕ  
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ  
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ  
ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАО «СИСТЕМА АКСЕКО»**

**ИНФОРМАЦИОННЫЕ ДАННЫЕ**

РАЗРАБОТАН

УТВЕРЖДЕН

Генеральный директор  
ЗАО «Система АКСЕКО»  
Приказ № 1-10-05 от 10.11.2014г.

Беденко А.Н.

ВВОДИТСЯ

«10» ноября 2014г.

ПЕРИОДИЧНОСТЬ ПЕРЕСМОТРА

срок не установлен

## СОДЕРЖАНИЕ

	Стр.
1. ОБЩИЕ ПОЛОЖЕНИЯ.....	4
2. ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ.....	4
3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	6
4. ПОРЯДОК ИСПОЛЬЗОВАНИЯ, МОДЕРНИЗАЦИИ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В СИСТЕМУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	8
5. ОТВЕТСТВЕННЫЕ ЛИЦА И СПЕЦИАЛИЗИРОВАННЫЕ ОРГАНИЗАЦИИ.....	11
6. ОСНОВНЫЕ ТРЕБОВАНИЯ И ПРАВИЛА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	14
7. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ СРЕДСТВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	20
8. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ПРИМЕНЕНИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.....	22
9. ПОРЯДОК ОРГАНИЗАЦИИ ВНУТРЕННЕГО ОБУЧЕНИЯ ПЕРСОНАЛА ПРАВИЛАМ И МЕРАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	22
10. ВНУТРЕННИЙ КОНТРОЛЬ РЕЖИМА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	24
11. ВЕДЕНИЕ ЖУРНАЛА.....	26
12. ИНФОРМИРОВАНИЕ, РАССЫЛКА И АКТУАЛИЗАЦИЯ.....	26
Лист регистрации и изменений	

## **1. Общие положения**

1.1. Настоящее Положение об обеспечении безопасности персональных данных (далее - ПД) при их обработке в информационных системах персональных данных (далее - ИСПД), (далее - Положение) регламентирует вопросы обеспечения безопасности ПД при их обработке в ИСПД в зоне ответственности ЗАО «Система АКСЕКО» (далее – Оператор, Общество) и определяет порядок организации работ по созданию и эксплуатации системы защиты ПД (далее – СЗПД).

1.2. Настоящее Положение разработано в целях:

- предотвращения неправомерного или случайного доступа к ИСПД, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;

- соблюдения правового режима использования информации, содержащей ПД;

- обеспечения возможности обработки и использования ПД с использованием средств автоматизации Обществом, а также лицами, уполномоченными на это Обществом.

1.3. Все работники Общества, допущенные к обработке ПД, должны быть ознакомлены с настоящим Положением и любыми изменениями к нему под подпись и должны руководствоваться в своей деятельности настоящим Положением и принятыми в соответствии с ними локальными нормативными актами.

1.4. Настоящее Положение разработано с учетом следующих законодательных и нормативных правовых актов:

- Федеральный закон от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных";

- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных ";

- Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ";

- иные нормативно-правовые акты Российской Федерации, регламентирующие вопросы обработки ПД.

## **2. Основные термины и сокращения**

2.1. Следующие употребляемые в настоящем Положении термины имеют указанные ниже значения:

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**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 назначению и техническим характеристикам.

**Ответственное лицо** – лицо, ответственное за организацию обработки ПД в Обществе или иное лицо, назначенное приказом генерального директора Общества.

**Технические средства, позволяющие осуществлять обработку ПД** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие ТС обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационной системе.

**Угроза безопасности ПД** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий при их обработке в ИСПД.

**АРМ** – автоматизированное рабочее место.

**АС** – автоматизированная система.

**ИБ** – информационная безопасность.

**ИР** – информационный ресурс.

**ИС** – информационная система.

**ИСПД** – информационная система ПД.

**ИТ** – информационная технология.

**НСД** – несанкционированный доступ.

**ОРД** – организационно-распорядительные документы.

**ПО** – программное обеспечение.

**СВТ** – средство вычислительной техники.

**СЗИ** – средство защиты информации.

**СЗПД** – система защиты ПД.

**СКЗИ** – средство криптографической защиты информации.

**ТС** – техническое средство.

**ФСТЭК России** – Федеральная служба по техническому и экспортному контролю России.

2.2. Иные термины, используемые в настоящем Положении и не определенные в нем, имеют значение, присвоенное им в Политике в отношении обработки ПД в ЗАО «Система АКСЕКО».

### **3. Обеспечение безопасности ПД**

3.1. Порядок организации и проведения работ по обеспечению безопасности ПД при их обработке в ИСПД

3.1.1. Под организацией обеспечения безопасности ПД при их обработке в ИСПД понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПД, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПД в ИСПД, восстановление нормального функционирования ИСПД после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

3.1.2. Организация работ по защите ПД при их обработке в ИСПД предусматривает определение:

- на основании законодательства и других нормативных актов, регулирующих деятельность Общества, перечня ПД, обрабатываемых в информационных системах (ИС) Общества;

- порядка классификации ИС Общества как ИСПД;

- порядка разработки, ввода в действие и эксплуатацию ИСПД в части реализации мероприятий по обеспечению безопасности ПД;

- порядка взаимодействия между ответственными за обеспечение безопасности ПД и эксплуатирующими подразделениями (администраторами) по вопросам обеспечения безопасности ПД;

- порядка привлечения структурных подразделений Общества и специализированных сторонних организаций к разработке и эксплуатации СЗПД, их задачи и функции на различных стадиях создания и эксплуатации ИСПД;

- ответственности должностных лиц за обеспечение безопасности ПД, своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗПД;

- порядка контроля обеспечения требуемого уровня защищенности ПД.

3.1.3. Ответственное лицо осуществляет разработку и проведение мероприятий по организации и обеспечению безопасности ПД при их обработке в ИСПД.

3.1.4. Непосредственно исполнение работ по защите информации (ПД) в ИСПД с использованием средств автоматизации возлагается на Ответственное лицо. Ответственное лицо взаимодействует с другими работниками Общества.

3.1.5. Проведение предпроектного обследования ИСПД, разработка и реализация СЗПД может осуществляться как Ответственным лицом, так и на договорной основе другими специализированными организациями, имеющими соответствующие лицензии. Научно-техническое и методическое руководство, непосредственная организация работ по созданию (модернизации) СЗПД и контроль за эффективностью использования предусмотренных мер возлагается на Ответственное лицо.

3.1.6. В случае разработки СЗПД или ее отдельных компонентов специализированными организациями, Ответственное лицо отвечает за организацию и проведение мероприятий по защите информации. Разработка, внедрение и эксплуатация СЗПД осуществляется во взаимодействии разработчика с Ответственным лицом.

3.1.7. Контроль за реализацией проектных решений возлагается на Ответственное лицо.

3.2. Порядок определения защищаемой информации и классификации ИСПД

3.2.1. На основании законодательства и других нормативных актов, регулирующих деятельность Общества, Ответственным лицом или генеральным директором Общества для каждой ИСПД определяется перечень ПД, уточняются цели и основание обработки ПД, а также срок хранения и условия прекращения обработки.

3.2.2. Целью классификации ИС Общества как ИСПД является определение по ее результатам перечня обоснованных организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности ПД с учетом особенностей конкретной ИСПД. Классификация может проводиться на этапе создания ИС или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИС).

3.2.3. Классификация ИСПД проводится Ответственным лицом или генеральным директором Общества и включает в себя следующие этапы:

- сбор и анализ исходных данных по ИС;
- присвоение ИС соответствующего уровня защищенности и его документальное оформление.

3.2.4. При проведении классификации ИСПД Ответственным лицом или генеральным директором Общества определяется:

- заданные Оператором характеристики безопасности ПД, обрабатываемых в ИС;
- структура ИС;

- наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена;

- режим обработки ПД;

- режим разграничения прав доступа пользователей ИС;

- местонахождение ТС ИС.

3.2.5. В случае выделения в составе ИС подсистем, каждая из которых является ИС, ИС в целом присваивается уровень защищенности, соответствующий наиболее высокому уровню защищенности входящих в нее подсистем.

3.2.6. Результаты классификации ИСПД оформляются приказом генерального директора Общества. Сформированные по результатам классификации материалы являются неотъемлемой частью организационно-распорядительной документации (ОРД) ИСПД.

3.2.7. Уровень защищенности ИСПД может быть пересмотрен Ответственным лицом или генеральным директором Общества в установленном порядке в следующих случаях:

- на основе результатов проведенного анализа и оценки угроз безопасности ПД с учетом особенностей и (или) изменений конкретной ИС;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПД при их обработке в ИС.

#### **4. Порядок использования, модернизации и внесения изменений в систему защиты персональных данных**

##### 4.1. Общий порядок

4.1.1. Общество использует СЗПД, представляющую собой совокупность СЗИ, используемых в реальном времени в автоматическом режиме.

4.1.2. Для целей эффективной защиты ПД в СЗПД Ответственное лицо осуществляет внутренние проверки режима защиты ПД.

4.1.3. При необходимости модернизации и/или внесения изменений в СЗПД, предусматриваются следующие стадии разработки изменений и сопровождения модернизации СЗПД:

- предпроектная стадия – включает предпроектное обследование ИСПД и разработку технического (частного технического) задания на модернизацию/изменение СЗПД;

- стадия проектирования (разработки проектов) и реализации ИСПД – включает разработку изменений в СЗПД в составе ИСПД;

- стадия ввода в действие модернизированной/измененной СЗПД (включает предварительные испытания, опытную эксплуатацию и приемо-сдаточные испытания средств защиты, а также оценку соответствия ИСПД требованиям безопасности информации);

## 4.2. Предпроектная стадия

4.2.1. На предпроектной стадии проводится предпроектное обследование ИСПД и разработка технического (частного технического) задания на модернизацию/изменение СЗПД.

4.2.2. Выполнение данных работ может быть поручено на договорной основе специализированной сторонней организации, имеющей соответствующую лицензию.

4.2.3. Условия соблюдения конфиденциальности специалистами привлекаемой сторонней организации при проведении работ оформляются в соответствии с установленным в Обществе порядком.

4.2.4. При проведении предпроектного обследования ИСПД определяются:

- перечень ПД, подлежащих защите;
- условия расположения ИСПД относительно границ контролируемой зоны;
- конфигурация и топология ИСПД и ее компонент;
- физические, функциональные и технологические связи как между компонентами ИСПД, так и между ИСПД и другими системами;
- состав ТС и систем ИСПД;
- состав общесистемных и программных средств ИСПД;
- режимы обработки ПД в ИСПД в целом и в отдельных компонентах;
- степень участия персонала в обработке ПД и характер их взаимодействия между собой;
- класс ИСПД;
- уточняются угрозы безопасности и модель вероятного нарушителя применительно к конкретным условиям функционирования ИСПД;
- мероприятия по обеспечению безопасности ПД в процессе проектирования СЗПД.

4.2.5. По результатам предпроектного обследования с учетом установленного уровня защищенности ИСПД задаются определенные требования по обеспечению безопасности ПД, включаемые в техническое (частное техническое) задание на разработку изменений в СЗПД.

4.2.6. Техническое (частное техническое) задание на разработку изменений в СЗПД должно содержать:

- обоснование необходимости модернизации/внесения изменений в СЗПД;
- исходные данные о модернизируемой/изменяемой ИСПД в техническом, программном, информационном и организационном аспектах;
- класс ИСПД;

- ссылку на нормативные документы, с учетом которых будет модернизироваться/изменяться СЗПД и приниматься в эксплуатацию ИСПД;

- конкретизацию мероприятий и требований к СЗПД;

- перечень предполагаемых к использованию сертифицированных средств защиты информации (СЗИ);

- обоснование проведения разработок собственных СЗИ при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СЗИ;

- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПД.

#### 4.3. Стадия проектирования и реализации модернизации/изменений в СЗПД

4.3.1. Проектирование и реализация модернизации/изменений в СЗПД проводится на основании требований, изложенных в техническом (частном техническом) задании на модернизацию/внесение изменений в СЗПД. При разработке модернизации/изменений в СЗПД в составе ИСПД проводятся следующие мероприятия:

- разработка задания и проекта на внесение изменений в ИСПД в соответствии с требованиями технического (частного технического) задания на разработку СЗПД;

- разработка раздела технического проекта на ИСПД в части защиты информации;

- использование серийно выпускаемых ТС обработки, передачи и хранения информации;

- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

- использование сертифицированных технических, программных и программно-технических СЗИ и их установка;

- сертификация по требованиям безопасности информации программных СЗИ в случае, если на рынке отсутствуют требуемые сертифицированные СЗИ;

- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПД информации;

- выполнение других мероприятий, характерных для конкретных ИСПД и направлений обеспечения безопасности ПД.

4.3.2. Проектная документация подлежит согласованию с генеральным директором Общества.

следую

- опытная эксплуатация средств защиты в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД и отработки технологического процесса обработки (передачи) информации;

- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;

- организация охраны и физической защиты помещений ИСПД, исключающих НСД к ТС ИСПД, их хищение и нарушение работоспособности, хищение носителей информации;

- оценка соответствия ИСПД требованиям безопасности ПД.

4.4.2. Ввод в эксплуатацию модернизированной/измененной СЗПД осуществляется на основании приказа, который издается на основании положительных результатов оценки соответствия ИСПД требованиям безопасности ПД.

4.4.3. Эксплуатация СЗПД осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией с учетом требований и положений, изложенных в настоящем документе.

4.4.4. При определении порядка проведения технического обслуживания и ремонтных работ в СЗПД должно быть учтено требование исполнения данных работ только Ответственным лицом.

Все процедуры, связанные с изменением конфигурации СЗПД, проведением технического обслуживания и ремонтных работ на ТС СЗПД должны предусматривать документирование объемов и сроков выполненных работ, а также лиц (организаций), проводивших эти работы.

4.4.5. Для организации и обеспечения безопасности ПД при их обработке в ИСПД ответственным за обеспечение безопасности ПД является Ответственное лицо.

## **5. Ответственные лица и специализированные организации**

### **5.1. Функции Ответственного лица**

5.1.1. Для организации и обеспечения безопасности ПД при их обработке в ИСПД ответственным за обеспечение безопасности ПД является Ответственное лицо.

5.1.2. Ответственное лицо обеспечивает методическое руководство, разработку требований к мерам защиты ИСПД и контроль за эффективностью использования предусмотренных мер защиты информации.

5.1.3. Ответственное лицо обеспечивает подготовку предложений по совершенствованию и реализации положений Положения и контролирует выполнение установленных требований в структурных подразделениях Общества.

5.1.4. Ответственное лицо осуществляет следующие функции:

- разрабатывает предложения по определению уровня защищенности объектов ИСПД и автоматизированной системы (АС);

- участвует в организации работ по выявлению актуальных угроз безопасности ПД;
- осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите ПД и разработке технического (частного технического) задания на создание СЗПД;
- согласовывает выбор конкретных средств обработки ПД, технических и программных средств защиты;
- осуществляет контроль реализации проектных решений на создание СЗПД;
- участвует в организации работ по оценке соответствия ИСПД предъявляемым требованиям по обеспечению безопасности ПД;
- участвует в организации разработки ОРД по защите информации в ИСПД;
- проводит контроль требуемого уровня обеспечения защищенности ПД при эксплуатации СЗПД, в том числе контроль соблюдения условий использования СЗИ;
- участвует в организации обучения должностных лиц Общества, ответственных за эксплуатацию СЗИ, по направлению обеспечения безопасности ПД;
- участвует в организации охраны и физической защиты помещений Общества, в которых размещаются средства обработки ПД, исключающих НСД к ТС ИСПД, их хищение нарушение работоспособности, хищение носителей информации;
- устанавливает правила работы с информацией, ТС и правила использования ПД в рамках своей ответственности согласно возможностям, функциям, предназначению и степени защищенности этих средств, ресурсов требованиям к защите и доступности ПД;
- осуществляет предоставление ИТ - сервисов всем структурным подразделениям Общества, отвечает за их целостность и доступность;
- обеспечивает разграничение доступа к ПД в процессе их использования, контроль над ходом информационных процессов.

## 5.2. Функции сторонних специализированных организаций

5.2.1. При необходимости Общество привлекает для модернизации/изменения СЗПД или ее отдельных компонентов сторонние специализированные организации.

5.2.2. В случае привлечения для обеспечения безопасности ПД сторонних специализированных организаций должны выполняться следующие условия:

- оформление соглашения о неразглашении конфиденциальных сведений;
- проведение инструктажа исполнителей работ по вопросам ИБ;
- другие условия, устанавливаемые соответствующими нормативными и ОРД Общества.

5.2.3. На предпроектной стадии на сторонние специализированные организации возлагаются следующие функции:

- уточнение перечня ПД, подлежащих защите;
- определение условий расположения ИСПД относительно границ контролируемой зоны;
- определение конфигурации и топологии ИСПД в целом, и ее отдельных компонент, физические, функциональные и технологические связи как внутри ИСПД, так и с другими системами различного назначения;
- определение ТС и систем, включаемых в состав ИСПД, условий их расположения, общесистемных и прикладных программных средств;
- определение режимов обработки ПД в ИСПД;
- разработка предложений по уточнению уровня защищенности ИСПД;
- уточнение степени участия персонала в обработке ПД, характера их взаимодействия между собой;
- определение (уточнение) угроз безопасности ПД с учетом конкретных условий функционирования ИСПД;
- разработка проекта частной модели угроз;
- участие в разработке (согласовании) конкретных требований по защите ПД и разработке технического (частного технического) задания на создание СЗПД.

5.2.4. На стадии проектирования на сторонние специализированные организации возлагаются следующие функции:

- разработка технического проекта на модернизацию/внесение изменений в СЗПД в соответствии с требованиями законодательства;
- использование сертифицированных технических, программных и программно-технических СЗИ и их установка;
- организация сертификации по требованиям безопасности информации программных СЗИ в случае, когда на рынке отсутствуют требуемые сертифицированные СЗИ;
- разработка разрешительной системы доступа пользователей к ПД, обрабатываемым в ИСПД;
- разработка (в согласованном объеме) эксплуатационной документации на СЗПД.

5.2.5. На стадии ввода СЗПД в эксплуатацию на сторонние специализированные организации возлагаются следующие функции:

- установка СЗИ;

- предварительные испытания и опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД;

- наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;

- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;

- оценка соответствия ИСПД требованиям безопасности ПД.

## **6. Основные требования и правила по обеспечению безопасности персональных данных**

### **6.1. Общие требования**

6.1.1. Обеспечение безопасности ПД при их обработке в ИСПД достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПД, и носители информации.

6.1.2. Основными направлениями защиты информации (ПД) являются:

- обеспечение защиты информации (ПД) от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;

- обеспечение защиты информации (ПД) от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

6.1.3. Основными мерами защиты информации (ПД) являются:

- назначение ответственного за организацию обработки ПД;

- разработка документов, определяющих политику Общества в отношении обработки ПД, локальных актов по вопросам обработки ПД;

- оценка вреда, который может быть причинен субъектам ПД в случае нарушения требований настоящего Положения и нормативных актов РФ;

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к ИР, ИС и связанным с ее использованием работам, документам;

- разграничение доступа пользователей и обслуживающего персонала к ИР, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль НСД и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации и их обращение, исключаящее хищение, подмену и уничтожение;

- резервирование ТС, дублирование массивов и носителей информации;
- использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
- использование защищенных каналов связи;
- размещение ТС, позволяющих осуществлять обработку ПД, в пределах охраняемой территории;
- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
- организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку ПД;
- предотвращение внедрения в ИС вредоносных программ (программ-вирусов) и программных закладок.

6.1.4. Для обеспечения безопасности ПД от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД в зависимости от уровня защищенности ИСПД, заданных характеристик безопасности обрабатываемых ПД, угроз безопасности ПД, структуры ИСПД, наличия межсетевого взаимодействия и режимов обработки ПД в рамках СЗИ от НСД реализуются функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

6.2. Требования по организации разрешительной системы доступа пользователей к обрабатываемой в ИСПД информации

6.2.1. Данный подраздел Положения регламентирует порядок взаимодействия структурных подразделений Общества по обеспечению безопасности ПД при организации разрешительной системы доступа к сервисам и ресурсам ИСПД.

6.2.2. Разрешительная система доступа к обрабатываемой в ИСПД информации должна предусматривать установление единого порядка обращения со сведениями, содержащими ПД клиентов и работников Общества, и их носителями, определять степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

6.2.3. Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности ПД и включает:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;
- определение порядка изменения правил доступа к защищаемой информации;
- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

- контроль функционирования разрешительной системы доступа и расследование фактов неправомерного доступа лиц к защищаемой информации, в случае выявления таковых;
- оценку эффективности проводимых мер по исключению утечки информации;
- организацию деятельности должностных лиц, ответственных за подготовку предложений о внесении изменений в должностные обязанности и иные документы, определяющие задачи и функции персонала ИСПД.

6.2.4. Основные условия правомерного доступа работников Общества к обрабатываемой в ИСПД информации включают в себя:

- подписание работником Общества Обязательства о неразглашении конфиденциальной информации либо включение обязательства о неразглашении работником конфиденциальной информации в Трудовой договор;
- наличие у сотрудника Общества права допуска к ПД, обрабатываемым в ИСПД;
- наличие утвержденных генеральным директором Общества должностных (функциональных) обязанностей работника, определяющих круг его задач и объем необходимой для их решения информации.

6.2.5. Лица, доступ которых к ПД, обрабатываемым в ИСПД, необходим для выполнения трудовых обязанностей, допускаются к соответствующим ПД на основании утвержденного Перечня должностей работников, допущенных к обработке ПД.

6.2.6. Для обеспечения персональной ответственности за свои действия каждому пользователю ИСПД, допущенному к работе с защищаемой информацией в ИСПД, присваивается уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе. В случае производственной необходимости пользователю ИСПД могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в ИСПД одного и того же имени пользователя ("группового имени") запрещается.

6.2.7. При регистрации и назначении прав доступа пользователей ИСПД должны быть выполнены следующие требования:

- каждому пользователю должен быть присвоен уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать;
- учетные записи всех пользователей должны быть привязаны к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты ИСПД;
- при регистрации пользователей должна быть проведена проверка соответствия уровня доступа возложенным на пользователя задачам (вмененным обязанностям);
- назначенные пользователю права доступа должны быть документированы;

- пользователь должен быть ознакомлен под роспись с предоставленными ему правами доступа и порядком его осуществления;

- в ИСПД должно быть предусмотрено разрешение доступа к сервисам только аутентифицированным пользователям;

- должен быть разработан и обновляться при внесении нового пользователя формальный список всех пользователей, зарегистрированных для работы в ИСПД;

- при изменении должностных обязанностей (увольнении) пользователя должно проводиться немедленное исправление (аннулирование) прав его доступа;

- Ответственным лицом должно проводиться удаление всех неиспользуемых учетных записей.

- предусмотренные в системе запасные идентификаторы должны быть недоступны другим пользователям.

6.2.8. Контроль выполнения требований разрешительной системы доступа к ПД возлагается на Ответственное лицо.

6.2.9. Допуск к ИР ИСПД сторонних организаций (правоохранительных органов, судебных органов, органов статистики, органов исполнительной и законодательной власти субъектов РФ) регламентируется законодательством РФ, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

6.2.10. Порядок допуска к ИР ИСПД сторонних организаций, выполняющих работы на договорной основе, определяется в договоре на выполнение работ (оказание услуг). Обязательным условием договора должно являться заключение соглашения о конфиденциальности.

веществ, а также кражи. ТС ИСПД и размещенное совместно с ними вспомогательное оборудование должны подвергаться ежегодным осмотрам с целью выявления изменения конфигурации средств вычислительной техники (СВТ) (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.).

Должно быть обеспечено размещение устройств вывода информации СВТ, дисплеев АРМ ИСПД таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПД.

#### 6.4. Правила обращения со съемными носителями ПД

6.4.1. При обращении со съемными носителями ПД должны выполняться следующие основные правила:

- носители ПД должны быть учтены и защищены;
- носители ПД, срок эксплуатации которых истек, должны уничтожаться в установленном порядке;
- для выноса носителей ПД за пределы Общества должно быть получено специальное разрешение, а факт выноса - зафиксирован в журнале выдачи носителей данных, содержащих персональные данные;
- все носители ПД должны храниться в безопасном месте в соответствии с требованиями по их эксплуатации, должны соблюдаться условия, обеспечивающие сохранность ПД и исключающие несанкционированный доступ к ним.

6.4.2. Ответственным за хранение, учет и выдачу съемных носителей ПД является Ответственное лицо.

#### 6.5. Порядок учета носителей информации

6.5.1. Все находящиеся на хранении и в обращении съемные носители ПД должны быть учтены в журнале учета материальных носителей, предназначенных для хранения персональных данных.

6.5.2. Пользователи ИСПД в структурных подразделениях, ответственных за обработку той или иной категории ПД согласно Перечню лиц, допущенных к обработке ПД, имеют право брать и использовать съемные носители ПД, содержащие персональные данные соответствующей категории, исключительно для выполнения своих должностных обязанностей в пределах отведенных для этого помещений Общества в течение рабочего дня без ограничений.

Контроль за использованием и своевременным возвратом носителей в течение рабочего дня возлагается на руководителя структурного подразделения.

6.5.3. В случае необходимости использования съемных носителей ПД за пределами отведенных для этого помещений Общества и/или по окончании рабочего дня Ответственное лицо или руководитель (заместитель руководителя) структурного подразделения делают

отметку о выдаче и возврате соответствующего материального носителя ПД в журнале учета выдачи материальных носителей данных, содержащих персональные данные.

6.5.4. Носители ПД, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Порядок уничтожения носителей ПД определен в Положении об уничтожении ПД. Уничтоженные носители ПД (утилизированное оборудование) снимаются с материального учета.

6.6. Для оперативного восстановления данных в случае утери или по другим причинам в Обществе осуществляется резервное копирование защищаемой информации (ПД) в соответствии с Инструкцией по организации резервного копирования и восстановления программного обеспечения баз данных информационных систем ПД ЗАО «Система АКСЕКО».

6.7. В целях защиты ИСПД от разрушающего воздействия компьютерных вирусов и вредоносных программ в Обществе должны выполняться соответствующие организационные меры, которые приведены в Инструкции по организации антивирусной защиты в информационной системе ПД ЗАО «Система АКСЕКО».

6.8. Требования по обеспечению безопасности при работе в сети Интернет

6.8.1. Доступ в сеть Интернет и другие глобальные сети работникам Общества предоставляется исключительно в целях повышения эффективности выполнения ими свои служебных обязанностей.

6.8.2. Работнику Общества может быть ограничен доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

6.8.3. При работе с ресурсами сети Интернет запрещается:

- разглашение сведений конфиденциального характера Общества, ставшие известными сотруднику Общества по служебной необходимости либо иным путем;

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и

прочие средства для получения НСД к платным ресурсам в сети Интернет, а также размещение ссылок на вышеуказанную информацию;

- загрузка и запуск исполняемых либо иных файлов без предварительной проверки на наличие - вирусов установленным антивирусным пакетом;

- использование анонимных прокси-серверов;

- доступ к ресурсам сети Интернет, содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию.

6.8.4. При нарушении работником Общества правил работы в сети Интернет либо возникновении нештатных ситуаций доступ к ресурсам сети Интернет может быть заблокирован.

## **7. Правила использования программного обеспечения и аппаратных средств информационной системы персональных данных**

Настоящий раздел регламентирует взаимодействие структурных подразделений Общества по обеспечению безопасности информации при проведении модификаций ПО, технического обслуживания и ремонта СВТ ИСПД.

### **7.1. Права на внесение изменений в ПО и аппаратные средства ИСПД**

7.1.1. Все изменения конфигурации ТС и программных средств АРМ и серверов ИСПД, обрабатывающих ПД, должны производиться только Ответственным лицом.

7.1.2. Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (АРМ, серверов) и телекоммуникационного оборудования, обрабатывающего ПД, предоставляется Ответственному лицу.

7.1.3. Изменение конфигурации аппаратно-программных средств защищенных АРМ и серверов кем-либо, кроме Ответственного лица, запрещено.

7.1.4. Право внесения изменений в конфигурацию программно-аппаратных средств АРМ (серверов) локальной вычислительной сети, не обрабатывающих ПД, предоставляется Ответственному лицу.

### **7.2. Порядок внесения изменений в ПО и аппаратные средства ИСПД**

7.2.1. Внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и АРМ ИСПД осуществляется Ответственным лицом.

7.2.2. Возможно внесение следующих видов необходимых изменений в составе программных и аппаратных средств рабочих станций (АРМ) и серверов структурного подразделения:

- установка в структурном подразделении новой рабочей станции (АРМ) или сервера;
- замена рабочей станции (АРМ) или сервера структурного подразделения;

- изъятие рабочей станции (АРМ) или сервера структурного подразделения;
- добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера структурного подразделения;
- замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера структурного подразделения;
- изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;
- установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);
- обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

7.2.3. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Ответственным лицом.

7.2.4. Если рабочая станция (АРМ) или сервер обрабатывают ПД, то установка, снятие, и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется Ответственным лицом. Работы производятся в присутствии пользователя данной рабочей станции.

7.2.5. Подготовка модификаций ПО защищенных серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в фонд алгоритмов и программ и другие необходимые действия производятся Ответственным лицом.

7.2.6. Установка или обновление подсистем ИСПД должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

7.2.7. Модификация ПО на сервере осуществляется Ответственным лицом.

7.2.8. После установки модифицированных модулей на сервер Ответственное лицо устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью специальных программных средств, прошедших оценку соответствия).

7.2.9. После проведения модификации ПО на рабочих станциях Ответственное лицо проводит антивирусный контроль.

7.2.10. Установка и обновление общего ПО (системного, тестового) на рабочие станции (АРМ) и серверы производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков и др.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств, полученных из фонда алгоритмов и программ.

7.2.11. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, контроль наличия проверок работоспособности осуществляет Ответственное лицо.

7.2.12. После установки (обновления) ПО Ответственное лицо должно произвести настройку средств управления доступом к данному программному средству и проверить работоспособность ПО и правильность настройки СЗИ.

7.2.13. После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), обрабатывающей ПД, ее системный блок закрывается Ответственным лицом на ключ (при наличии штатных механических замков).

7.2.14. При изъятии рабочей станции (сервера), обрабатывающей ПД, из состава рабочих станций (серверов) структурного подразделения ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как Ответственное лицо снимет с данной рабочей станции (сервера) СЗИ и предпримет необходимые меры для затирания/удаления защищаемой информации, которая хранилась на дисках компьютера.

## **8. Требования по обеспечению безопасности при применении средств криптографической защиты информации**

8.1. Криптографическая защита в ИСПД создается на основе сертифицированных СКЗИ, встраивание которых в ИСПД должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

8.2. Ответственным за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ является Ответственное лицо. К работе с СКЗИ допускаются только работники, знающие правила их эксплуатации, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

8.3. Ответственное лицо должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и СЗИ.

8.4. Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее - помещения), должны обеспечивать безопасность информации, СКЗИ и крипто ключей, должны быть сведены к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

## **9. Порядок организации внутреннего обучения персонала правилам и мерам защиты персональных данных**

## 9.1. Общий порядок

9.1.1. Решение основных вопросов обеспечения защиты ПД должно предусматривать соответствующую подготовку кадров. Проведение обучения работников Общества позволит организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности ПД при их обработке в ИСПД и реализовать установленный комплекс организационных и технических мер по защите ПД.

9.1.2. Систему внутреннего обучения персонала в области защиты ПД составляет:

- проведение инструктажа пользователей ИСПД;
- самостоятельное изучение работниками Общества необходимых для работы документов, средств и продуктов.

В результате прохождения обучения работники Общества получают необходимые знания и навыки в отношении:

- правил использования СЗИ;
- содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности ПД при их обработке в ИСПД;
- основных мероприятий по организации и техническому обеспечению безопасности ПД при их обработке в ИСПД;
- планирования, организации и контроля выполнения мероприятий по обеспечению безопасности ПД при их обработке в ИСПД.

## 9.2. Проведение инструктажа пользователей ИСПД

9.2.1. Пользователи ИСПД, допущенные к работе с ПД, обязаны пройти инструктаж по вопросам обеспечения безопасности ПД с целью подтверждения своих знаний и уяснения своих обязанностей по поддержанию установленного режима защиты ПД.

9.2.2. Инструктаж представляет собой ознакомление работников Общества, допущенных к работе в ИСПД, с положениями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при ее обработке в ИСПД.

9.2.3. Работники Общества, не прошедшие инструктаж, к работе в ИСПД не допускаются. Инструктаж проводится перед началом работы в ИСПД новых работников Общества.

Инструктаж проводится в соответствии с Инструкцией по проведению инструктажа лиц, допущенных к работе с информационной системой ПД ЗАО «Системой АКСЕКО»

9.2.4. Проверка знаний пользователями ИСПД положений нормативной документации по вопросам обеспечения безопасности ПД проводится Ответственным лицом в ходе периодического контроля соблюдения режима безопасности информации.

9.3. Ответственность должностных лиц за обеспечение безопасности ПД, своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗПД

9.3.1. Ответственность за обеспечение безопасности ПД, организацию режима обеспечения безопасности ПД, своевременность качество формирования требований по защите ПД, за качество и научно-технический уровень разработки СЗПД, контроль исполнения правил и требований, направленных на обеспечение безопасности ПД, возлагается на Ответственное лицо.

9.4. Порядок контроля обеспечения уровня защищенности ПД и оценки соответствия ИСПД

9.4.1. Контроль обеспечения требуемого уровня защищенности ПД заключается в проверке выполнения требований нормативных документов по защите ПД, а также в оценке обоснованности эффективности принятых мер. Мероприятия по контролю защищенности ПД могут проводиться как Ответственным лицом, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации. Мероприятия по контролю защищенности ПД и оценке соответствия ИСПД включают:

- внутренний контроль режима безопасности ПД (оперативный и периодический);
- обследование защищенности ПД с привлечением сторонней организации;
- оценку соответствия ИСПД требованиям безопасности ПД.

## **10. Внутренний контроль режима безопасности персональных данных и оценки соответствия информационной системы персональных данных требованиям безопасности персональных данных**

10.1. Общие положения и виды контроля

10.1.1. Внутренний оперативный контроль соблюдения режима безопасности ПД проводится Ответственным лицом в режиме реального времени. Внутренний контроль заключается в анализе защищенности ПД посредством используемых в составе ИСПД программных и программно-аппаратных средств (систем) анализа защищенности.

10.1.2. В ходе проведения контроля соблюдения режима безопасности ПД Ответственное лицо:

- осуществляет анализ лог-файлов, производимых средствами защиты и другими элементами ИСПД (ОС, прикладные программы);
- просматривает оповещения средств защиты ИСПД;

- принимает меры по результатам анализа полученных оповещений и лог-файлов.

10.1.3. Внутренний периодический контроль заключается в оценке выполнения требований нормативных документов по обеспечению безопасности ПД, обрабатываемых в ИСПД.

10.1.4. В ходе проведения внутреннего периодического контроля проверяются следующие вопросы:

- соответствие состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (ПД), документированному составу и структуре средств, разрешенных для обработки такой информации;

- знание работниками Общества руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях;

- проверка наличия документов, подтверждающих возможность применения технических и программных СВТ для обработки ПД и применения СЗИ (сертификатов соответствия и других документов);

- проверка правильности применения СЗИ;

- проверка выполнения требований по условиям размещения АРМ в рабочих помещениях;

- соответствие реального уровня полномочий по доступу к защищаемой информации (ПД) различных пользователей установленному в списке лиц, допущенных к обработке ПД, уровню полномочий;

- знание инструкций по обеспечению безопасности информации пользователями ИСПД;

- организация хранения носителей ПД и допуска в помещения, где размещены средства обработки и осуществляется обработка ПД;

- прохождение инструктажа пользователей по вопросам обеспечения безопасности ПД и выполнение ими установленных требований.

10.1.5. По фактам несоблюдения условий хранения носителей ПД, использования СЗИ, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, проводится разбирательство составляется соответствующее заключение, на основе которого впоследствии осуществляется разработка и реализация мер по предотвращению возможных опасных последствий подобных нарушений.

10.2. Обследование защищенности ПД внешней специализированной организацией

10.2.1. При необходимости обследование защищенности ПД проводится внешней специализированной организацией.

10.2.2. Привлекаемая для проведения обследования внешняя специализированная организация должна иметь лицензию на деятельность по технической защите конфиденциальной информации.

### 10.3. Порядок оценки соответствия ИСПД требованиям безопасности ПД

10.3.1. Оценка соответствия ИСПД требованиям безопасности ПД проводится в форме проверки готовности СЗИ к использованию.

10.3.2. Проверка готовности СЗИ к использованию осуществляется в ходе приемосдаточных испытаний СЗИ с составлением протоколов проверки и заключений о возможности их эксплуатации.

10.3.3. Проверка готовности СЗИ к использованию проводится в соответствии с разрабатываемой программой и методикой испытаний соответствующих СЗИ, определяющих порядок проверки выполнения СЗИ заявленных функций защиты.

## 11. Ведение журнала

11.1. Форма Журнала регистрации и выдачи материальных персональных данных (далее - Журнал) утверждается приказом генерального директора Общества.

11.2. Ответственность за ведение Журнала, а также за сохранность Журнала возлагается на Ответственное лицо.

11.3. Ведение Журнала может осуществляться с привлечением иных работников, допущенных к обработке соответствующих категорий ПД.

11.4. Обработка ПД, связанная с соблюдением требований настоящего Положения, осуществляется без использования средств автоматизации следующими способами: сбор, запись, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), удаление, уничтожение ПД, за исключением копирования.

11.5. Хранение Журнала осуществляется в течение 5 лет с 1 января года, следующего за годом окончания их делопроизводства. Хранение иных документов, предусмотренных настоящим Положением, осуществляется в течение сроков, предусмотренных законодательством об архивном деле в Российской Федерации.

11.6. При ведении Журнала должны соблюдаться следующие условия:

- копирование содержащейся в Журнале информации не допускается;
- ПД каждого субъекта ПД могут заноситься в Журнал не более одного раза в каждом случае.

## 12. Информирование, рассылка и актуализация

12.1. Периодическая проверка данного Положения проводится Ответственным лицом по мере необходимости.

12.2. Изменения в настоящее положение утверждаются Ответственным лицом. Все работники Общества должны быть ознакомлены со всеми вносимыми изменениями.