Губернские аптеки Положение по виду деятельности **Положение об обработке персональных данных**	СМК П 44 - 2018 (версия 2.0)

РАЗРАБОТЧИК:		
Должность	**ФИО**	**Подпись**
Юрист	Кочеткова С.И.	

Введен в действие 04.06.2018
каким документом/ от какого числа

Сведения о документе взамен СМК П 44 - 2016 (версия 1.0)
введен впервые/ взамен (№ и дата предыдущей версии)

УТВЕРЖДАЮ
Генеральный директор
_____ А.М. Попова
«4» июня 2018г

Содержание:

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ 2
2. НОРМАТИВНЫЕ ДОКУМЕНТЫ 2
3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 2
4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 5
5. ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С СОГЛАСИЯ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ. 6
6. ФУНКЦИИ ДЕПАРТАМЕНТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЧАСТИ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 7
7. ДЕЙСТВИЯ (ОПЕРАЦИИ) С ПЕРСОНАЛЬНЫМИ ДАННЫМИ 8
8. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ 14
9. ОСНОВНЫЕ ТРЕБОВАНИЯ И ПРАВИЛА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН ОБЩЕСТВА 15
10. ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ОБРАБАТЫВАЕМОЙ В ИСПДН ИНФОРМАЦИИ 16
11. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО РАЗМЕЩЕНИЮ, СПЕЦИАЛЬНОМУ ОБОРУДОВАНИЮ, ОХРАНЕ И РЕЖИМУ ДОПУСКА В ПОМЕЩЕНИЯ, ГДЕ РАЗМЕЩЕНЫ СРЕДСТВА ИСПДН 17
12. ПРАВИЛА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ 18
13. ТРЕБОВАНИЯ К РЕЗЕРВИРОВАНИЮ ИР 19
14. ПРАВИЛА ЗАЩИТЫ ИСПДН ОТ ВРЕДОНОСНЫХ ПРОГРАММ 20
15. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ. 20
16. ПОРЯДОК ОРГАНИЗАЦИИ ВНУТРЕННЕГО ОБУЧЕНИЯ ПЕРСОНАЛА ПРАВИЛАМ И МЕРАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ 21
17. ПОРЯДОК КОНТРОЛЯ ОБЕСПЕЧЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОЦЕНКИ СООТВЕТСТВИЯ ИСПДН 21
18. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ПОЛОЖЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ 23

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 24

ЛИСТ ОЗНАКОМЛЕНИЯ 25

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Положение об обработке персональных данных в АО «Губернские аптеки» (далее – «Положение») определяет порядок и условия Оператора в отношении обработки персональных данных, устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, связанных с обработкой персональных данных.

1.2. Данное Положение разработано с целью обеспечения защиты персональных данных работников, соискателей, контрагентов по договорам гражданско-правового характера, льготополучателей, врачей, покупателей Интернет-магазина и иных категорий граждан в соответствии с требованиями действующего законодательства Российской Федерации.

1.3. Требования данного положения распространяются на всех работников Общества.

1.4. Действие настоящего Положения не распространяется на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

2. НОРМАТИВНЫЕ ДОКУМЕНТЫ

Реквизиты документа	Название
Принята всенародным голосованием 12.12.1993	Конституция Российской Федерации
№ 197-ФЗ от 30.12.2001	Трудовой кодекс Российской Федерации
Федеральный закон № 152-ФЗ от 27.07.2006	Федеральный закон «О персональных данных»
Федеральный закон № 149-ФЗ от 27.07.2006	Федеральный закон «Об информации, информационных технологиях и о защите информации»
Постановление Правительства РФ от 01.11.2012 № 1119	«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Постановление Правительства РФ от 15.09.2008 № 687	«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Приказ ФСТЭК России от 18.02.2013 № 21	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящего Положения используются следующие основные понятия:

Автоматизированная обработка персональных данных – обработка персональных данных (ПДн) с помощью средств вычислительной техники.

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

Администратор безопасности информации (администратор безопасности) – Сотрудник ДИТ, ответственный за защиту информационных систем персональных данных (ИСПДн) от несанкционированного доступа (НСД) к информации.

Администратор информационной системы персональных данных – администратор автоматизированной системы, администратор локальной вычислительной сети, администратор баз данных, администратор информационного ресурса (ИР) – ответственный за функционирование ИСПДн в установленном штатном режиме работы.

Владелец информации (информационного ресурса) – структурное подразделение АО «Губернские аптеки», реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец устанавливает в пределах своей компетенции режим и правила обработки информации, защиты ИР, доступа к ИР, условия копирования и тиражирования ИР (в распоряжении на создание ИР или в виде отдельных регламентов).

Доступ к информации – возможность получения информации и ее использования.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств (ТС).

Инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности (отказ в обслуживании, сбор информации, НСД и т.д.).

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

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн (в данном Положении – АО «Губернские аптеки»).

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

Технические средства, позволяющие осуществлять обработку персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:

- сбор,
- запись,
- систематизацию,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передачу (распространение, предоставление, доступ),
- обезличивание,
- блокирование,
- удаление,
- уничтожение персональных данных;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность персональных данных – обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом

специальные категории персональных данных – персональные данные, в том числе, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости

биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность

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

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

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

доступ к информации – возможность получения информации и ее использования;
обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
база данных - представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ);
юридические последствия - возникновение, изменение или прекращение личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы
Иные понятия в настоящих Правилах используются в значениях, определенных действующим законодательством Российской Федерации либо их значение дается по тексту.
АРМ – автоматизированное рабочее место
ДИТ – департамент информационных технологий
ИСПДн – информационная система персональных данных
ПДн – персональные данные
ПО – программное обеспечение
ТС – техническое средство

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных должна осуществляться на основе следующих принципов:
- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого или поручителем по которому является субъект персональных данных;
- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- соблюдение конфиденциальности персональных данных;
- обработки персональных данных с письменного согласия субъектов персональных данных либо на ином законом основании;
- принятии необходимых правовых, организационных и технических мер или обеспечении их принятия для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;
- документального оформления всех принятых решений по обработке и обеспечению безопасности персональных данных.

5. ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С СОГЛАСИЯ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

В случае если обработка персональных данных субъекта персональных данных в информационной системе персональных данных осуществляется на основании согласия и не имеется оснований для обработки таких персональных данных без получения согласия, должны выполняться указанные в настоящем пункте правила.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных должно быть:

- конкретным,
- информированным,
- сознательным.

Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа,

подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие,

общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

- подпись субъекта персональных данных.

Согласие на обработку персональных данных Обществом может быть дано субъектом персональных данных или его представителем только в письменной форме. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны представить документы, подтверждающие их полномочия.

Допускается включение согласия в типовые формы (бланки) документов и в договоры с субъектами персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем направления обращения в адрес Общества.

6. ФУНКЦИИ ДЕПАРТАМЕНТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЧАСТИ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для организации и обеспечения безопасности ПДн при их обработке в ИСПДн ответственным структурным подразделением за обеспечение безопасности ПДн является отдел администрирования и информационных технологий

6.1. Функции подразделения ДИТ

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

7. ДЕЙСТВИЯ (ОПЕРАЦИИ) С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Обработкой персональных данных называется любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая:

- сбор персональных данных,
- запись персональных данных,
- систематизацию персональных данных,
- накопление персональных данных,
- хранение персональных данных,
- уточнение (обновление) персональных данных,
- уточнение (изменение) персональных данных,
- извлечение персональных данных,
- использование персональных данных,
- передачу (распространение) персональных данных,
- передачу (предоставление) персональных данных,
- передачу (доступ) персональных данных,
- обезличивание персональных данных,
- блокирование персональных данных,

- удаление персональных данных,
- уничтожение персональных данных.

7.1. **Осуществление сбора персональных данных**

В Обществе применяются следующие способы получения персональных данных субъектов персональных данных:

- заполнение субъектом персональных данных соответствующей формы;
- получение персональных данных от третьих лиц;

Получение персональных данных В Обществе допускается только:

- непосредственно от субъекта персональных данных;
- от третьих лиц по основаниям, указанным в разделе 5 настоящего Положения.

Получение персональных данных из иных источников не допускается.

7.2. **Правила сбора персональных данных**

Если основания на обработку персональных данных без согласия отсутствуют, то необходимо получение согласия субъекта персональных данных на обработку его персональных данных. Обработка персональных данных без получения такого согласия категорически запрещается.

Если персональные данные получены не от субъекта персональных данных, Общество до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию;

наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные права субъекта персональных данных;

источник получения персональных данных.

Общество освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены Обществом на основании федерального закона или в связи с исполнением договора, стороной которого является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- Общество осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

7.3. **Осуществление систематизации, накопления, уточнения и использования персональных данных**

Систематизация, накопление, уточнение, использование персональных данных могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами, регламентами и иными документами, определяющими технологический процесс обработки информации.

В Обществе могут быть установлены особенности учета персональных данных в ИСПд, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей ИСПд, конкретному субъекту персональных данных

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в ИСПд, конкретному субъекту персональных данных.

Уточнение персональных данных должно производиться только на основании законно полученной в установленном порядке информации.

Решение об уточнении персональных данных субъекта персональных данных принимается лицом, ответственным за организацию обработки персональных данных в Обществе.

Использование персональных данных должно осуществляться исключительно в заявленных целях. Использование персональных данных в заранее не определенных и не оформленных установленным образом целях не допускается.

7.4. **Осуществление записи и извлечения персональных данных**

Запись персональных данных в ИСПд Общества может осуществляться с любых носителей информации или из других ИСПд.

Извлечение персональных данных из информационных систем персональных данных может осуществляться с целью:

- вывода персональных данных на бумажный или иной носитель информации, не предназначенный для его обработки средствами вычислительной техники;
- вывода персональных данных на носители информации, предназначенные для их обработки средствами вычислительной техники.

При извлечении персональных данных должен проводится учет и обозначение носителей информации.

При осуществлении записи и извлечения персональных данных должны соблюдаться условия обработки персональных данных и конфиденциальность персональных данных.

7.5. **Осуществление передачи персональных данных**

В Обществе используются следующие способы передачи персональных данных субъектов персональных данных:

- передача персональных данных на электронных носителях информации посредством средств шифрования и криптографической защиты;
- передача персональных данных на бумажных носителях посредством нарочного;
- передача персональных данных посредством электронной связи с помощью средств шифрования и криптографической защиты.

Перед осуществлением передачи персональных данных проверяется основание на осуществление такой передачи и наличие согласия на передачу персональных данных в согласии субъекта персональных данных на обработку персональных данных или наличие иных законных оснований.

Передача персональных данных должна осуществляться на основании:

- согласия субъекта персональных данных на обработку и передачу ПДн;
- договора с третьей стороной, которой осуществляется передача персональных данных;
- запроса, полученного от третьей стороны, которой осуществляется передача персональных данных;
- исполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей.

Передача персональных данных без согласия субъекта ПДн или иных законных оснований запрещается.

7.6. **Осуществление хранения персональных данных**

Хранение персональных данных допускается только в форме документов – зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

- фотодокумент – изобразительный документ, созданный фотографическим способом;
- текстовой документ – документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;
- письменный документ – текстовой документ, информация которого зафиксирована любым типом письма;
- рукописный документ – письменный документ, при создании которого знаки письма наносят от руки;
- машинописный документ – письменный документ, при создании которого знаки письма наносят техническими средствами;
- изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта (например, рентгеновские снимки);
- документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Персональные данные субъектов персональных данных могут храниться как на бумажных носителях, так и в электронном виде (компьютерной сети).

Хранение персональных данных в Обществе осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого или поручителем по которому является субъект персональных данных.

Хранение персональных данных в ИСПд и вне таких систем осуществляется только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного:

доступа к ним,
их уничтожения,
изменения,
блокирования,
копирования,
предоставления,
распространения.

7.7. **Осуществление блокирования персональных данных**

Блокирование персональных данных конкретного субъекта персональных данных должно осуществляться во всех информационных системах персональных данных Общества, включая архивы баз данных, содержащих такие персональные данные, информационных систем персональных данных.

Блокирование персональных данных осуществляется:
- в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;
- в случае отсутствия возможности уничтожения персональных данных в установленные сроки до их уничтожения.

После устранения выявленной неправомерной обработки персональных данных осуществляется снятие блокирования персональных данных.

Решение о блокировании и снятии блокирования персональных данных субъекта персональных данных принимается ответственным за организацию обработки персональных данных в Обществе.

7.8. **Осуществление обезличивания персональных данных**

Обезличивание персональных данных при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей. Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.9. **Осуществление удаления и уничтожения персональных данных**

Уничтожение персональных данных это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Уничтожение персональных данных производится только в следующих случаях:

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки персональных данных, если обеспечить правомерность обработки персональных данных невозможно;
- в случае достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных.

По факту уничтожения персональных данных обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования, осуществляется уведомление указанных в таком требовании лиц.

При уничтожении персональных данных необходимо:

- убедиться в необходимости уничтожения персональных данных;
- убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;
- уничтожить персональные данные подходящим способом, в соответствии с настоящими Правилами или способом, указанным в соответствующем требовании или распорядительном документе;
- проверить необходимость уведомления об уничтожении персональных данных;

при необходимости, уведомить об уничтожении персональных данных требуемых лиц.

При уничтожении персональных данных применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) – для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержавшем персональные данные;
- измельчение в специальной бумагорезательной (бумагоуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для носителей информации на оптических дисках;
- физическое уничтожение частей носителей информации – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);

- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе. При уничтожении персональных данных необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством Российской Федерации.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится лицами, обрабатывающими персональные данные в соответствующей информационной системе персональных данных, в которой производится уничтожение персональных данных, только в присутствии лица, ответственного за организацию обработки персональных данных в Обществе.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, который подписывается лицами, производившими уничтожение, заверяется лицом, ответственным за организацию обработки персональных данных в Обществе, присутствовавшим при уничтожении и утверждается заместителем генерального директора по управлению инфраструктурой.

Хранение актов уничтожения персональных данных осуществляется в течение срока исковой давности, если иное не установлено нормативно-правовыми актами Российской Федерации.

7.10. **Особенности обработки специальных категорий персональных данных**

В Обществе категорически запрещается обработка специальных категорий персональных данных касающихся:

расовой принадлежности;
национальной принадлежности;
политических взглядов;
религиозных убеждений;
философских убеждений;
интимной жизни.

В Обществе разрешается обработка специальных категорий персональных данных, касающихся состояния здоровья при обязательном соблюдении любого из следующих условий:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, о противодействии терроризму, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

Обработка специальных категорий персональных данных в остальных случаях в Обществе не допускается.

Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

8. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЯ

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

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

Модель угроз решает следующие задачи:

- анализ защищенности информационной системы персональных данных от угроз безопасности персональных данных в ходе учреждении и выполнения работ по обеспечению безопасности персональных данных;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационной системы персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональных данных и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы персональных данных, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных Общества должна содержать систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных, обусловленных преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационной системе персональных данных, связанным:

- с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационной системы персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационной системы персональных данных и обрабатываемых в них персональных данных с использованием

программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

Состав и содержание угроз безопасности персональным данным определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным.

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы персональных данных, свойств среды распространения информативных сигналов, содержащих защищаемую информацию, и возможностей и источников угроз.

При обеспечении безопасности персональных данных с использованием криптографических средств защиты информации производится нейтрализация атак, готовящимися и проводимыми нарушителями, причем возможности проведения атак обусловлены их возможностями. С учетом этого все возможные атаки определяются моделью нарушителя.

Модель нарушителя тесно связана с частной моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие:

- в модели угроз содержится максимально полное описание угроз безопасности объекта;
- модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

9. ОСНОВНЫЕ ТРЕБОВАНИЯ И ПРАВИЛА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН ОБЩЕСТВА

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

Основными направлениями защиты информации (ПДн) являются:

- обеспечение защиты информации (ПДн) от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;
- обеспечение защиты информации (ПДн) от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

Основными мерами защиты информации (ПДн) являются:

- назначение ответственного за организацию обработки ПДн;
- разработка документов, определяющих политику Общества в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ в области обеспечения безопасности ПДн, устранение последствий таких нарушений;
- оценка вреда, который может быть причинен субъектам ПДн 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;
- ограничение доступа пользователей в помещения, где размещены ТС, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;
- 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, исключающее хищение, подмену и уничтожение;
- резервирование ТС, дублирование массивов и носителей информации;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
- использование защищенных каналов связи;
- размещение ТС, позволяющих осуществлять обработку ПДн, 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 ПДн;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

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

Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

10. ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ОБРАБАТЫВАЕМОЙ В ИСПДН ИНФОРМАЦИИ

Данный раздел Положения регламентирует порядок взаимодействия подразделений Общества по обеспечению безопасности ПДн при организации разрешительной системы доступа к сервисам и ресурсам ИСПДн Общества.

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

Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности ПДн 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 ИСПДн Общества;
- разработку ВНД, определяющих порядок реализации и функционирования разрешительной системы доступа.

Основные условия правомерного доступа сотрудников Общества к обрабатываемой в ИСПДн Общества информации включают в себя:

- подписание сотрудником Общества Обязательства о неразглашении конфиденциальной информации либо включение обязательства о неразглашении работником конфиденциальной информации в Трудовой договор;
- наличие утвержденных руководством Общества должностных (функциональных) обязанностей сотрудника, определяющих круг его задач и объем необходимой для их решения информации.

Лица, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании утвержденного Перечня должностей работников, допущенных к обработке ПДн.

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

При регистрации и назначении прав доступа пользователей ИСПДн Общества 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 ИСПДн Общества;
- 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 ИСПДн 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 ИСПДн;
- при изменении должностных обязанностей (увольнении) пользователя должно проводиться немедленное исправление (аннулирование) прав его доступа;
- администраторами ИСПДн должно проводиться удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы должны быть недоступны другим пользователям.

Контроль выполнения требований разрешительной системы доступа к ПДн возлагается на начальника отдела администрирования и информационной безопасности.

Допуск к ИР ИСПДн 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.

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

11. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО РАЗМЕЩЕНИЮ, СПЕЦИАЛЬНОМУ ОБОРУДОВАНИЮ, ОХРАНЕ И РЕЖИМУ ДОПУСКА В ПОМЕЩЕНИЯ, ГДЕ РАЗМЕЩЕНЫ СРЕДСТВА ИСПДН

Данный раздел Положения содержит общие требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены ИСПДн Общества.

Должен быть организован контроль доступа персонала и посетителей в помещения Общества, в которых установлены ТС ИСПДн и осуществляется обработка ПДн, а также хранятся носители ПДн.

Доступ должностных лиц структурных подразделений Общества в помещения, в которых осуществляется обработка ПДн, организовывается в соответствии с должностными обязанностями сотрудников. Доступ другого персонала Общества и посетителей в эти помещения должен осуществляться в сопровождении ответственных должностных лиц.

Для защиты помещений, в которых расположены ТС ИСПДн, должны быть приняты меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

ТС ИСПДн и размещенное совместно с ними вспомогательное оборудование должны подвергаться регулярным осмотрам с целью выявлений изменения конфигурации средств вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.).

Должно быть обеспечено размещение устройств вывода информации средств вычислительной техники, дисплеев АРМ ИСПДн таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

12. ПРАВИЛА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

При обращении со съемными носителями ПДн должны выполняться следующие основные правила:

- носители ПДн должны быть учтены, выданы пользователям под роспись и защищены;
- носители ПДн, срок эксплуатации которых истек, должны уничтожаться в установленном порядке;
- для выноса носителей ПДн за пределы объектов Общества должно быть получено специальное разрешение, а факт выноса – зафиксирован в специальной базе данных;
- все носители ПДн должны храниться в безопасном месте в соответствии с требованиями по их эксплуатации.

Ответственным за хранение, учет и выдачу съемных носителей ПДн является ответственный сотрудник ДИТ - начальник отдела администрирования и информационной безопасности.

Все находящиеся на хранении и в обращении съемные носители ПДн должны быть учтены в Журнале учета носителей ПДн.

Каждый носитель, с записанными на нем ПДн, должен иметь этикетку, на которой указывается метка съемного носителя и гриф.

Пользователи ИСПДн для выполнения работ получают учтенный съемный носитель от ответственного работника ДИТ. При получении делаются соответствующие записи в Журнале учета.

После окончания работ пользователь ИСПДн сдает съемный носитель в помещение для хранения, о чем делается соответствующая запись в Журнале учета. При наличии личного сейфа у пользователя ИСПДн допускается хранение учтенных съемных носителей в личных сейфах, опечатанных печатью пользователя ИСПДн.

Носители ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

Уничтожение носителей ПДн осуществляется комиссией по уничтожению, назначенной приказом по представлению руководителя ДИТ.

Уничтожение магнитных, оптических и магнитооптических носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него должна быть стерта (уничтожена), если это позволяют физические принципы работы носителя.

Бумажные носители данных уничтожаются на специальных бумагорезательных устройствах (шредерах).

Перед утилизацией оборудования, участвующего в обработке ПДн, сотрудником подразделения ИТ осуществляется проверка всех его компонентов, включая носители информации (жесткие диски) на отсутствие ПДн и лицензированного программного обеспечения (ПО).

По результатам уничтожения комиссией составляется Акт уничтожения носителей ПДн, который хранится в помещении для хранения носителей ПДн, уничтоженные носители ПДн (утилизированное оборудование) снимается с материального учета.

13. ТРЕБОВАНИЯ К РЕЗЕРВИРОВАНИЮ ИР

Резервное копирование защищаемой информации (ПДн) применяется для оперативного восстановления данных в случае утери или по другим причинам.

В состав ИР, подлежащих резервному копированию, в обязательном порядке включаются ИР, являющиеся объектом защиты в Общества.

При организации резервирования ИР необходимо обеспечить выполнение следующих требований:

- резервные копии ИР и инструкции по их восстановлению должны храниться в специально выделенном месте, территориально отдаленном от места хранения основной копии информации;
- к резервным копиям должен быть применен комплекс физических и организационных мер защиты;
- носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие сбоев;
- применяемая система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью;
- должны быть предусмотрены регулярная проверка процедур восстановления и практический тренинг персонала по восстановлению данных.

Резервное копирование информации осуществляется работниками ДИТ в пределах своих полномочий в соответствии с графиком резервного копирования. Допускается осуществление резервного копирования в автоматизированном режиме.

График резервного копирования составляется для каждого вида информации, подлежащей периодическому резервному копированию, утверждается руководителем подразделения ИТ и согласовывается с руководителем подразделения ИБ. Периодичность проведения резервного копирования устанавливается Графиком резервного копирования не реже одного раза в неделю и может осуществляться ежедневно (в автоматизированном режиме).

Резервное копирование информации производится в соответствии с документацией на используемое ПО.

Программно-аппаратные средства, обеспечивающие проведение резервного копирования и носители, на которые осуществляется резервное копирование, не реже одного раза в месяц проверяются на отсутствие сбоев сотрудниками ДИТ в соответствии с документацией на программно-аппаратные средства с отметкой в Журнале проверки работоспособности системы резервного копирования.

Резервные копии данных хранятся вместе с инструкцией по восстановлению данных из резервных копий в отдельном помещении от используемых данных.

Восстановление данных из резервной копии производится сотрудниками подразделения ИТ на основании Заявки руководителя структурного подразделения – владельца информационного ресурса. Заявка может предоставляться в электронной форме.

Восстановление данных из резервных копий осуществляется в соответствии с документацией на используемое ПО в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

14. ПРАВИЛА ЗАЩИТЫ ИСПДН ОТ ВРЕДОНОСНЫХ ПРОГРАММ

При использовании в ИСПДн средств антивирусной защиты и защиты от вредоносных программ, должны выполняться следующие организационные меры:

- использование съемных носителей ПДн пользователя ИСПДн на других компьютерах только с механической защитой от записи;
- запрет на использование посторонних съемных носителей ПДн при работе в ИСПДн;
- запрет на передачу съемных носителей ПДн посторонним лицам
- запрет на запуск программ с внешних съемных носителей информации при работе в ИСПДн;
- запрет на несанкционированное использование отчуждаемых носителей информации (оптических дисков, флэш-карт и т. п.);
- использование в ИСПДн только дистрибутивов программных продуктов, приобретенных у официальных дилеров фирм-разработчиков этих продуктов;
- обязательная проверка всех программных продуктов;
- проверка всех программных файлов и файлов документов, полученных по электронной почте, специальными антивирусными средствами;
- систематическая проверка содержимого дисков файловых хранилищ обновленными версиями антивирусных программ;
- контроль и обновление списка разрешенных ссылок на веб-ресурсы сети Интернет.

Ответственность за эксплуатацию средств антивирусной защиты и защиты от вредоносных программ возлагается на сотрудников ДИТ в части наличия антивирусного ПО на клиентских рабочих станциях и использования данного ПО пользователями.

15. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

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

Организация доступа пользователей ИСПДн к сети Интернет осуществляется сотрудником подразделения ИТ на основании служебной записки начальника отдела.

Пользователю 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.

При работе с ресурсами сети Интернет запрещается:

- разглашение сведений конфиденциального характера Общества, включая ПДн, 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 несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа 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.

Вся информация о ресурсах, посещаемых сотрудниками Общества, протоколируется.

При нарушении сотрудником Общества правил работы в сети Интернет либо возникновении нештатных ситуаций доступ к ресурсам сети Интернет может быть блокирован.

16. ПОРЯДОК ОРГАНИЗАЦИИ ВНУТРЕННЕГО ОБУЧЕНИЯ ПЕРСОНАЛА ПРАВИЛАМ И МЕРАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Решение основных вопросов обеспечения защиты ПДн достигается за счет соответствующей подготовки кадров.

Систему внутреннего обучения персонала в области защиты ПДн составляет:
- проведение инструктажа пользователей ИСПДн;
- изучение сотрудниками Общества необходимых для работы документов, средств и продуктов.

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

Инструктаж представляет собой ознакомление сотрудников Общества, допущенных к работе в ИСПДн, с настоящим Положением и действующими нормативными документами по обеспечению безопасности информации при ее обработке в ИСПДн.

Ознакомление с положениями нормативной документации сотрудник Общества подтверждает своей личной подписью в журнале инструктажа, что свидетельствует о прохождении инструктажа.

Контроль проведения инструктажа и периодическая проверка знания пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на начальника отдела администрирования и информационной безопасности совместно с руководителями структурных подразделений Общества, использующих ИСПДн. Ответственность за непосредственное проведение инструктажа возлагается на руководителей структурных подразделений Общества.

Сотрудники Общества, не прошедшие инструктаж, к работе в ИСПДн не допускаются. Инструктаж проводится перед началом работы в ИСПДн новых сотрудников Общества, а также не реже одного раза в год для всех пользователей ИСПДн.

Проверка знаний пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн проводится начальником отдела администрирования и информационной безопасности не реже одного раза в год в ходе периодического контроля соблюдения режима безопасности информации.

17. ПОРЯДОК КОНТРОЛЯ ОБЕСПЕЧЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОЦЕНКИ СООТВЕТСТВИЯ ИСПДН

Контроль обеспечения требуемого уровня защищенности ПДн заключается в проверке выполнения требований нормативных документов по защите ПДн, а также в оценке

обоснованности и эффективности принятых мер. Мероприятия по контролю защищенности ПДн могут проводиться как уполномоченными сотрудниками КРО, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации. Мероприятия по контролю защищенности ПДн и оценке соответствия ИСПДн включают:

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

Внутренний оперативный контроль соблюдения режима безопасности ПДн проводится начальником отдела администрирования и информационной безопасности ежедневно в режиме «реального времени». Внутренний контроль заключается в анализе защищенности ПДн посредством используемых в составе ИСПДн программных и программно-аппаратных средств (систем) анализа защищенности.

В ходе проведения контроля соблюдения режима безопасности ПДн начальник отдела администрирования и информационной безопасности:

- осуществляет анализ лог-файлов, производимых средствами защиты и другими элементами ИСПДн (операционная система, прикладные программы);
- просматривает оповещения средств защиты ИСПДн;
- принимает меры по результатам анализа полученных оповещений и лог-файлов.

Внутренний периодический контроль осуществляется КРО 1 раз в год и заключается в оценке выполнения требований нормативных документов по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

В ходе проведения внутреннего периодического контроля проверяются следующие вопросы:

- соответствие состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (ПДн), документированному составу и структуре средств, разрешенных для обработки такой информации;
- знание персоналом 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 средств вычислительной техники для обработки ПДн и применения средств защиты информации (сертификатов соответствия и других документов);
- проверка правильности применения средств защиты информации;
- проверка выполнения требований по условиям размещения АРМ в рабочих помещениях;
- соответствие реального уровня полномочий по доступу к защищаемой информации (ПДн) различных пользователей установленному в списке лиц, допущенных к обработке ПДн, уровню полномочий;
- знание инструкций по обеспечению безопасности информации пользователями ИСПДн;
- организация хранения носителей ПДн и допуска в помещения, где размещены средства обработки и осуществляется обработка ПДн;
- прохождение инструктажа пользователей по вопросам обеспечения безопасности ПДн и выполнение ими установленных требований.

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

Результаты контроля оформляются Актом, в котором делаются выводы о состоянии обеспечения безопасности ПДн на проверяемом объекте информатизации и приводятся рекомендации по его совершенствованию.

18. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ПОЛОЖЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Настоящее Положение вступает в силу с момента его утверждения генеральным директором Общества и действует бессрочно, до утверждения новой версии Положения либо его отмены.

Изменения в Положение вносятся приказом генерального директора.

Работники Общества должны быть ознакомлены с Положением под роспись.

СОГЛАСОВАНИЕ

	Должность	Фамилия	Подпись
Согласовал	Менеджер по качеству	Иванеева Н.С.	
	Начальник юридического отдела	Логунова А.М.	
	Заместитель генерального директора по правовым вопросам	Чернова О.В.	
	Заместитель генерального директора по управлению инфраструктурой	Баркалова Т.В.	
	Заместитель генерального директора по кадровым вопросам	Политова Е.С.	
	Заместитель генерального директора по льготному лекарственному обеспечению	Чудинова Л.Б.	
	Начальник отдела администрирования и информационной безопасности	Салогубов А.В.	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Версия	Дата	Автор	Содержание изменения
2.0		Кочеткова С.И.	Актуализация в связи реорганизацией

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Должность сотрудника	Ф.И.О.	личная подпись	дата ознакомления