

УТВЕРЖДАЮ
Директор ООО «УК «Пионер»
Р.В. Копьюв
15 августа 2015 г.

ПОЛОЖЕНИЕ
о защите персональных данных ООО УК «Пионер»

(620137, г. Екатеринбург, ул. Новая, д.9)

г. Екатеринбург, 2015

ОГЛАВЛЕНИЕ

1. Общие положения 5

2. Понятия и определения 6

3. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Обществе

3.1. Общие положения 8

3.2. Принципы и цели обработки персональных данных 8

3.3. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных 7

3.4. Перечень обрабатываемых персональных данных 9

3.5. Категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения 10

3.6. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований 11

3.7. Обязанности уполномоченных лиц на получение, обработку, хранение, передачу и любое другое использование персональных данных при обработке персональных данных 12

3.8. Права и обязанности Общества при обработке персональных данных субъектов персональных данных 12

3.9. Меры, направленные на обеспечение выполнения Обществом своих обязанностей 16

3.10. Права и обязанности субъекта персональных данных 18

3.11. Ответственность лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных 18

3.12. Меры, принимаемые для защиты персональных данных 19

4. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных 19

5. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных 20

6. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных 20

6.1. Порядок внешнего контроля над соблюдением требований по обработке и обеспечению безопасности данных 21

6.2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных 22

7. Правила взаимодействия с субъектами персональных данных и иными лицами 23

7.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных 24

7.2. Требования по уведомлениям (предоставлению информации, разъяснениям) субъектов персональных данных и в иных случаях 25

7.3. Лица, ответственные за организацию обработки персональных данных 27

7.3.1. Должностная инструкция ответственного за организацию обработки персональных данных в Обществе 28

7.3.2. Должностная инструкция ответственного за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества 29

7.4. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав 32

7.5. Порядок действий при обращениях субъектов персональных данных 32

7.6. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных 35

7.7. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных 35

8. Правила обработки персональных данных в информационных системах персональных данных.....35
8.1. Обработка персональных данных без использования средств автоматизации.....35
8.2. Обработка персональных данных с использованием средств автоматизации.....36
8.2.1. Исключительно автоматизированная обработка персональных данных.....38
8.2.2. Обработка персональных данных средствами автоматизации при поручении обработки персональных данных.....38
8.2.3. Обработка персональных данных средствами автоматизации при поручении обработки персональных данных другим лицом.....39
8.3. Смешенная обработка персональных данных.....39
9. Мероприятия по обеспечению безопасности персональных данных.....39
9.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.....40
9.2. Состав и содержание мер по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации.....40
9.3. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств персональных данных.....41
10. Правила работы с обезличенными персональными данными, обрабатываемыми в Обществе.....43
11. Политика Общества в отношении обработки персональных данных и реализации требований к защите персональных данных.....44
12. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.....48
13. Мероприятия по защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных.....50
13.1. Порядок доступа работников Общества в помещения, в которых ведется обработка персональных данных и организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и обеспечения сохранности носителей персональных данных.....51
13.2. Порядок обеспечения сохранности носителей персональных данных в Обществе.....52
13.3. Перечень лиц Общества, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.....53
13.4. Правила резервирования и восстановления данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним в Обществе.....53
14.1. Общие правила и требования, предъявляемые к системам резервирования информационных систем.....53
14.2. Разграничение полномочий по резервированию данных в информационных системах. Формирование рабочих резервных копий ИС Общества должно проводиться в автоматизированном режиме, путем соответствующих настроек комплекса резервирования.....54
14.3. Требования по размещению оборудования резервного копирования.....54
14.4. Объекты резервирования ИС и периодичность создания резервных копий.....54
14.5. Срок хранения рабочих резервных копий.....54
14.6. Количество резервных копий, объекты и субъекты их хранения.....54
14.7. Учет и регистрация съемных носителей резервных копий.....54
14.8. Правила работы и обязанности должностных лиц по процедуре резервирования и восстановления данных, хранению и уничтожению рабочих резервных копий.....54
14.9. Ответственность.....55
14.10. Контроль.....55
14.11. Расследование нарушений положений настоящей Политики.....55
15. Инструкция по обеспечению безопасности сведений при их обработке в информационных систем.....55
15.1. Порядок допуска персонала к сведениям при их обработке в информационных системах.....55
15.2. Принципы формирования личных паролей.....56

15.3. Обязанности персонала по использованию и сохранению в тайне личных паролей и ключевой информации.....57
15.4. Обязанности персонала по обеспечению защиты ИСПДн от вредоносных программ.....57
15.5. Правила работы персонала со сведениями при их обработке в информационных системах Общества.....58
15.5.1. Требования к пользователю.....59
15.5.2. Требования к администратору.....61
15.6. Контроль деятельности персонала.....63
15.7. Ответственность за нарушения информационной безопасности, порядок их рассмотрения.....63
16. Положение о служебном расследования нарушений режима информационной безопасности в информационных системах.....63
16.1. Классификация инцидентов информационной безопасности.....63
16.2. Перечень нарушений ИБ.....63
16.3. Порядок назначения и проведения служебного расследования.....65
16.4. Состав комиссии для проведения служебного расследования.....65
16.5. Ответственность.....65
16.6. Оформление результатов работы комиссии.....66
17. Порядок предоставления и контроля прав доступа к сведениям в информационной системе.....66
18. Порядок приостановления предоставления доступа к ресурсам информационной системы в случае обнаружения нарушений порядка ее использования.....67
19. Порядок обеспечения информационной безопасности в информационных системах средствами протоколирования и анализа значимых событий.....68

1. Общие положения

Настоящее Положение о защите персональных данных в ООО УК «Пионер» (далее - Положение) разработано на основании и во исполнение:

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

- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Настоящее Положение утверждается и вводится в действие приказом генерального директора ООО УК «Пионер» (далее - Общество) и является обязательным для исполнения всеми сотрудниками Общества. Настоящее Положение:

1. Устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

2. Определяет для каждой цели обработки персональных данных:

- содержание обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- сроки их обработки и хранения;
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- устанавливает порядок рассмотрения запросов субъектов персональных данных или их представителей;
- устанавливает порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;
- устанавливает типовую форму согласия на обработку персональных данных сотрудников и иных субъектов персональных данных;
- устанавливает типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- устанавливает порядок работы с обезличенными данными;
- определяет перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- определяет перечень программного обеспечения, используемого при обработке персональных данных в информационных системах Общества;
- определяет перечень должностей сотрудников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- определяет перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- устанавливает порядок ознакомления работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных сотрудников;
- устанавливает перечень и правила ведения иных локальных актов по вопросам обработки персональных данных, включая:
- перечень мест хранения персональных данных (материальных носителей);
- порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;
- должностную инструкцию ответственного за организацию обработки персональных данных;
- типовое обязательство сотрудников, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ними трудового контракта прекратить обработку персональных данных, ставших известными в связи с исполнением должностных обязанностей.

2. Понятия и определения

В настоящем Положении используются следующие основные понятия:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

- **автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники;
- **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;

- **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

- **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, earn иное не предусмотрено федеральным законом;

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

- **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;

- **под техническими средствами,** позволяющими осуществлять обработку персональных данных, понимаются 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 технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

- **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);

- **к юридическим последствиям** относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

Иные понятия в настоящем Положении используются в значениях, определенных действующим законодательством Российской Федерации либо их значение дается по тексту.

3. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Обществе

3.1. Общие положения

Настоящие правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Обществе (далее - Правила) разработаны на основании требований Трудового кодекса Российской Федерации, Жилищного кодекса Российской Федерации, «Правил предоставления коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов», утвержденных Правительством Российской Федерации от 6 мая 2011 г. № 354, федерального закона от 22 октября 2004 г. № 125-ФЗ "Об архивном деле в Российской Федерации", от 27 июля 2006 г. № 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", от 17 ноября 2007 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Целью Правил является определение порядка действий при обработке персональных данных, содержания обрабатываемых персональных данных, категорий субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Обществе.

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Действие настоящих Правил не распространяется на отношения, возникшие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям ограниченного распространения;
- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 г. № 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

3.2. Принципы и цели обработки персональных данных

Принципы обработки персональных данных:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, определенных настоящими Правилами 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. Должностные лица Общества должны 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 законодательством, законодательством Свердловской области, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости і достижении этих целей, если иное не предусмотрено законодательством.

Обработке в Обществе подлежат только персональные данные, которые отвечаю' нижеследующим целям их обработки:

- обеспечение соблюдения Конституции Российской Федерации, федеральных законов, законов Свердловской области, иных нормативных правовых актов Российской Федерации и Свердловской области, содействие работнику в обучении и должностном рост обеспечение его личной безопасности и членов его семьи, обеспечение сохранное принадлежащего ему имущества и имущества Общества, учет результатов исполнения и должностных обязанностей;

- предоставление коммунальных услуг собственникам и пользователям помещен в многоквартирных домах и жилых домах в соответствии с постановлением Правительства; Российской Федерации от 06.05.2011 № 354;

- статистическим целям;

- исполнения договора, стороной которого является субъект персональных данных.

3.3. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

Обработка персональных данных должна осуществляться на законной и справедливой основе.

Общество устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

- издание нормативных правовых актов, локальных актов Общества по вопросам обработки персональных данных;

- назначение ответственных за организацию обработки персональных данных;

- определение лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Обществе и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных;

- ознакомление сотрудников Общества, непосредственно осуществляющих обработку персональных данных под роспись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

- получение персональных данных лично у субъекта персональных данных, в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта

персональных данных, в случае возникновения необходимости получения персональных данных у третьей стороны Общество извещает об этом субъекта персональных данных заранее, получает его письменное согласие и сообщает ему о целях, предполагаемых источниках и способах получения персональных данных;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- опубликование на официальном сайте Общества в информационно-телекоммуникационной сети "Интернет" документов, определяющих политику Общества в отношении обработки персональных данных, реализуемые требования к защите персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Общества;
- уведомление субъекта персональных данных о совершенных операциях над персональными данными в установленной форме.

3.4. Перечень обрабатываемых персональных данных

В соответствии с целями обработки персональных данных, в Обществе обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- ИНН;
- СНИЛС;
- реквизиты документа, удостоверяющего личность (кем выдан, дата выдачи, код подразделения, срок действия);
- контактные телефоны (домашний и рабочий);
- адрес по прописке (с указанием даты регистрации);
- адрес места проживания;
- адрес для информирования (почтовый адрес)
- общие сведения о заработной плате в соответствии со штатным расписанием;
- сведения об образовании;
- сведения о повышении квалификации и переподготовке;
- сведения о воинском учете;
- сведения об отсутствии/наличии инвалидности и/или проф. заболевании;
- сведения о начислениях (удержаниях) заработной платы (на текущую дату или за период);
- иные сведения (банковский счет и т.д.).
- сведения о начислениях и поступлениях денежных средств на лицевые счета собственников и нанимателей за ЖКУ и прочие услуги;
- сведения о нанимателе жилого помещения, ордере решении жилищной комиссии, решении суда (номер, дата выдачи, кем выдан);
- сведения о собственнике жилого помещения, доли собственности (серия, номер, дата выдачи, кем выдан).

Сроки обработки указанных выше персональных данных определяются в соответствии со сроком действия соглашения с субъектом, приказом Министерства культуры Российской Федерации от 25 августа 2010 г. № 558 (с изм. от 04.02.2015) "Об утверждении "Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения"

(Зарегистрировано в Минюсте России 08.09.2010 № 18380), сроком исковой давности, а также иными требованиями законодательства и нормативными документами.

3.5. Категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения

К категориям субъектов, персональные данные которых обрабатываются в Обществе, относятся:

- работники, с которым заключены трудовые Договоры;
- жильцы, пользующиеся услугами Общества и входящие в состав ТСЖ;
- физические лица, состоящие в договорных отношениях с оператором;
- юридические лица, состоящие в договорных отношениях с оператором;
- субъекты, обратившиеся с письменным запросом и/или при помощи средств электронного портала для работы с запросами и обращениями.

Документы, содержащие персональные данные, обрабатываются в сроки, обусловленные заявленными целями их обработки.

Персональные данные, связанные с реализацией трудовых отношений обрабатываются и хранятся в течение действия служебного контракта (трудового договора) и в течение 75 (семидесяти пяти) лет после его прекращения.

Персональные данные, связанные с предоставлением услуг и осуществлением государственных функций, обрабатываются и хранятся до достижения цели их обработки.

Сроки хранения письменных обращений граждан - 5 лет.

Использование персональных данных осуществляется с момента их получения оператором и прекращается:

- по достижении целей обработки персональных данных;
- в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных.

Сроки хранения персональных данных устанавливаются в соответствии с номенклатурой дел Общества.

3.6. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

В случае достижения цели обработки персональных данных Общество обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

Уничтожение документов, содержащих персональные данные, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения персональных данных.

3.7. Обязанности уполномоченных лиц на получение, обработку, хранение, передачу и любое другое использование персональных данных при обработке персональных данных

Уполномоченные лица на получение, обработку, хранение, передачу и любое другое использование персональных данных обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных, настоящих Правил;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

При обработке персональных данных уполномоченным лицам на получение, обработку, хранение, передачу и любое другое использование персональных данных запрещается:

- использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях - при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;
- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации;
- снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные;
- выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, из места их хранения.

3.8. Права и обязанности Общества при обработке персональных данных субъектов персональных данных

Общество при обработке персональных данных субъектов персональных данных имеет право:

- обрабатывать персональные данные в соответствии с настоящим Положением;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, либо путем принятия Обществом соответствующего акта;
- мотивированно отказать субъекту персональных данных в выполнении повторного запроса в целях получения сведений касающейся обработки его персональных данных, при нарушении субъектом персональных данных своих обязанностей по подаче такого запроса;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором или Обществом;

- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- отказать субъекту персональных данных в выполнении запроса в целях получения сведений касающейся обработки его персональных данных в случае, если предоставление субъекту персональных данных таких сведений, нарушает права и законные интересы третьих лиц;

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных, если иное не предусмотрено указанным законом и другими федеральными законами;

- если обеспечить правомерность обработки персональных данных невозможно, осуществлять или обеспечивать осуществление блокирования или уничтожения персональных данных в сроки, указанные в настоящем Положении;

- в случае достижения цели обработки персональных данных осуществлять или обеспечивать осуществление уничтожения персональных данных в сроки, указанные в настоящем Положении;

- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных;

- в случае достижения цели обработки персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Положением или федеральными законами;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если это предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных продолжить обработку персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Положением или федеральными законами;

- в случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в настоящем Положении, осуществить блокирование таких персональных данных и обеспечить уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;

- осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, указанных в настоящем Положении.

Кроме указанных прав в вопросах обработки персональных данных субъектов персональных данных Общество обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

Общество при обработке персональных данных субъектов персональных данных обязано:

- строго соблюдать принципы обработки персональных данных, указанные в настоящем Положении;

- в случае если, обработка персональных данных осуществляется по поручению оператора, строго соблюдать и выполнять требования поручения оператора;

- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов исключить из общедоступных источников персональных данных сведения о субъекте персональных данных;

- обеспечить конкретность и информированность согласия на обработку персональных данных;

- получать согласие на обработку персональных данных в форме, указанной в настоящем Положении;

- в случае получения согласия на обработку персональных данных от представителя субъекта персональных данных проверять полномочия данного представителя на дачу согласия от имени субъекта персональных данных;

- предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований обработки персональных данных без получения согласия;

- строго соблюдать требования к содержанию согласия в письменной форме субъекта персональных данных на обработку его персональных данных в соответствии с настоящим Положением;

- незамедлительно прекратить обработку специальных категорий персональных данных если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом;

- предоставить субъекту персональных данных сведения по запросу субъекта персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;

- мотивировать и представить доказательства обоснованности отказа в выполнении повторного запроса субъекта персональных данных;

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

- рассмотреть возражение против принятия решения на основании исключительно автоматизированной обработки его персональных данных в течение срока, указанного в настоящем Положении и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;

- предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных;

- разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом;

- до начала обработки персональных данных, полученных не от субъекта персональных данных, предоставить субъекту персональных данных информацию о своем наименовании и адресе, цели обработки персональных данных и ее правовом основании, предполагаемых пользователей персональных данных, установленные права субъекта персональных данных, источник получения персональных данных;

- принимать меры, необходимые и достаточные для обеспечения выполнения своих обязанностей в области персональных данных, если иное не предусмотрено федеральными законами;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

- по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, определяющие политику в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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;

- сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо при получении запроса субъекта персональных данных или его представителя;

- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя дать в письменной форме мотивированный ответ;

- предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

- внести в персональные данные необходимые изменения или уничтожить такие персональные данные в случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными;

- строго соблюдать сроки по уведомлениям, блокированию и уничтожению персональных данных в соответствии с настоящим Положением;

- уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;

- 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 оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;

- в случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

- уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снять блокирование персональных данных в случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов;

- прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора;

- уничтожить персональные данные или обеспечить их уничтожение в случае, если обеспечить правомерность обработки персональных данных невозможно;

- уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган об устранении допущенных нарушений или об уничтожении персональных данных;

- прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае достижения цели обработки персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Положением или федеральными законами;

- прекратить обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если обработка персональных данных осуществляется без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Положением или федеральными законами;

- уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных в соответствии с настоящим Положением;

- уведомить уполномоченный орган по защите прав субъектов персональных данных в случае изменения сведений, указанных в уведомлении о своем намерении осуществлять обработку персональных данных;

- назначить лицо, ответственное за организацию обработки персональных данных;

- предоставлять лицу, ответственному за организацию обработки персональных данных, необходимые сведения, указанные в настоящем Положении;

- неукоснительно соблюдать все требования настоящего Положения;

- ознакомить работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучить таких сотрудников.

Кроме указанных обязанностей в вопросах обработки персональных данных субъектов персональных данных на Общество налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

3.9. Меры, направленные на обеспечение выполнения Обществом своих обязанностей

Общество принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных. Общество определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения указанных обязанностей, в том числе:

- назначает ответственного за организацию обработки персональных данных в Обществе из числа сотрудников Общества;

- разрабатывает и утверждает должностную инструкцию ответственного за организацию обработки персональных данных в Обществе;

- назначает ответственных за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества;

- разрабатывает и утверждает должностную инструкцию ответственных за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества
- создает комиссию, в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям.

Издает и утверждает приказом генерального директора Общества Положение по защите персональных данных в Обществе (настоящее Положение), включающее в себя:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных и локальным актам Общества;
- правила работы с обезличенными данными;
- типовую форму согласия на обработку персональных данных субъектов персональных данных;
- типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- оценку вреда, который может быть причинен субъектам персональных данных в случае в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- издает и утверждает актом генерального директора Общества документ, определяющий соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области персональных данных;
- издает и утверждает актом директора Общества перечень программного обеспечения, используемого при обработке персональных данных в информационных системах Общества;
- перечень должностей работников Общества, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- перечень должностей работников Общества, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- типовое обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;
- порядок доступа работников Общества в помещения, в которых ведется обработка персональных данных в соответствие со списком;
- принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные законодательством Российской Федерации в области персональных данных;
- осуществляют ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных работников;
- уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных.

3.10. Права и обязанности субъекта персональных данных

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

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения Общества, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании законодательства;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных.

Право субъекта персональных данных на доступ к его персональным данным ограничивается в соответствии с частью 8 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

Субъект персональных данных вправе требовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, указанные в пункте 8.1. раздела 8 Правил, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Субъект персональных данных обязан:

- передавать Обществу комплекс достоверных, документированных персональных данных, состав которых установлен законодательством;
- своевременно сообщать уполномоченным Обществом лицам на получение, обработку, хранение, передачу и любое другое использование персональных данных об изменении своих персональных данных.

В целях защиты частной жизни, личной и семейной тайны субъекты персональных данных не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

3.11. Ответственность лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных

Лица, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных, виновные в нарушении требований законодательства о защите персональных данных, в том числе допустившие разглашение персональных данных, несут персональную гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством ответственность.

Текущий контроль за соблюдением требований законодательства при обработке персональных данных осуществляется Обществом путем проведения проверок по соблюдению и исполнению законодательства о персональных данных.

Проверки выполнения требований законодательства при обработке персональных данных проводятся в соответствии с Порядком осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленными Обществом.

3.12. Меры, принимаемые для защиты персональных данных

Общество 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 принимает следующие меры:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных и уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

При обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных при выполнении заявленных в Положении о защите персональных данных Общества основных полномочий и прав Общества, либо в рамках перечня задач или функций структурных подразделений (должностных лиц) Общества, указанных в положениях о таких структурных подразделениях (должностных обязанностях) с учетом особых Положений и способов обработки персональных данных.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения 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, а также определения соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

Обработка персональных данных без оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных не допускается.

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных документально оформляется в порядке, установленном настоящим Положением.

5. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в Обществе.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных, для каждой информационной системы персональных данных Общества производится экспертное сравнение заявленной Обществом в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и применяемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и изложенных в настоящем Положении.

По итогам сравнений принимается решение о достаточности применяемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного в Обществе порядка обработки и обеспечения безопасности персональных данных.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных в Обществе оформляется в виде отдельного документа, подписывается лицом, ответственным за организацию обработки персональных данных в Обществе либо председателем комиссии, образуемой генеральным директором Общества, и утверждается генеральным директором Общества.

По результатам принятых решений, лицом, ответственным за организацию обработки персональных данных в Обществе организуется работа по их реализации

6. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных

Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в Обществе состоит из следующих направлений:

- внешний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных;
- внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных.

Внутренний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности персональных данных в Обществе состоит из:

- контроля и надзора за исполнением требований по обработке и обеспечению безопасности персональных данных;
- оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер.

6.1. Порядок внешнего контроля над соблюдением требований по обработке и обеспечению безопасности данных

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Внешний контроль и надзор за выполнением требований законодательства в области персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации в области защиты прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, подзаконных нормативных актов Правительства Российской Федерации, ведомственных нормативных актов и административных регламентов.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Уполномоченный орган по защите прав субъектов персональных данных имеет право:

- запрашивать у Общества информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных Общества, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от Общества уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства в области персональных данных;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;
- направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, необходимые сведения;
- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
- привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

6.2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных в Обществе либо комиссией, образуемой генеральным директором Общества не реже одного раза в год.

При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе производится проверка:

- соблюдения принципов обработки персональных данных в Обществе;
- соответствия локальных актов в области персональных данных Обществе действующему законодательству Российской Федерации;
- выполнения работниками Общества требований и Положений (в том числе особых) обработки персональных данных в информационных системах персональных данных Общества;
- перечней персональных данных, используемых для решения задач и функций структурными подразделениями Общества и необходимости обработки персональных данных в информационных системах персональных данных Общества;
- актуальности содержащихся в Правилах обработки персональных данных в каждой информационной системе персональных данных Общества информации о законности целей обработки персональных данных и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;
- правильность осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Общества;
- актуальность перечня должностей работников Общества, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- актуальность перечня должностей работников Общества, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Общества;
- соблюдение обязанностей работников Общества, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Общества и, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов

персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

- наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Общества;
- актуальность сведений, содержащихся в уведомлении Общества об обработке персональных данных;
- актуальность перечня информационных систем персональных данных в Обществе;
- наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Общества;
- знания и соблюдение работниками Общества положений действующего законодательства Российской Федерации в области персональных данных;
- знания и соблюдение работниками Общества положений локальных актов Общества в области обработки и обеспечения безопасности персональных данных;
- знания и соблюдение работниками Общества инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдение работниками Общества конфиденциальности персональных данных;
- актуальность локальных актов Общества в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;
- соблюдение работниками Общества требований по обеспечению безопасности персональных данных;
- наличие локальных актов Общества, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных Общества;
- иных вопросов.

Результаты внутреннего контроля оформляются ответственным лицом в виде отдельного документа и подписываются директором.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, генеральному директору Общества докладывает ответственный за организацию обработки персональных данных в Обществе либо председатель комиссии.

7. Правила взаимодействия с субъектами персональных данных и иными лицами

Настоящее Положение при определении порядка взаимодействия Общества с субъектами персональных данных устанавливает:

- сроки выполнения действий по защите прав субъектов персональных данных;
- требования по уведомлениям/предоставлению информации субъектов персональных данных и в иных случаях;
- требования к лицам, ответственным за организацию обработки персональных данных;
- порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав;
- порядок реагирования на обращения субъектов персональных данных;
- порядок действий при обращениях субъектов персональных данных;
- требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных;
- порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных;
- порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации;

- действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;

порядок реализации права субъекта персональных данных на обжалование действий или бездействия Общества;

- порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных;
- порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных.

7.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных

В Обществе устанавливаются следующие сроки по защите прав субъектов персональных данных:

- в случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Общество или направить ему повторный запрос в целях получения таких сведений, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо поручителем по которому является субъект персональных данных;
- в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Общество обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;
- в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Общество обязано внести в них необходимые изменения;
- в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Общество обязано уничтожить такие персональные данные;
- в случае выявления неправомерной обработки персональных данных, осуществляемой Обществом или лицом, действующим по его поручению, Общество в срок, трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по его поручению;
- в случае если обеспечить правомерность обработки персональных данных невозможно, Общество в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение;
- в случае достижения цели обработки персональных данных Общество обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами;

- в случае отсутствия возможности уничтожения персональных данных в течение указанных сроков, Общество осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;

- Общество обязано рассмотреть возражение субъекта персональных данных о принятии на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;

- Общество обязано сообщить в установленном порядке, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;

- Общество обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса;

- в случае подтверждения факта неточности персональных данных Общество на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных;

- в случае изменения сведений, указных в уведомлении об обработке персональных данных, а также в случае прекращения обработки персональных данных Общество обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Установленные сроки обязательны к исполнению всеми должностными лицами Общества.

7.2. Требования по уведомлениям (предоставлению информации, разъяснениям) субъектов персональных данных и в иных случаях

Общество обязано осуществлять уведомления и предоставлять информацию в следующих случаях:

- Общество обязано разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

- Общество обязано рассмотреть возражение субъекта персональных данных о принятии на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении него или иным образом затрагивающих его права и законные интересы, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;

- если предоставление персональных данных является обязательным в соответствии с федеральным законом, Общество обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

- Общество обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

- Общество обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринять мерах в случаях, когда персональные данные являются неполными, неточными или неактуальными и персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- об устранении допущенных нарушений или об уничтожении персональных данных в случае выявления неправомерной обработки персональных данных Общество обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;

- Общество до начала обработки персональных данных обязано уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных;

- в случае изменения сведений, а также в случае прекращения обработки персональных данных Общество обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных;

- обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия иных законных оснований возлагается на оператора;

- персональные данные могут быть получены Обществом от лица, не являющегося субъектом персональных данных, при условии предоставления им подтверждения наличия законных оснований обработки, в том числе передачи таких персональных данных;

- Обществом должны быть предоставлены субъекту персональных данных запрашиваемые им сведения в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;

- сведения, запрашиваемые субъектом персональных данных, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя;

- обязанность представления доказательств обоснованности мотивированного отказа в выполнении повторного запроса субъекта персональных данных лежит на Обществе;

- Общество обязано разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

- при сборе персональных данных Общество обязано по просьбе субъекта персональных данных предоставить информацию, касающуюся обработки его персональных данных;

- если персональные данные получены не от субъекта персональных данных, Общество, до начала обработки таких персональных данных обязано предоставить субъекту персональных данных информацию, касающуюся обработки его персональных данных;

- Общество по запросу уполномоченного органа по защите прав субъектов персональных данных обязано представить документы и локальные акты, и (или) иным образом подтвердить принятие мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных действующим законодательством в области персональных данных;

- Общество обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя;

- Общество обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных;

- Общество обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах в случае выявления того, что персональные данные являются неполными, неточными или неактуальными, или являются незаконно полученными или не являются необходимыми для заявленной цели обработки и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

- Общество обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию;

- Общество обязано предоставлять лицу, ответственному за организацию обработки персональных данных в Обществе сведения, предусмотренные действующим законодательством в области персональных данных.

Общество освобождается от обязанности предоставить субъекту персональных данных сведения об обрабатываемых персональных данных, относящихся к субъекту персональных данных, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Обществом;

- персональные данные получены Обществом на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому 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;

- предоставление субъекту персональных данных нарушает права и законные интересы третьих лиц.

Уведомление в указанных случаях готовится лицом, ответственным за организацию обработки персональных данных в Обществе. Подготовленное уведомление утверждается генеральным директором Общества Отправка уведомления осуществляется лицом, ответственным за организацию обработки персональных данных в Обществе в установленные сроки.

Требования к уведомлению уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных и об изменении поданных сведений устанавливаются настоящими Положением.

7.3. Лица, ответственные за организацию обработки персональных данных

В Обществе из числа работников Общества назначается лицо, ответственное за организацию обработки персональных данных в Обществе. Лицо, ответственное за организацию обработки персональных данных в Обществе, получает указания непосредственно от генерального директора Общества, и подотчетно ему.

Общество предоставляет лицу, ответственному за организацию обработки персональных данных сведения об обработке персональных данных в Обществе, в соответствии с требованиями действующего законодательства в области персональных данных.

В Обществе разрабатывается должностная инструкция ответственного за организацию обработки персональных данных в Обществе.

Основными обязанностями лица, ответственного за организацию обработки персональных данных в Обществе являются:

- осуществление внутреннего контроля за соблюдением Общества и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения сотрудников Общества положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

7.3.1. Должностная инструкция ответственного за организацию обработки персональных данных в Обществе

Общие положения

Ответственный за организацию обработки персональных данных назначается приказом генерального директора Общества на основании Федерального Закона «О персональных данных» №152-ФЗ от 27 июля 2006 года.

Ответственный за организацию обработки персональных данных проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю Российской Федерации, Федеральной службы безопасности Российской Федерации и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

Непосредственное руководство работой ответственного за организацию обработки персональных данных осуществляет директор Общества.

Ответственный за организацию обработки персональных данных назначается из числа заместителей генерального директора Общества, который по основной деятельности курирует вопросы кадровой работы и информатизации.

В своей работе ответственный за организацию обработки персональных данных руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и нормативными правовыми актами Общества по обеспечению безопасности персональных данных.

Основные функции

На ответственного за организацию обработки персональных данных в Обществе возлагаются следующие основные функции:

- проведение единой технической политики Общества и координация работ по организации обработки и обеспечению безопасности персональных данных;
- планирование мероприятий по организации обеспечения безопасности персональных данных;
- организация мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- организация мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передача их лицам, не имеющим права доступа к такой информации;
- организация контроля обеспечения уровня защищенности персональных данных;
- координация действий по подготовке объектов Общества к аттестации по выполнению требований обеспечения безопасности персональных данных;
- контроль исполнения организационных распорядительных документов по организации обработки и обеспечению безопасности персональных данных в Обществе;
- организация проведения периодического контроля эффективности мер защиты персональных данных в Обществе. Анализ результатов контроля;

- рассмотрение предложений по устранению недостатков и предупреждению нарушений при обеспечении безопасности персональных данных, осуществление контроля устранения нарушений;
- рассмотрение и утверждение предложений по совершенствованию системы безопасности персональных данных в Обществе;
- осуществление непосредственного контроля соблюдения установленного законодательством порядка рассмотрения запросов субъектов персональных данных;
- организация повышения квалификации сотрудников в области защиты персональных данных;
- изучение отчетов о состоянии работ по обеспечению безопасности персональных данных в Обществе.

Права

Должностное лицо Общества, ответственное за организацию обработки персональных данных имеет право:

- запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.
- осуществлять контроль за реализацией организационных и распорядительных документов по организации обработки и обеспечению безопасности персональных данных.
- рассматривать предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на соответствующие виды деятельности.
- контролировать деятельность работников любого структурного подразделения Общества в части выполнения ими требований по обеспечению безопасности персональных данных.
- принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.
- привлекать в установленном порядке необходимых специалистов из числа работников Общества для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

Ответственность

Ответственный за организацию обработки персональных данных несет персональную ответственность за:

- правильность и объективность принимаемых решений;
- правильное и своевременное выполнение организационных и распорядительных документов, принятых Обществом по вопросам обработки и защиты персональных данных;
- выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;
- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;

соблюдение трудовой дисциплины, охраны труда.

7.3.2. Должностная инструкция ответственного за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества

Общие положения

Настоящая должностная инструкция по обеспечению безопасности персональных данных (далее - Инструкция) определяет основные цели, функции и права должностного лица Общества, ответственного за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества (далее - Ответственный за защиту).

Ответственный за защиту назначается приказом генерального директора Общества на основании Федерального Закона «О персональных данных» № 152-ФЗ от 27 июля 2006 года.

Ответственный за защиту проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю Российской Федерации, Федеральной службы безопасности Российской Федерации и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

Непосредственное руководство работой Ответственного за защиту осуществляет работник Общества, курирующий вопросы защиты информации, ответственный за организацию обработки персональных данных.

Ответственный за защиту назначается из числа работников Общества, имеющих опыт работы по основной деятельности в области защиты персональных данных.

Работа Ответственного за защиту проводится в соответствии с планом работ по защите персональных данных.

В своей работе Ответственный за защиту руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и нормативными правовыми актами Общества по обеспечению безопасности персональных данных.

Основные функции

На Ответственного за защиту возлагаются следующие основные функции:

- готовить и направлять первичное уведомление об обработке персональных данных, а также в случае изменения сведений, указанных в Уведомлении (ч.3 ст. 22 Федерального Закона №152-ФЗ от 27.07.2006 «О персональных данных») или в случае прекращения обработки персональных данных в орган по защите прав субъектов персональных данных (Управление Роскомнадзора по Уральскому федеральному округу);
- предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой их обращений и запросов. Форма журнала регистрации и учета обращений и запросов субъектов персональных данных приведена в Приложении № 24;
- получать обязательство от работников Общества, имеющих доступ к персональным данным, в случае расторжения с ними государственного контракта, о прекращении обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей;
- получать согласие на обработку персональных данных у субъекта персональных данных;
- разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных.
- проводить мероприятия по организации обеспечения безопасности персональных данных, включая классификацию систем персональных данных;
- проводить мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:

1. Мероприятия по охране, организации доступа в помещения, где ведется обработка персональных данных.
2. Мероприятия по закрытию технических каналов утечки персональных данных при их обработке.
3. Мероприятия по защите от несанкционированного доступа к персональным данным.
4. Мероприятия по выбору средств защиты персональных данных при их обработке.

- проводить мероприятия, направленных на предотвращение передачи персональных данных лицам, не имеющим права доступа к такой информации.
- не допускать воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных;

- участие в подготовке объектов Общества к аттестации по выполнению требований обеспечения безопасности персональных данных.
- разработка организационных распорядительных документов по обеспечению безопасности персональных данных в Обществе;
- проведение периодического контроля эффективности мер защиты персональных данных в Обществе. Учет и анализ результатов контроля;
- организация в установленном порядке изучения причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений;
- разработка предложений и участие в проводимых работах по совершенствованию системы безопасности персональных данных в Обществе;
- ознакомление работников Общества с законодательством в области обработки и защиты персональных данных, а также с локальными нормативными правовыми Общества по данному вопросу;
- оказание методической помощи по вопросам обеспечения безопасности персональных данных работниками Общества;
- подготовка отчетов о состоянии работ по обеспечению безопасности персональных данных в Обществе.

Права

Ответственный за защиту имеет право:

- запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных;
- разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных;
- готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на соответствующие виды деятельности;
- вносить предложения ответственному за организацию обработки персональных данных Общества о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных;
- пользоваться необходимой помощью работников из числа работников Общества для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

Ответственность

Ответственный за защиту несет персональную ответственность за:

- правильность и объективность принимаемых решений;
- правильное и своевременное выполнение распоряжений и указаний ответственного за организацию обработки персональных данных Общества, ответственного за организацию обработки персональных данных по вопросам, входящим в возложенные на него функции;
- правильное и своевременное выполнение организационных и распорядительных документов, принятых Обществом по вопросам обработки и защиты персональных данных;
- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;
- согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы;
- соблюдение трудовой дисциплины, охраны труда.

7.4. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав

Сотрудники Общества обязаны разъяснять субъектам персональных данных особенности обработки персональных данных и порядок защиты их прав в следующих случаях:

- при принятии решения на основании исключительно автоматизированной обработки его персональных данных - разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных, возможные юридические последствия такого решения, а также порядок защиты субъектом персональных данных своих прав и законных интересов;
- если предоставление персональных данных является обязательным в соответствии с федеральным законом - разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Разъяснение субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав осуществляется работниками Общества, осуществляющими непосредственные операции по обработке персональных данных или лицом, ответственным за организацию обработки персональных данных в Обществе.

Разъяснения осуществляются на основании настоящего Положения и действующего законодательства Российской Федерации в области персональных данных.

Для разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав используются официальный сайт Общества, стенды, раздаточный материал.

7.5. Порядок действий при обращениях субъектов персональных данных

Если обращения субъектов персональных данных принимаются в письменном виде, то они подлежат учету, наряду с остальными входящими документами.

С целью соблюдения сроков по реагированию на обращения субъектов персональных данных они должны незамедлительно передаваться лицу, ответственному за организацию обработки персональных данных в Обществе.

Ответы на обращения, не отвечающие требованиям, предъявляемым к ним действующим законодательством в области персональных данных, не производятся.

Передача ответов субъекту персональных данных осуществляется требуемым им способом, или, если такой способ не указан, посредством отправки заказного письма с уведомлением.

Передача ответов на обращения субъектов персональных данных осуществляется в установленном в Обществе для исходящей корреспонденции порядке с соблюдением указанных в настоящем Положении сроков.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, при личном обращении в Общество, либо путем направления запроса, в том числе в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации.

Письменный запрос субъекта персональных данных на получение информации, касающейся обработки его персональных данных Обществом должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе с указанием кода подразделения;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом;
- подпись субъекта персональных данных или его представителя.

Письменные запросы, не отвечающие указанным требованиям, обработке не подлежат.

При личном обращении в Общество субъект персональных данных обязан предъявить документ, удостоверяющий его личность, а его представитель - документ, удостоверяющий личность представителя и документы, подтверждающие полномочия этого представителя, и сообщить сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом.

Данные предоставляемые субъектом персональных данных при личном обращении в Общество фиксируется в Журнале учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана.

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в следующих случаях если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

В случае отказа в предоставлении субъекту персональных данных при обращении информации, касающейся обработки его персональных данных Обществом, либо при получении запроса субъекта персональных данных о такой информации, работники, ответственные за обеспечение безопасности персональных данных в информационных системах Общества, составляют в письменной форме мотивированный ответ, содержащий ссылку на пункты или статьи федерального закона, являющегося основанием для такого отказа.

Предоставление доступа к своим персональным данным в случае непосредственного обращения субъекта персональных данных осуществляется по адресу: город Екатеринбург, ул. Посадская, Д.28А. Доступ субъекта персональных данных в этом случае осуществляется в порядке, установленном в настоящем Положении.

Субъект персональных данных имеет право на получение при обращении или при подаче запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Обществом;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Обществом способы обработки персональных данных;
- наименование и место нахождения Общества, сведения о лицах (в том числе о сотрудниках Общества в объеме, предусмотренном настоящим Положением), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством в области персональных данных;
- наименование или фамилию, имя, отчество лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством в области персональных данных или другими федеральными законами.

Ответ на обращения и запросы субъектов персональных данных готовится лицом, ответственным за организацию обработки персональных данных в Обществе, по существу такого обращения в двух экземплярах. Запрашиваемые сведения предоставляются в соответствии с настоящим Положением, Положениями об обработке персональных данных в конкретных информационных системах персональных данных Общества и действующего законодательства Российской Федерации в области персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Форма ответа на обращение или запрос субъекта персональных данных не должна противоречить установленным в Обществе требованиям по защите информации и обеспечению безопасности персональных данных.

Хранение информации об обращении или запрос субъекта персональных данных, а также второй экземпляр ответа на такое обращение или запрос, хранятся в соответствии с установленным в Обществе порядком.

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, Общество осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Общество осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных: данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Общество на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и снимает блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой Обществом или лицом, действующим по поручению оператора, Общество прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Общества.

В случае если обеспечить правомерность обработки персональных данных невозможно, Общество уничтожает такие персональные данные или обеспечивает их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

При совершении указанных действий должны соблюдаться сроки, установленные в настоящем Положении.

При обнаружении нарушений Положение обработки или обеспечения безопасности персональных данных лицо, ответственное за организацию обработки персональных данных в Обществе незамедлительно принимает меры по устранению таких нарушений и минимизации их последствий. При этом должен проводиться анализ таких нарушений и приниматься меры по их недопущению в дальнейшем.

В случае если произошло нарушение прав субъекта персональных данных и данное нарушение может повлиять на нарушение прав такого субъекта в дальнейшем, Общество организует оповещение этого субъекта о возможных последствиях выявленных нарушений и принятых по ним мерам. Порядок такого оповещения устанавливается в каждой конкретной ситуации лицом, ответственным за обеспечение безопасности персональных данных в Обществе.

Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства в области персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в установленном законодательством Российской Федерации судебном порядке.

7.6. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных

В случае достижения цели обработки персональных данных Общество обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества).

При совершении указанных действий должны соблюдаться сроки, установленные в настоящем Положении.

7.7. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества).

При совершении указанных действий должны соблюдаться сроки, установленные в настоящем Положении.

8. Правила обработки персональных данных в информационных системах персональных данных

Обработка персональных данных в информационных системах персональных данных Общества может осуществляться следующими способами:

– обработка персональных данных без использования средств автоматизации;

– обработка персональных данных с использованием средств автоматизации;

– исключительно автоматизированная обработка персональных данных;

– смешенная обработка персональных данных.

8.1. Обработка персональных данных без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков) используемых в обществе.

Для обработки различных категорий персональных данных, осуществляемой без использования средств информатизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности, при необходимости использования или распространения определенных

персональных данных отдельно от находящихся на том же материальном носителе других персональных данных, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

1) Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации,
- 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.

2) Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных.

3) 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.

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

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, -путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

8.2. Обработка персональных данных с использованием средств автоматизации

Обработка персональных данных средствами автоматизации в Обществе допускается только в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка персональных данных средствами автоматизации должна осуществляться на основании настоящего Положения, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащих такие данные, определенные для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящего Положения.

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 Положении.

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.

Согласие на обработку персональных данных Обществу 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.

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

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) материальных носителей персональных данных и в договоры с субъектами персональных данных.

Письменные согласия субъектов персональных данных должны храниться в Обществе.

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

Обработка персональных данных без согласия субъекта персональных данных

Обработка персональных данных, осуществляемая без получения согласия на такую обработку от субъекта персональных данных может осуществляться только по основаниям, указанным в настоящем Положении, при этом обязанность предоставить доказательство наличия таких оснований возлагается на Общество.

Порядок определения оснований обработки персональных данных без согласия на обработку персональных данных от субъекта персональных данных, их определения, оформления и предоставления приведен в настоящем Положении.

8.2.1. Исключительно автоматизированная обработка персональных данных

При исключительно автоматизированной обработке персональных данных должны выполняться требования по обработке персональных данных средствами автоматизации.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы запрещается.

При исключительно автоматизированной обработке персональных данных необходимо:

- разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных;
- разъяснить возможные юридические последствия такого решения;
- предоставить возможность заявить возражение против такого решения;
- рассмотреть возражение;
- уведомить субъекта персональных данных о результатах рассмотрения такого возражения в порядке и в сроки, предусмотренные настоящим Положением.

8.2.2. Обработка персональных данных средствами автоматизации при поручении обработки персональных данных

Обработка персональных данных средствами автоматизации при поручении обработки персональных данных другому лицу.

Общество вправе поручить обработку персональных данных другому лицу (поручение оператора):

- с согласия субъекта персональных данных;
- если иное не предусмотрено федеральным законом;
- на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта;
- либо путем принятия соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать Положение об обработке персональных данных. В поручении оператора:

- должен быть определен перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- должны быть определены цели обработки персональных данных;
- должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных;
- должна быть установлена обязанность такого лица обеспечивать безопасность персональных данных при их обработке;

- должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с настоящим Положением и техническим заданием (или техническим проектом) на создание системы защиты персональных данных;
- установлена ответственность такого лица перед Обществом, в случаях нарушений установленных требований и законодательства Российской Федерации в области персональных данных;
- при необходимости получения согласий на обработку персональных данных от субъектов персональных данных, предусмотрен порядок сбора и передачи в Общество таких согласий субъектов персональных данных.

В случае если Общество поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Общество.

В случае необходимости получения согласия на обработку персональных данных от субъекта персональных данных обязанность получения таких согласий возлагается на Общество.

8.2.3. Обработка персональных данных средствами автоматизации при поручении обработки персональных данных другим лицом

В случае поручения обработки персональных данных средствами автоматизации Обществу другим лицом, такое лицо своим поручением оператору обязано:

- определить перечень действий (операций) с персональными данными, которые будут совершаться Обществом при осуществлении обработки персональных данных;
- определить цели обработки персональных данных;
- указать требования к защите обрабатываемых персональных данных.

В случае не определения такой информации и требований другим лицом, Общество обязано добиться их определения и документального оформления.

В случае принятия поручения оператора от другого лица Обществом без указанной информации и требований, такая обработка не считается обработкой, осуществляемой по поручению оператора и Общество будет являться оператором персональных данных. При этом обработка персональных данных должна выполняться в соответствии с настоящим Положением.

Общество обязано выполнить все требования, установленные другим лицом в поручении оператора и за все нарушения в обработке персональных данных, несет ответственность перед таким лицом.

Общество при осуществлении обработки персональных данных по поручению оператора не обязан получать согласие субъекта персональных данных на обработку его персональных данных.

8.3. Смешенная обработка персональных данных

При смешенной обработке персональных данных необходимо выполнять требования, объединяющие требования обработки персональных данных при их обработке каждым из используемых при смешенной обработке персональных данных способов.

9. Мероприятия по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящем Положении.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящим Положением.

9.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места

хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка , которых осуществляется в различных целях.

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

Ответственным за организацию и контроль за обеспечением безопасности персональных данных в информационных системах общества при обработке персональных данных, осуществляемой без использования средств автоматизации, является лицо, ответственное за обеспечение безопасности персональных данных в соответствующих информационных системах.

9.2. Состав и содержание мер по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

Персональные данные в Обществе обрабатываются в информационных системах обработки персональных данных.

В информационных системах обработки персональных данных определяются следующие показатели информационной системы:

- категория обрабатываемых персональных данных

- тип угрозы, актуальной для информационной системы;

- объем обрабатываемых персональных данных субъектов, не являющихся сотрудниками оператора, или являющихся таковыми.

В зависимости от показателей информационной системы определяется уровень защищенности персональных данных при их обработке в информационной системе.

Состав и содержание мер по обеспечению безопасности персональных данных определяется исходя из уровня защищенности персональных данных.

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

- определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных;

- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы;

- уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер. В результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

- дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

9.3. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств персональных данных

Безопасность обработки персональных данных с использованием криптосредств организуется и обеспечивается Обществом.

Обеспечение безопасности персональных данных с использованием криптосредств осуществляется в соответствии с:

1. Приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);

2. Постановлением Правительства РФ от 16 апреля 2012 г. N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)";

3. Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/5-144, 2008 г. ФСБ России);

4. Настоящим Положением.

При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационных системах Общество (с возможным привлечением экспертов) осуществляет:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) неправомерных действий при их обработке;
- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;
- обучение лиц, использующих криптосредства, работе с ними;
- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);
- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности

персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

- описание организационных и технических мер, которые Общество обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах.

Пользователи криптосредств допускаются к работе с ними по решению, утверждаемому Обществом в соответствии с документально оформленным списком. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы. В обществе обязательно ведется журнал учета пользователей криптосредств. Учет выданных и уничтоженных ключей шифрования и электронной подписи ведется в журнале по форме.

Лица, оформляемые на работу в качестве пользователей (ответственных пользователей) криптосредств, должны быть ознакомлены с настоящими обязанностями, а также с типовой инструкцией «О порядке изготовления, учета, хранения и уничтожения ключей шифрования и электронной подписи и действий работников Общества в случае компрометации ключевой информации.

Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Форма такого учета приведена в Приложении № 8. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражаются также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей.

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожают путем сжигания или с помощью любых бумагорезательных машин.

10. Правила работы с обезличенными персональными данными, обрабатываемыми в Обществе

Обезличивание персональных данных в Обществе проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных.

Способами обезличивания персональных данных при условии их дальнейшей обработке являются:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Перечень должностей работников Общества, ответственных за проведение мероприятий по обезличиванию персональных данных (далее - Перечень должностей), приведен в Приложении № 19.

В соответствии с Перечнем должностей:

- директор Общества принимает решение о необходимости обезличивания персональных данных;
- ответственные за обеспечение безопасности персональных данных в информационных системах общества готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;
- работники, осуществляющие обработку персональных данных в связи с реализацией трудовых отношений, совместно с ответственным за организацию обработки персональных данных в связи с реализацией трудовых отношений, осуществляют непосредственное обезличивание персональных данных;

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные обрабатываются с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

11. Политика Общества в отношении обработки персональных данных и **реализации требований к защите персональных данных**

Настоящий документ определяет Политику Общества в отношении обработки персональных данных и реализации требований к защите персональных данных (далее - Политика) в соответствии с требованиями ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В настоящей Политике используются следующие основные понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

- оператор - юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

- 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.

1. Принципы обработки персональных данных в Обществе:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается 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 из обработки;
- содержание и объем обрабатываемых персональных данных соответствую заявленным целям обработки и не являются избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целя обработки персональных данных. Принимаются необходимые меры по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных 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, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, подлежат уничтожению либо обезличиванию.

2. Правовые основания обработки персональных данных.

Обработка персональных данных в Обществе осуществляется в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Трудовым кодексом Российской Федерации, Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 6 июля 2008 г. №512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

3. Цели обработки персональных данных.

Обработка персональных данных в Обществе осуществляется в целях исполнения функций в связи с реализацией трудовых отношений и в связи с оказанием услуг населению в сфере жилищно - коммунального хозяйства:

в области персональных данных, в целях рассмотрения обращений граждан, а также в целях ведения кадровой работы.

4. Состав и субъекты персональных данных.

В Обществе обрабатываются персональные данные:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- ИНН;
- СНИЛС;
- реквизиты документа, удостоверяющего личность (кем выдан, дата выдачи, код подразделения, срок действия);
- контактные телефоны (домашний и рабочий);

- адрес по прописке (с указанием даты регистрации);
- адрес места проживания;
- адрес для информирования (почтовый адрес)
- общие сведения о заработной плате в соответствии со штатным расписанием;
- сведения об образовании;
- сведения о повышении квалификации и переподготовке;
- сведения о воинском учете и бронировании;
- сведения об отсутствии/наличии инвалидности и/или проф. заболевании;
- сведения о начислениях (удержаниях) заработной платы (на текущую дату или за период);
- иные сведения (банковский счет и т.д.).
- сведения о начислениях и поступлениях денежных средств на лицевые счета собственников и нанимателей за ЖКУ и прочие услуги;
- сведения о нанимателе жилого помещения, ордере решении жилищной комиссии, решении суда (номер, дата выдачи, кем выдан);
- сведения о собственнике жилого помещения, доли собственности (серия, номер, дата выдачи, кем выдан).

5. Обработка персональных данных.

Обработка персональных данных осуществляется Обществом с использованием средств автоматизации, а также без использования таких средств (на бумажном носителе информации).

Общество не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных без его согласия могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;
- в органы федеральной службы безопасности;
- в органы прокуратуры;
- в органы полиции;
- в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

Сроки хранения носителей персональных данных определены Номенклатурой Общества. Порядок уничтожения носителей персональных данных установлен отдельным документом.

6. Конфиденциальность персональных данных.

Информация, относящаяся к персональным данным, ставшая известной в связи с реализацией трудовых отношений и в связи с оказанием услуг и осуществлением государственных функций, является конфиденциальной информацией и охраняется законом.

Работники Общества и иные лица, получившие доступ к обрабатываемым персональным данным предупреждены о возможной дисциплинарной, административной, гражданско-правовой и уголовной ответственности в случае нарушения норм и требований действующего законодательства Российской Федерации в области обработки персональных данных.

7. Права субъектов персональных данных.

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

- подтверждение факта обработки персональных данных Оператором;

- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников/работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- наименование или фамилию, имя, отчество лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в орган по защите прав субъектов персональных данных (Управление Роскомнадзора по Уральскому федеральному округу) или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Иные права, определенные главой 3 Федерального закона «О персональных данных». 8. Меры, направленные на обеспечение выполнения Обществом обязанностей, предусмотренных ст. ст. 18.1, 19 Федерального закона «О персональных данных»:

- назначен ответственный за организацию обработки персональных данных в Обществе;
- приказом генерального директора Общества утверждены «Положение о защите персональных данных в Обществе», другие локальные акты, устанавливающее процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- применяются предусмотренные соответствующими нормативными правовыми актами правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Общества.
- при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняются требования, установленные Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

- в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Обществе организовано проведение периодических проверок условий обработки персональных данных.

- осуществляется ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

- Общество несет ответственность за нарушение обязательств по обеспечению безопасности и конфиденциальности персональных данных при их обработке в соответствии с законодательством Российской Федерации.

- Общество включено в Реестр операторов персональных данных, приказ о включении от 06.05.2010 № 293, регистрационный № 10-0102254.

Настоящий документ определяет политику в отношении обработки персональных данных в Обществе и подлежит опубликованию на официальном сайте Общества в течение 10 дней после утверждения.

К указанному документу обеспечивается неограниченный доступ.

12. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.

Общество уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. При этом должны соблюдаться сроки подачи уведомлений (в соответствии со ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ).

Общество вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;
- полученных Обществом в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Обществом исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения и обрабатываемых соответствующими общественным объединением, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;
- сделанных субъектом персональных данных общедоступными, включающих в себя только фамилии, имена и отчества субъектов персональных данных;

необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится Общество, или в иных аналогичных целях;

обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Уведомление готовится лицом, ответственным за выполнение работ по обеспечению безопасности персональных данных в Обществе, подписывается генеральным директором Общества и направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;

- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер направленных на обеспечение выполнения обязанностей, предусмотренных законодательством в области персональных данных и по обеспечению безопасности персональных данных при их обработке;
- фамилия, имя, отчество физического лица, ответственного за организацию обработки персональных данных в Обществе, и номер его контактного телефона, почтовый адрес и адрес электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных.

Письменная форма уведомления устанавливается уполномоченным органом по защите прав субъектов персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения в реестр операторов.

Сведения, содержащиеся в реестре операторов, за исключением сведений о средства? обеспечения безопасности персональных данных при их обработке, являются общедоступными.

На Общество не могут возлагаться расходы в связи с рассмотрением уведомления о (обработке персональных данных уполномоченным органом по защите прав субъекта персональных данных, а также в связи с внесением сведений в реестр операторов.

В случае предоставления неполных или недостоверных сведений, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от Общества уточнения предоставленных сведений до их внесения в реестр операторов.

В случае изменения сведений, а также в случае прекращения обработки персональных данных Общество обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в сроки, указанные в настоящем Положении.

В случае изменения сведений, содержащихся в уведомлении об обработке персональных данных, структурное подразделение Общества, являющееся инициатором таких изменений в обработке персональных данных, готовит изменения в уведомление и передает такие изменения лицу, ответственному за организацию обработки персональных данных в Обществе. Дальнейшие действия по подготовке изменений в уведомление для передачи в уполномоченный орган по защите прав субъектов персональных данных осуществляются аналогично действиям при первоначальной подаче уведомления.

13. Мероприятия по защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

В информационных системах обработки персональных данных определяются следующие показатели информационной системы:

- категория обрабатываемых персональных данных;
- тип угрозы, актуальной для информационной системы;

- объем обрабатываемых персональных данных субъектов, не являющихся сотрудниками оператора, или являющихся таковыми.

В зависимости от показателей информационной системы определяется уровень защищенности персональных данных информационной системы.

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение генеральным директором Общества документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо *дт* нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке і информационных системах помимо выполнения требований, предусмотренных **дл5** обеспечения 4-го уровня защищенности персональных данных, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных для обеспечения 4-го и 3-го уровней защищенности персональных данных, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных для обеспечения 4-го, 3-го и 2-го уровней защищенности персональных данных, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Контроль за выполнением настоящих требований организуется и проводится Обществом (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые Обществом (уполномоченным лицом).

Так как для информационных систем Общества в ходе определения уровней защищенности определен уровень защищенности УЗ 3, то к защите персональных данных при их обработке должны предъявляться требования, предусмотренные для обеспечения 4-го и 3-го уровней защищенности персональных данных.

13.1. Порядок доступа работников Общества в помещения, в которых ведется обработка персональных данных и организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и обеспечения сохранности носителей персональных данных

В Обществе персональные данные работников и граждан хранятся:

- в бухгалтерии;

- в общем отделе;

- в Управлении по расчетам с населением.

Доступ работников Общества в помещения, в которых ведется обработка персональных данных, осуществляется по Спискам работников Общества, допущенных в помещения, в которых ведется обработка персональных данных. Такие списки готовятся и уточняются лицами, ответственными за выполнение работ по обеспечению безопасности персональных данных в информационных системах Общества и утверждаются директором.

3. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется работниками, указанными в Списках работников Общества, допущенных в помещения, в которых ведется обработка персональных данных. Пребывание таких посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии работников, указанных в Списках работников Общества, допущенных в помещения, в которых ведется обработка персональных данных.

Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.

Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

Бумажные носители персональных данных и электронные носители персональных данных (диски, USB носители) хранятся в шкафах, оборудованных замками.

Помещения, в которых ведется обработка персональных данных, запираются на ключ.

Вскрытие и закрытие помещений, в которых ведется обработка персональных данных, производится работниками Общества, имеющими право доступа в эти помещения.

Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании служебного дня работники Общества, имеющие право доступа в помещения, обязаны:

- убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флэш-карты) в шкафы, закрыть шкафы;

- отключить технические средства (кроме постоянно действующего оборудования) и электроприборы от сети, выключить освещение;

- закрыть окна, двери;

Перед открытием помещений, в которых ведется обработка персональных данных, работники Общества, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери и замка;

- открыть дверь и осмотреть помещение, проверить наличие и целостность замков на шкафах.

При обнаружении неисправности двери и запирающих устройств работники Общества обязаны:

- не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю;

- в присутствии не менее двух работников Общества, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

- составить акт о выявленных нарушениях и передать установленным порядком своему непосредственному руководителю.

Право самостоятельного входа в помещения, где обрабатываются персональных данные, имеют только работники Общества, непосредственно работающие в данной помещении.

Иные граждане имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников Общества, непосредственно работающих в данных помещениях.

При работе с информацией, содержащей персональные данные, двери помещений

должны быть всегда закрыты.

Присутствие лиц, не имеющих права доступа к персональным данным, должно быть

исключено.

Техническое обслуживание компьютерной техники, сопровождение программных средств, уборка помещений, в которых ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника Общества, работающего в данном помещении.

Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей структурных подразделений Общества, обрабатывающих персональные данные.

13.2. Порядок обеспечения сохранности носителей персональных данных в Обществе

Все носители информации, содержащие ПДн, а именно к ним могут относиться:

- жесткие диски, находящиеся в системных блоках серверов;
- жесткие диски, находящиеся во внешних RAID-массивах серверов;
- жесткие диски, находящиеся в системных блоках рабочих компьютеров пользователей ИСПДн;
- USB носители, находящиеся у пользователей ИСПДн Общества либо в архивах;
- CD-R, CD-RW, DVD-R и/или DVD-RW носители, находящиеся у пользователей ИСПДн Общества;
- CD-R, CD-RW, DVD-R и/или DVD-RW носители, находящиеся в архивах Общества,

должны быть учтены в «Журнале учета машинных носителей информации».

Страницы «Журнала учета машинных носителей информации» должны быть пронумерованы, журнал прошит, опечатан и учтен в системе документооборота Общества.

Ведение «Журнале учета машинных носителей информации» поручается работнику, исполняющему функции администратора информационной безопасности в Обществе.

Учетный номер носителя, содержащего ПДн, должен наноситься непосредственно на корпус носителя и быть нестираемым.

На рабочих местах пользователей ИСПДн Общества не должны находиться неучтенные носители.

Запрещается копирование ПДн пользователями ИСПДн Общества с целью их передачи другим сотрудникам или посторонним лицам.

Работник, получивший носитель для работы с ПДн, обязан обеспечить его недоступность для третьих лиц (посторонних лиц и работников, не имеющих допуск к ПДн).

Полученные извне носители, содержащие необходимые для деятельности Общества ПДн, должны:

- проверяться на наличие вредоносных программных продуктов;
- учитываться в соответствии с настоящей политикой;

- передаваться работникам, являющимся пользователями ИСПДн Общества, только с разрешения руководителя структурного подразделения с записью в соответствующих: формах учета.

13.3. Перечень лиц Общества, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

Форма Перечня лиц Общества, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей приведена в Приложении № 13 к настоящему Положению.

14. Правила резервирования и восстановления данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним в Обществе

14.1. Общие правила и требования, предъявляемые к системам резервирования информационных систем

Системы резервного копирования должны располагаться в помещениях, относящихся к категории «ограниченного доступа», работа в которых разрешена сотрудникам, допущенным к эксплуатационному обслуживанию систем резервного копирования.

Качество записи резервных копий на внешних носителях должно проверяться непосредственно после изготовления копии, в том числе, в автоматизированном режиме.

Надежность и правильность записи критической информации следует периодически проверять тестированием и использованием контрольных процедур восстановления.

Текущее резервирование данных должно производиться автоматически, постоянно либо в ночное время, в специально выделенные директории сервера резервирования.

Количество сотрудников, допущенных к эксплуатационному обслуживанию систем резервного копирования и восстановления данных, должно быть максимально ограничено.

Съемные носители, предназначенные для целей резервного копирования/архивирования, должны быть соответствующим образом промаркированы и учтены в специальном журнале.

Запись резервных копий на неучтенные носители категорически запрещена.

Все факты нарушения и восстановления работоспособности систем или оборудования должны регистрироваться в специальном журнале за подписью администратора информационной безопасности Общества.

Все факты нарушения работоспособности систем или оборудования, а также разрушения данных на серверах или рабочих станциях Общества классифицируются как «нарушения информационной безопасности 1 и 2 категорий» и должны анализироваться через процедуру служебного расследования согласно «Положению о служебном расследовании нарушений режима информационной безопасности».

Все действия систем резервного копирования должны фиксироваться в электронном журнале, ведущемся в автоматизированном режиме и не допускающем модификации и уничтожения данных, доступном только для просмотра администратору информационной безопасности (далее - АИБ) и администратору системы резервного копирования (если таковой имеется)

14.2. Разграничение полномочий по резервированию данных в информационных системах

Формирование рабочих резервных копий ИС Общества должно проводиться в автоматизированном режиме, путем соответствующих настроек комплекса резервирования.

Восстановление работоспособности систем или оборудования, а также восстановление разрушенных данных на серверах ИС должны выполняться ответственным сотрудником Общества, исполняющим обязанности АИБ.

Мониторинг событий, фиксируемых сервером резервирования, должен выполняться работником Общества, исполняющим функции АИБ.

14.3. Требования по размещению оборудования резервного копирования

Не рекомендуется размещение оборудования резервного копирования в одних помещениях с серверами, данные которых резервируются.

Допускается размещение основного и дублирующего (резервирующего) оборудования резервного копирования в разных помещениях (на разных этажах) одного здания.

Системы резервного копирования должны располагаться в помещениях ограниченного доступа, доступ в которые должен быть регламентирован.

14.4. Объекты резервирования ИС и периодичность создания резервных копий

Объекты резервирования в компьютерной сети Общества и периодичность их создания:

- ИС (БД) Общества - один раз в 7 суток в ночное время (в автоматизированном режиме).

14.5. Срок хранения рабочих резервных копий

Срок хранения резервных копий ИС Общества - 7 суток, по истечении 7 суток резервная копия уничтожается автоматически, путем записи поверх нее последующей резервной копии по циклу.

14.6. Количество резервных копий, объекты и субъекты их хранения

В информационной системе Общества должна изготовляться одна еженедельная рабочая резервная копия, которая хранится на RAID массиве жестких дисков сервера резервного копирования. Может изготовляться дублирующая резервная копия на съемных носителях.

14.7. Учет и регистрация съемных носителей резервных копий

Администратором информационной безопасности ведется «Журнал учета и выдачи машинных носителей информации».

Журнал учета должен быть зарегистрирован в системе документооборота Общества, страницы журнала должны быть пронумерованы, а журнал прошит и опечатан так, чтобы: исключить замену страниц.

Все носители, на которые производится запись резервных копий ИС, должны регистрироваться в «Журнале учета машинных носителей информации».

14.8. Правила работы и обязанности должностных лиц по процедуре резервирования и восстановления данных, хранению и уничтожению рабочих резервных копий

Запрещается копирование и обработка любой информации, переносимой с помощью съемных носителей, без производственной необходимости.

Запрещается производить резервирование данных на неучтенные носители.

Рабочие резервные копии на КАШ массиве жестких дисков сервера резервирования должны уничтожаться автоматически путем проведения процедуры перезаписи по окончанию срока их актуальности.

В случае обоснованных подозрений о разрушении части данных в ИС Общества, сотрудникам, обнаружившим признаки разрушения, необходимо немедленно сообщить об этом АИБ.

Администратор аварийного восстановления данных, совместно с администратором баз данных и администратором информационной безопасности (АИБ), в рабочем порядке производят анализ ситуации и, при необходимости, принимают решение о восстановлении данных с соответствующей рабочей резервной копии ИС.

После проведения процедуры восстановления ИС ответственные лица, участвующие в указанной процедуре, составляют совместную докладную записку о проведенных действиях по восстановлению ИС.

Все факты разрушения ИС на серверах Общества, классифицируются как «нарушения информационной безопасности I и П категорий» и должны анализироваться через процедуру служебного расследования согласно «Положению о служебном расследовании нарушений информационной безопасности».

14.9. Ответственность

Ответственность за учет и выдачу съемных носителей для резервирования (далее резервных носителей) возлагается на АИБ Общества.

Ответственность за мониторинг событий, фиксируемых сервером резервирования, возлагается на сотрудника Общества, исполняющего функции администратора информационной безопасности системы резервирования данных.

Ответственность за своевременное восстановление работоспособности систем или оборудования, а также разрушенных данных на серверах Общества, возлагается на сотрудника Общества, исполняющего функции администратора аварийного восстановления данных.

Ответственность за ввод в действие, установку и обновление необходимого программно-аппаратного обеспечения технологии резервирования данных информационной системы возлагается на администратора компьютерной сети Общества.

14.10. Контроль

Контроль за соблюдением правильности технологии резервного копирования данных возлагается на администратора информационной безопасности Общества.

Контроль за соблюдением правильности политики резервирования данных и учет* съемных носителей информации, предназначенных для создания резервных копий информационной системы, возлагается на структурное подразделение - **OTflej** информационных технологий Общества.

14.11. Расследование нарушений положений настоящей Политики

Все факты разрушения данных на серверах или компьютерах, нарушения работоспособности ИС и/или оборудования в информационной инфраструктуре Общества, а также их последствия, классифицируются как нарушения 1 и 2 категории.

Нарушения 1 и 2 категории должны анализироваться через процедуру служебного расследования в соответствии с «Положением о служебном расследовании нарушений информационной безопасности».

15. Инструкция по обеспечению безопасности сведений при их обработке в информационных системах

15.1. Порядок допуска персонала к сведениям при их обработке в информационных системах

Подключение пользователя к информационной системе Общества (или изменение прав доступа) осуществляется на основании «перечня лиц, допущенных к работе в информационной системе Общества» и «Заявки на подключение...», поданной руководителем лица, допущенного к работе в информационной системе, согласованной и утвержденной соответствующими должностными лицами Общества.

Перед началом работы администратор информационной безопасности, должен ознакомить пользователя с присвоенными ему параметрами доступа, правилами применения и функционирования парольной и антивирусной защиты, а также правилами настоящей Инструкции под роспись и выдать копию инструкции на руки.

15.2. Принципы формирования личных паролей

Принципы выбора и формирования личных паролей:

- пароль первого входа в информационную систему, «Password_l», устанавливается администратором при создании или корректировке учетной записи пользователя;

- при первом входе в сеть пользователь должен поменять пароль, с выполнением требований, указанных в следующем пункте.

Пароль должен удовлетворять следующим требованиям сложности:

- в качестве парольной информации следует выбирать последовательность букв, цифр и служебных символов длиной не менее шести знаков;

- политика безопасности домена задана следующим образом: символы, из которых может состоять пароль, делятся на четыре группы:

1 группа: a...z;

2 группа: A...Z;

3 группа 0...9;

4 группа: специальные символы (например - !;%:?{}?>< и т.п.).

Смена паролей пользователем производится ежеквартально, о чем за 3 дня до истечения срока использования пароля система должна напоминать пользователю при каждом входе в систему.

Вновь вводимые пароли не должны совпадать, как минимум, с пятью последними использовавшимися паролями.

Возможна генерация паролей пользователя администратором вычислительной сети или самим пользователем с использованием специальных программ генерации паролей.

После ознакомления с настоящей инструкцией пользователь информируется о назначенном ему пароле однократного доступа. Используя указанный пароль, со своего рабочего места, он должен войти в компьютерную сеть, самостоятельно составить или сгенерировать пароль доступа к системе и ввести выбранный пароль в систему. В случае если в прикладных программах используются самостоятельные пароли, их выбор и ввод осуществляется аналогично.

Пароли пользователя на доступ к различным информационным системам не должны повторяться.

15.3. Обязанности персонала по использованию и сохранению в тайне личных паролей и ключевой информации

Ввод личного пароля следует проводить, предварительно убедившись в отсутствии возможности визуального ознакомления с его набором другими лицами. Запрещается:

- ознакомление с парольной информацией сотрудников Общества, а также других посторонних лиц, независимо от их должности;
- вход в сеть с использованием чужих идентификаторов доступа;
- передача личного пароля сотрудникам или руководителям подразделений Общества, независимо от их должности;
- оставлять без присмотра рабочее место с незаблокированным монитором (при оставлении рабочего места необходимо использовать функцию «временной блокировки»);
- хранить личный пароль доступа в потенциально доступном для ознакомления посторонними и другими сотрудниками месте;
- работникам Общества, ознакомленным, в пределах своих должностных обязанностей и полномочий, с системными паролями, паролями ключей электронной подписи, ключевой информацией, сообщать эту информацию кому бы то ни было без письменного указания администратора информационной безопасности Общества.

В случае утраты пароля, либо при обоснованном подозрении его раскрытия, пользователь обязан незамедлительно поставить об этом в известность администратора информационной безопасности Общества, а затем произвести экстренную замену личного пароля.

Сообщение своего пароля другому сотруднику (за исключением случаев проверю качества парольной информации), является нарушением требований информационно безопасности Общества. Контроль выполнения указанного требования возлагается н: руководителей всех структурных подразделений Общества.

Пользователи информационной системы Общества должны незамедлительно докладывать администратору информационной безопасности Общества обо всех замеченные нарушениях в работе с парольной информацией. Некорректные действия любого сотрудника с парольной информацией могут стать предметом служебного расследования.

15.4. Обязанности персонала по обеспечению защиты ИСПДн от вредоносных

программ

Копирование любой информации, переносимой с помощью съемных носителей, должно производиться только после проведения процедуры антивирусного контроля съемного носителя.

В случае появления подозрений на наличие вирусов в информационной системе Общества пользователи компьютерной сети должны немедленно ставить в известность администратора информационной безопасности Общества.

Все факты нерегламентированного копирования, модификации и разрушения данных на серверах или рабочих станциях, включенных в компьютерную сеть Общества, а также заражение их вирусами, классифицируются как нарушения информационной безопасности и должны рассматриваться через процедуру служебного расследования.

15.5. Правила работы персонала со сведениями при их обработке в информационных системах Общества

В настоящей главе приведены требования, определяющие условия и порядок подключения пользователей ПК к информационным ресурсам Общества (далее - ресурсы), а также требования по обеспечению при этом безопасности конфиденциальной информации.

Передача конфиденциальной информации по каналам связи, выходящим за пределы контролируемой зоны, разрешается только при использовании защищенных каналов связи, в том числе защищенных волоконно-оптических линий связи.

Доступ к информационным ресурсам предоставляется пользователям исключительно для выполнения ими своих служебных обязанностей при выполнении следующих условий:

- существует техническая возможность для предоставления конкретного вида доступа к ресурсу;
- не создается предпосылок к возникновению угроз информационной безопасности;
- деятельность пользователя не наносит экономический ущерб и не нарушает российское и международное законодательство.

Несоблюдение хотя бы одного из этих условий, является основанием для отказ пользователю в доступе к ресурсам.

Доступ к ресурсам ограничивается для каждого пользователя по принцип} минимально необходимого для выполнения его функций набора ресурсов и сервисов.

Решение о необходимости доступа к ресурсам принимает ответственный з; обеспечение безопасности персональных данных информационной системы пользователя Основанием для предоставления доступа является обоснованная заявка в адрес Руководителя проектов по информационным. технологиям. Заявка должна содержать:

- реквизиты пользователя (подразделение, занимаемая должность, фамилия, их отчество);
- наименование информационных ресурсов, к которым предполагаете подключение;
- состав СВТ пользователя (ПК, принтер, сканер);

предполагаемые виды работ и используемые прикладные сервисы (E-Mail,

HTTP);

режим подключения пользователя к ресурсам (постоянный, временный. Если временный, то указать интервал);

- состав общего и телекоммуникационного программного обеспечения (ОС, клиентские прикладные программы для сети);
- число и перечень предполагаемых абонентов (для электронной почты); перечень сведений конфиденциального характера, обрабатываемых (хранимых)

на ПК, подлежащих передаче и получаемых из сети;

- установленные средства защиты информации.

После соответствующих согласований, в случае положительного решения заявка направляется к АИБ для обеспечения подключения пользователя к соответствующим ресурсам.

При увольнении сотрудника его доступ к ресурсам ликвидируется АИБ.

При переводе сотрудника на другую должность и (или) в другое подразделение доступ приостанавливается до выполнения требований по порядку подключения к информационным ресурсам.

В случае болезни, убытия в командировку или отпуск пользователя, ответственный за обеспечение безопасности персональных данных в информационной системе пользователя обязан принять решение о необходимости блокировки пароля данного пользователя.

Администрирование средств доступа к ресурсам, осуществление их бесперебойной работы, учет пользователей, протоколирование их работы и контроль выполнения требований информационной безопасности ведется информационным подразделением и подразделением по защите информации или АИБ.

Администратор информационной безопасности имеет право осуществлять контроль деятельности любого пользователя. В случае невыполнения одного из условий по подключению пользователя к информационным ресурсам, он обязан немедленно блокировать доступ пользователя с последующим информированием ответственного за обеспечение безопасности персональных данных соответствующей информационной системы.

Администратор информационной безопасности имеет право вмешаться і технологический процесс обработки информации только средствами временной блокировки.

Журналы работы пользователей ведутся на серверах доступа и могут был использованы для обоснования проведения служебных проверок и принята соответствующих мер по их результатам.

15.5.1. Требования к пользователю

Пользователь обязан:

- обращаться к АИБ по вопросам использования аппаратно-программного обеспечения своего ПК, выполнять его устные распоряжения или письменные указания соответствии с настоящим Положением;
- использовать предоставленные ему аппаратно-программные средства только для выполнения своих должностных обязанностей;
- устанавливать пароль на СВТ, не включенных в ЛВС;
- производить смену установленного пароля.

Пароль является средством идентификации доступа, представляющим собой буквенно-цифровую последовательность, и служит для предотвращения несанкционированного доступа к информации, хранящейся на компьютере.

Пароль является служебной информацией, не подлежащей разглашению. Пароль не должен состоять из простых общеизвестных слов, имен, фамилий. Желательно использование в пароле цифр, символов пунктуации, других редко используемых символов. Длина пароля должна быть не меньше шести символов. При компрометации паролей пользователь обязан немедленно поставить в известность администратора сети, который должен незамедлительно принять меры к замене скомпрометированного пароля. Ответственность за несвоевременность уведомления о факте компрометации пароля несет непосредственно пользователь;

- определять (самостоятельно или с помощью администратора сети) информационные ресурсы, требующие регулярного резервного сохранения (архивирования). Конкретный вид, периодичность и порядок архивирования определяется пользователем самостоятельно или с помощью администратора сети. Ответственность за проведение архивирования информационных ресурсов возлагается на пользователя. Пользователю рекомендуется также убедиться в возможности восстановления информационных ресурсов из архивных копий;
- регулярно (не реже чем раз в неделю) проводить антивирусную проверку компьютера, знать и уметь пользоваться антивирусным программным обеспечением;

- производить антивирусную проверку внешнего носителя информации перед проведением любых операций с внешним носителем информации (дискета, компакт - диск, винчестер). Антивирусная проверка проводится пользователем также при получении файлов электронной почты;

- использовать предоставленное ему дисковое пространство сервера ЛВС только для хранения информационных ресурсов, необходимых для осуществления своих должностных обязанностей;

- немедленно информировать руководителя подразделения (штатного специалиста) по защите информации и своего непосредственного руководителя о любых нарушениях сохранности информационных ресурсов, а также о возможности появления нарушений, которые могут привести к несанкционированному доступу, модификации, разрушению удалению информационных ресурсов или сбоям в работе СВТ (ЛВС) в целом.

Пользователю запрещается:

- разглашать пароли, предназначенные для регистрации в сети (сетях) и получена доступа к защищаемым информационным ресурсам, дискам (физическим и логическим) томам, отдельным каталогам, базам данных, отдельным файлам и другим информационные объектам, в том числе при убытии в командировку, отпуск и в случае болезни;

- осуществлять несанкционированный доступ к информационным ресурсам, ему н предназначенным;

- предпринимать какие-либо действия, приводящие к незаконному просмотр] копированию, модификации или удалению информационных ресурсов;

- работать от имени другого пользователя;

- допускать к работе в сети других лиц под своим регистрационным именем, также оставлять без присмотра зарегистрированный в сети компьютер (рабочую станцию); выполнять работы и услуги по организации и предоставлению доступа к сетевым ресурсам сторонним организациям и отдельным лицам;

- самостоятельно производить установку, настройку и модификацию программного обеспечения;

- использовать сменные машинные носители информации без предварительной проверки на наличие программных вирусов;

- использовать СВТ и сетевые ресурсы для выполнения работ, не относящихся к служебной деятельности;

- отключать (блокировать) средства защиты информации;

- записывать и хранить информацию, содержащую конфиденциальные сведения, на неучтенные машинные носители, а также использовать для этих целей носители с выявленными неисправностями;

- хранить съемные машинные носители в накопителях и других устройствах считывания-записи;

- самостоятельно вскрывать и производить разборку компьютеров, периферийного и вспомогательного оборудования;

- производить какие-либо изменения в электрических схемах, монтаже, размещении и комплектации технических средств на ОВТ;

- использовать сторонние общедоступные почтовые ресурсы (подписка по E-mail);

- производить загрузку и запуск неизвестных файлов и программ;

- разрабатывать, использовать и распространять вредоносные программы и программные вирусы, а также машинные носители с такими программами;

- производить какие-либо действия с информацией зараженного вирусом внешнего носителя или зараженными файлами электронной почты.

При обнаружении вируса пользователь ставит об этом в известность администратора сети (информационной безопасности).

Пользователям рекомендуется осуществлять обмен данными, размещенными на компьютере или на сервере ЛВС, используя сетевые средства обмена информацией, а не внешние носители информации.

Пользователь имеет право:

- получать квалифицированные консультации по правилам и навыкам использования средств доступа к ресурсам и по вопросам защиты информации **3** специалистов информационного подразделения и подразделения (специалиста) по защите информации;

- получать техническую помощь в установке, настройке и обслуживании средств доступа к ресурсам у специалистов информационного подразделения;

- ходатайствовать перед руководством подразделения о предоставлении ем; необходимых программно-аппаратных средств для выполнения должностных обязанностей.

15.5.2. Требования к администратору

Не допускается возложение функций администратора сети (информационно безопасности) на представителя организации, не входящей в структуру Общества.

В настоящем Положении под термином «администратор» следует понимать ка «администратора сети», так и «администратора информационной безопасности», зависимости от контекста и полномочий, возлагаемых на администратора по выполнению.

требований организационно-технических мероприятий в соответствии с настоящим Положением.

Администратор информационной безопасности несет персональную ответственность за оперативный контроль действия пользователей и администратора сети, поддерживает в актуальном состоянии базу ключевой информации пользователей.

Администратор информационной безопасности должен иметь техническую возможность временно блокировать (разблокировать) действия любого пользователя, включая администратора сети.

Администратор сети отвечает за администрирование ЛВС своего структурного подразделения, имеющего сервер ЛВС. Он несет персональную ответственность за назначение и изменение прав доступа пользователей к информационным ресурсам, поддерживает в актуальном состоянии базу прав доступа.

Функции выполнения требований по обеспечению сохранности и защите информационных ресурсов возлагаются на администратора сети, если должность администратора информационной безопасности отсутствует.

Администратором назначается один из работников информационного подразделения, на которого возлагаются полномочия и обязанности по обеспечению сохранности и защите информационных ресурсов в соответствии с его должностной инструкцией и настоящим Положением. В зависимости от объема работ по администрированию могут быть назначены несколько администраторов.

Устные или письменные указания администратора, не противоречащие его должностной инструкции и требованиям настоящего Положения, являются обязательными для исполнения пользователями.

К администратору предъявляются те же требования, что и к пользователю в соответствии с настоящим Положением. Помимо этого, администратор обязан:

- знать и правильно использовать имеющиеся программно-аппаратные средства;

- знать и правильно использовать программно-аппаратные средства защиты информационных ресурсов, установленные на СВТ, и обеспечивать сохранность информационных ресурсов посредством этих средств;

- при установке, модернизации программно- аппаратных средств использовал только сертифицированную продукцию;

- оказывать методическую помощь пользователям по вопросам, входящим в его компетенцию, в соответствии с настоящим Положением;

- определять необходимость замены или модификации, новой установи прикладного, операционного, сетевого и других видов программного обеспечения: производить ее самостоятельно или с привлечением работников информационного подразделения, в функциональные обязанности которых входит данная работа;

- определять и предоставлять пользователям СВТ только те права доступа информационным ресурсам, которые необходимы им для выполнения своих должностных обязанностей;

- при передаче СВТ, обрабатывающих конфиденциальную информацию, в друге структурное подразделение уничтожить информацию таким образом, чтобы *t* восстановление было невозможным (если только продолжение обработки информации і этих СВТ, но уже в другом структурном подразделении не связано с производственной необходимостью);

определять совместно с руководителем подразделения пользователя информационные ресурсы общего пользования, требующие регулярного резервного сохранения (архивирования), и принимать меры для обеспечения данного архивирования пользователями или проводить эту процедуру самостоятельно. Администратор также при необходимости совместно с пользователем определяет периодичность (составляет график) архивирования соответствующих информационных ресурсов. Администратору необходимо также убедиться в возможности восстановления информационных ресурсов из архивных копий;

- устанавливать и своевременно обновлять антивирусное программное обеспечение на СВТ в составе ЛВС и на сервере ЛВС.

Конкретный вид сертифицированного антивирусного программного обеспечения зависит как от технических характеристик СВТ, так и от используемого операционного или сетевого программного обеспечения и определяется администратором;

- настраивать интерфейс СВТ пользователя таким образом, чтобы последний смог производить антивирусную проверку любого внешнего носителя информации (дискета, компакт - диск, винчестер), а также файлов электронной почты;

- предусматривать выделение необходимых сетевых ресурсов, доступных всем пользователям ЛВС, для ограничения обмена данными посредством внешнего носителя информации между пользователями ЛВС;

- проводить периодически, но не реже одного раза в полгода, проверку программного обеспечения серверов на состояние защищенности от несанкционированного доступа;

- анализировать регистрационную информацию, относящуюся к функционированию ЛВС, на предмет отслеживания попыток несанкционированного доступа к информационным ресурсам, других действий пользователей, которые могут привести к модификации, разрушению, удалению информационных ресурсов или сбоям в работе СВТ или ЛВС;

- производить распечатку файлов, содержащих регистрационные показатели ЛВС, если обнаружены факты несанкционированного доступа или другие нестандартные ситуации в работе ЛВС. Распечатки подшиваются в дело, которое хранится у администратора;

- немедленно блокировать доступ любого пользователя к ресурсам в случае невыполнения хотя бы одного из условий подключения к информационным ресурсам с последующим информированием руководителя подразделения (штатного специалиста) защите информации, информационного подразделения и руководителя подразделена пользователя;

- иметь структурную схему ЛВС с указанием схемы соединения всех входящих в ЕЮ средств обработки информации: серверов, ПК, концентраторов, модемов, сетевых принтеров других элементов ЛВС с указанием их технических параметров и мест расположения;

- информировать ответственного за обеспечение безопасности персональных данных в информационной системе о любых нарушениях требований по обеспечению сохранности защите информационных ресурсов в соответствии с настоящим Положением, другим нормативными правовыми документами, а также о возможности появления нарушение которые могут привести к несанкционированному доступу, модификации, разрушения удалению информационных ресурсов или сбоям в работе ПК и (или) ЛВС;

- вести учет СВТ, обрабатывающих конфиденциальную информацию;

- хранить все установленные им пароли у руководителя подразделения в запечатанном конверте и своевременно их обновлять;

- при увольнении пользователя или смене его рабочего места удалить идентификатор пользователя в ЛВС, сменить криптографические ключи, если пользователем использовались средства шифрования информации, провести другие аналогичные организационно - технические мероприятия, уменьшающие возможность несанкционированного доступа к информационным ресурсам;

- предоставлять руководителю подразделения (штатному специалисту) по защите информации необходимые ему сведения в части возложенных на администратора полномочий и обязанностей в соответствии с настоящим Положением.

Администратору запрещается:

- назначать один и тот же пароль или его несущественные модификации на СВТ в составе ЛВС и на серверах ЛВС;

- передавать или разглашать список паролей или каждый пароль в отдельности другому лицу, если у последнего нет на, то полномочий, определенных его должностными обязанностями или другими распорядительными, предписывающими документами.

Не допускается назначение идентификатора уволившегося пользователя новому (другому) пользователю ЛВС.

15.6. Контроль деятельности персонала

Контроль действий пользователей в информационных системах Общества осуществляется руководителями структурных подразделений, администратором информационной безопасности на основе анализа журналов входа, попыток несанкционированного доступа, журналов работы пользователей рабочих станций, а также систем мониторинга сетевых протоколов.

15.7. Ответственность за нарушения информационной безопасности, порядок их рассмотрения

Нарушения информационной безопасности 3 категории доводятся до руководителя подразделения, сотрудник которого совершил нарушение. По представлению руководитель* нарушитель может быть временно или постоянно ограничен в правах на ресурсы сети.

По нарушениям информационной безопасности 1 и 2 категорий, назначаете служебное расследование, проводимое в соответствии с «Положением о служебном расследовании нарушений режима информационной безопасности».

По решению председателя комиссии по служебному расследованию, на врем, проведения расследования пользователь сети, совершивший нарушение, может быт отключен от всех сервисов удаленного доступа, конфиденциальных ресурсов компьютерной сети и информационных систем Общества.

16. Положение о служебные расследования нарушений режим информационной безопасности в информационных системах

16.1. Классификация инцидентов информационной безопасности

Нарушения режима информационной безопасности (далее - ИБ) и их последствия классифицируются по значимости на:

- нарушения I категории;
- нарушения П категории;

- нарушения Ш категории.

Для классификации инцидентов ИБ ИС следует придерживаться «Перечня нарушений ИБ».

Служебное расследование назначается по нарушениям I и П категорий. 16.2. Перечень нарушений иб

Нарушения 1 категории, к которым относятся события, повлекшие за собой разглашение (утечку) защищаемых сведений и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) сведений, выведение из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- несанкционированная переконфигурация параметров информационной системы (далее - ИС);
- утрата или кража резервной копии ИС;
- необоснованная передача массивов ИС;
- организация утечки сведений по техническим каналам;
- умышленное нарушение работоспособности ИС;
- НСД к сведениям ИС;
- несанкционированное внесение изменений в ИС;
- умышленное заражение компьютеров и серверов ИС вирусами;
- проведение работ с ИС, повлекшее за собой необратимую потерю данных;
- другие действия, подпадающие под действия статей 272, 273, 274 УК РФ. **Нарушения 2 категории,** к каковым относятся: события, в результате которых

возникают предпосылки к разглашению (утечке) защищаемых сведений, утрата содержащих их отчуждаемых носителей, уничтожение (искажение) ИС, выведение из строя технических и программных средств, а именно:

- ошибка при входе в ИС (набор не назначенного пароля, более трех раз подряд периодически);
- несанкционированное (неоднократное) оставление включенного ПК;
- перезагрузка компьютера, при сбоях в работе ПК, (неоднократная) в т.ч аварийная (неоднократная) перезагрузка, путем нажатия кнопки RESET;
- утрата учтенного отчуждаемого съемного носителя;
- попытка входа под чужим именем, паролем, многократная неудачная;
- попытка входа под чужим именем, паролем, удачная;
- несанкционированная очистка журналов аудита;
- несанкционированное копирование данных на внешние носители;
- несанкционированная установка (удаление) ПО ИС;
- несанкционированное изменение конфигурации ПО ИС;

- попытка получения прав администратора на локальном ПК (увеличен собственных прав, получение прав на отладку программ), удачная и неудачная;
- попытка получения прав администратора в домене или на удаленной сервис удачная и неудачная;
- неумышленное заражение локального или сетевого ПК компьютера* вирусами.
- несанкционированное использование сканирующего ПО;
- несанкционированное использование анализаторов протоколов (сниффероов);
- несанкционированный просмотр, вывод на печать и т.п. сведений. **Нарушения 3 категории,** к каковым относятся события, не несущие признаков

нарушений 1 и 2 категорий, а именно:

ошибка при входе в ИС (набор неправильного пароля, сетевого имени более трех раз подряд, не периодически);

попытка неудачного доступа к сведениям в ИС (периодическая);

- перевод времени на ПК;

- выполнение собственных производственных обязанностей на компьютере в неразрешенное время;

перезагрузка компьютера при сбоях в работе ПК (однократная), в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

- нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

16.3. Порядок назначения и проведения служебного расследования

Служебное расследование назначается по нарушениям 1 и 2 категорий.

Состав комиссии, а также сроки проведения служебного расследования назначаются распоряжением ответственного за организацию обработки персональных данных по каждому отдельному факту нарушения или по факту группы нарушений.

Служебное расследование может быть инициировано на основании устного заявления, докладной или служебной записки любого работника Общества, а также по выявленному отдельному факту нарушения, либо по факту группы нарушений.

16.4. Состав комиссии для проведения служебного расследования

В состав комиссии в обязательном порядке входят:

- председатель комиссии - ответственный за организацию обработки персональных данных в Обществе;
- заместитель председателя - администратор информационной безопасности. Члены комиссии:
- начальник Общего Отдела;
- заместитель генерального директора по расчетам;
- главный бухгалтер;
- начальника Управления по расчетам с населением;
- Начальник Службы безопасности;
- Заместитель начальника юридического отдела.

В случае необходимости Председатель комиссии может привлекать к работе:

- администратора компьютерной сети Общества;
- непосредственного начальника нарушителя;
- экспертов из других подразделений:
- специалистов организаций-лицензиатов. Члены комиссии имеют право:
- требовать документального подтверждения факта нарушений информационной безопасности ИС;
- устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству Российской Федерации;
- брать письменные объяснения по поводу выявленных нарушений у любого сотрудника Общества.

16.5. Ответственность

За выявление и классификацию инцидента ИБ, требующего проведения процедуры служебного расследования, ответственность несут:

- администраторы информационной безопасности;
- администраторы ИС.

За назначение процедуры служебного расследования ответственность несет руководитель, ответственный за организацию и руководство работами по защите информации в Обществе.

За проведение процедуры служебного расследования ответственность несет председатель комиссии.

За содержание, обоснованность, актуализацию настоящей политики, а также надлежащее выполнение ее положений, ответственность несет администратор информационной безопасности.

16.6. Оформление результатов работы комиссии

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения на имя заместителя генерального директора, ответственного за организацию и руководство работами по технической защите информации, с предложениями по необходимым организационным выводам, а также по расширению или дополнению «Перечня нарушений ИБ».

Результатом работы Комиссии должен стать АКТ, в котором изложены:

- документальное подтверждение факта нарушений информационное безопасности ИС;
- установленные причины выявленных нарушений в ИС;
- сформированные предложения по устранению причин, выявленных инцидента ИБ в ИС;
- предложения по расширению (дополнению) «Перечня нарушений ИБ».

17. Порядок предоставления и контроля прав доступа к сведениям информационной системе

В составе ИС должны использоваться встроенные или наложенные СЗИ от НС Д.

Учет СЗИ, а также эксплуатационной и технической документации на них ведется эксплуатационной и технической документации к СЗИ. Журнал ведется по форме согласно Приложению № 8.

В ИС должны обеспечиваться:

- идентификация;
- аутентификация;
- авторизация;
- управление доступом;
- контроль целостности и регистрации, включая функционирование системы парольной защиты ПК и ИС;
- непротиворечивая и «прозрачная» для пользователя административно-техническая поддержка задач управления доступом к ресурсам ПК и ИС.

Доступ к ИС, размещенной на магнитных носителях серверного и сетевого оборудования информационной инфраструктуры Общества, должен регламентироваться правами пользователей и иметь несколько уровней защиты.

Контроль доступа пользователей к ИС должен обеспечиваться:

- применением паролей (парольной информации) как механизма авторизации пользователя в информационной инфраструктуре Общества в целях защиты от НСД;
- регистрацией действий администраторов и пользователей ИС (при наличии технической возможности) в специальном электронном журнале, доступном для чтения, просмотра, анализа, хранения, резервного копирования и архивирования только сотруднику, исполняющему функции администратора ИБ;
- формированием уникальных идентификаторов сообщений и идентификаторов пользователей.

Назначение прав доступа пользователей к ИС Общества осуществляется в соответствии заявками на предоставление пользователю прав доступа к ресурсу ИС (далее -заявка) от руководителей структурных подразделений Общества.

Назначение прав и уровня доступа осуществляется исключительно администратором ИС Общества, о чем делается соответствующая запись в Журнале учета логинов сотрудников, допущенных к работе с персональными данными в информационных системах персональных данных компьютерной сети Общества. Журнал ведется согласно Приложению №22.

Разрешение на установление прав доступа пользователю производится на основании письменной заявки начальника подразделения, в котором работает сотрудник. В заявке должны указываться:

- содержание запрашиваемых изменений (регистрация нового пользователе информационной инфраструктуры, удаление учетной записи пользователя, расширение ИЛЕ сужение полномочий и прав доступа к ресурсам информационной инфраструктуры ране* зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчестве сотрудника;
- имя пользователя в компьютерной сети Общества (учетная запись сотрудника);
- полномочия, которые необходимо добавить пользователю, или которые необходимо лишить пользователя (путем указания решаемых пользователе] производственных задач на конкретных ПК).

При увольнении работников, изменении их должности или перемещении их из одного подразделения в другое, отделение по общим вопросам обязано информировать администратора ИБ о необходимости аннулирования (блокирования) прав доступа данных сотрудника к информационным ресурсам КС Общества.

Все факты несанкционированной организации доступа и регистрации в ИС Обществ, а также их последствия, классифицируются в соответствии с «политикой проведен служебного расследования нарушения режима ИБ ИС».

Нарушения 1 и 2 категории должны анализироваться через процедуру служебного расследования в соответствии с «Положением о служебном расследовании нарушения режима ИБ ИС».

Ответственность за техническую реализацию системы защиты при управлении доступом и регистрацией пользователей в компьютерной сети и ИС несет администратор информационной безопасности.

Ответственность за мониторинг и ведение анализа событий, фиксируемых подсистемами регистрации инцидентов ИС, несёт администратор информационной безопасности.

За мониторинг и ведение анализа событий, фиксируемых системами информационной безопасности, ответственность несет сотрудник, выполняющий функции администратора информационной безопасности.

Контроль за выполнением положений и требований настоящей главы должен осуществлять сотрудник, выполняющий функции администратора информационной безопасности.

Контроль за выполнением требований информационной безопасности осуществляется администратором информационной безопасности. Наличие у сотрудника избыточных, неконтролируемых прав доступа является нарушением требований информационной безопасности ИС Общества.

Распределение прав доступа сотрудников к ИС должен осуществлять администратор информационной безопасности.

18. Порядок приостановления предоставления доступа к ресурсам информационной системы в случае обнаружения нарушений порядка ее использования

Работа с ИС должна приостанавливаться только при обнаружении нарушений 1 и/или 2 категорий.

Требования настоящей главы обязательны для всех пользователей и администраторе ИС.

Пользователь, обнаруживший нарушения при работе с ИС, обязан сообщить об этом своему непосредственному руководителю либо администратору ИБ. Администратор ИБ обязан:

- установить категорию выявленного нарушения;
- при установлении 1 или 2 категории нарушения инициировать проведение служебного расследования;
- оповестить все отделы и сотрудников, работающих с ИС, о прекращении доступа к ресурсам ИС на время проведения служебного расследования.

Все отделы и сотрудники, работающие с ИС, обязаны:

- временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИС;
- содействовать проведению служебного расследования.

Работа с ресурсами ИС может быть возобновлена только после устранения всех выявленных нарушений, их последствий.

19. Порядок обеспечения информационной безопасности в информационных системах средствами протоколирования и анализа значимых событий

Правила и порядок протоколирования и анализа (аудита) значимых событий в ИС Общества, направлены на предупреждающую фиксацию и изучение действий субъектов и объектов в ИС.

Все события, происходящие в ОС, ИС, других критических приложениях и СЗИ, должны протоколироваться в специальных электронных журналах аудита.

Созданные ИС, в которых отсутствуют функции ведения электронных журналов протоколирования и анализа (аудита) значимых событий, должны предусматривать такие функции при модернизации системы.

Техническое задание на вновь создаваемые ИС должно содержать требования по созданию электронных журналов протоколирования и анализа (аудита) значимых событий.

Аудит событий, зафиксированных в указанных электронных журналах, должен анализироваться в плановом порядке на постоянной основе.

Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

Настройки журналов аудита должны однозначно интерпретировать все значимые события в ИС.

Электронные журналы аудита не должны быть доступны для чтения, уничтожения и модификации пользователями ИС.

Электронные журналы аудита не должны быть доступны для уничтожения и модификации администраторами ИС.

Электронные журналы аудита должны быть доступны для чтения и архивирования сотруднику, выполняющему функции администратора информационной безопасности.

Архивные копии электронных журналов аудита событий должны регистрироваться администратором информационной безопасности в специальном журнале и сдаваться на ответственное хранение. Срок хранения архивных копий электронных журналов аудита должен составлять не менее 5 (пяти) лет.

Ответственность за техническую реализацию системы протоколирования и анализа (аудита) значимых событий в ИС несет заместитель генерального директора Общества, курирующий вопросы технической защиты информации.

Ответственность за мониторинг событий, фиксируемых информационными подсистемами, несут администраторы соответствующих ИС.

Ответственность за мониторинг и анализ событий, фиксируемых системами безопасности, несет администратор информационной безопасности.

Ответственность за организационно-технические меры, направленные *m* предотвращение угроз информационной безопасности, зафиксированных системам протоколирования событий, несет администратор ИБ.

Контроль за текущей деятельностью пользователей информационной инфраструктуры Общества осуществляет сотрудник, выполняющий функции администратора информационной безопасности.