УТВЕРЖДАЮ
Руководитель Уральского управления
Федеральной службы по экологическому,
технологическому и атомному надзору

_____ А.С. Поляков
«05» октября 2017 г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УРАЛЬСКОГО УПРАВЛЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ

Используемые сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	Базы данных
ЗИ	Защита информации
ИСПДн	Информационная система персональных данных
КС	Корпоративная сеть
КВС	Корпоративная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
РД	Руководящий документ
СВТ	Средства вычислительной техники
СЗИ	Система защиты информации
СКЗИ	Средства криптографической защиты информации
СКУД	Система контроля управления доступом
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЧС	Чрезвычайная ситуация
ЭВМ	Электронная вычислительная машина
ЭК	Экспертная комиссия

Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации определенного вида деятельности

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних и внешних угроз

Доступность информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных и правовых документов или требованиями, устанавливаемыми собственником информации

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

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

Несанкционированный доступ – получение защищаемой информации заинтересованным субъектом с нарушением установленных нормативными правовыми документами или обладателем информации прав или правил доступа к защищаемой информации

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

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

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

Система защиты информации в автоматизированной системе – совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации

Техническая защита конфиденциальной информации – комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней

Целостность информации – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения

1. Общие положения

1.1. Настоящее Положение определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных в Уральском управлении Федеральной службы по экологическому, технологическому и атомному надзору (далее по тексту — Управление) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение разработано в соответствии с действующим законодательством Российской Федерации в области безопасности информации, а также ГОСТ и руководящими документами (РД) ФСТЭК (Гостехкомиссии) России, перечень которых приведен в разделе 10.

1.3. Положение является основой для разработки локальных нормативных актов Управления по обеспечению безопасности ПДн.

1.4. Настоящее положение распространяется на всех сотрудников Управления, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с Управлением на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

2. Цели и задачи обеспечения безопасности персональных данных

2.1. Целью реализации различных мер и мероприятий по защите персональных данных является минимизация возможных потерь от разглашения, утечки или несанкционированного доступа к информации Управления, содержащей персональные данные государственных гражданских служащих и сотрудников сторонних организаций, взаимодействующих с Управлением.

2.2. Задачами, которые необходимо решить для достижения поставленной цели являются:

- своевременное выявление потенциальных угроз защищаемой информации и средствам ее обработки и передачи;
- выявление причин, обстоятельств и условий, способствующих реализации выявленных угроз и выработка мероприятий по их нейтрализации;
- предотвращение НСД к информации и средствам ее обработки и передачи;
- предотвращение непреднамеренных воздействий на информацию и средства ее обработки и передачи;
- контроль эффективности защитных мер и мероприятий.

3. Защищаемые информационные ресурсы

3.1. К защищаемым информационным ресурсам Управления относятся:

- информация, зафиксированная на различных носителях;
- средства обработки, хранения, передачи персональных данных и средства связи, в том числе программное обеспечение указанных средств (при его наличии);
- средства защиты информации.

3.2. Информация подлежащая защите:

3.2.1. Защите подлежит информация, содержащая персональные данные государственных гражданских служащих и сотрудников сторонних организаций, взаимодействующих с Управлением.

3.2.2. Согласно ФЗ № 152 от 27 июля 2006 года «О персональных данных», персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.2.3. Конкретный состав персональных данных, обрабатываемых в Управлении, закреплен в Приказе «Об утверждении перечня персональных данных, обрабатываемых в Уральском управлении Федеральной службы по экологическому, технологическому и атомному надзору».

3.2.4. Защищаемые информационные ресурсы могут быть представлены в виде отдельных документов (массивов документов) на бумажных носителях, а также в виде документов (файлов) и массивов документов в сети Управления и/или на машинных носителях информации.

4. Методы и способы обеспечения безопасности персональных данных

4.1. Методы и способы защиты персональных данных при их обработке в информационных системах персональных данных Управления:

- регламентация разрешительной системы доступа пользователей к сведениям, содержащим персональные данные;
- размещение технических средств обработки персональных данных в пределах контролируемой зоны, организация физической защиты помещений и технических средств обработки персональных данных, а также средств и систем защиты;
- ограничение доступа пользователей в помещения, где ведется обработка персональных данных, расположены технические средства обработки, а также средства и системы защиты информации;
- разграничение доступа пользователей к программным средствам обработки персональных данных, средствам защиты информации;
- учет и хранение носителей персональных данных;
- контроль несанкционированного доступа к персональным данным, регистрация действий пользователей (управление доступом, регистрация и учет);
- резервирование технических средств, дублирование массивов персональных данных;
- использование средств антивирусной защиты;
- использование средств межсетевого экранирования при взаимодействии информационных систем персональных данных друг с другом, а также с сетью общего пользования и/или сетью международного информационного обмена;
- криптографическая защита каналов передачи персональных данных за пределы контролируемой зоны;

- обнаружение вторжений в информационные системы персональных данных, создающих условия нарушения безопасности персональных данных;
- анализ защищенности информационных систем персональных данных.

5. Обработка персональных данных

5.1. Под обработкой персональных данных понимается 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.

5.2. В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

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

5.3. Обработка персональных данных может осуществляться оператором только с согласия субъектов персональных данных, за исключением следующих случаев:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, 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;
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- 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 оператора или третьих лиц либо для достижения Управлением значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы 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 (общедоступные ПДн);

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.4. Получение персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения их из иных источников. Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

5.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

5.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

6. Защита персональных данных

6.1. Регламентация состава персональных данных

6.1.1. Перечень сведений отнесённых к персональным данным определяется в соответствии с действующим в Управлении документом «Перечень персональных данных, обрабатываемых в Управлении».

6.2. Доступ к персональным данным, определение полномочий доступа сотрудников к персональным данным и их реализация

6.2.1. Порядок доступа сотрудников к информационным ресурсам Управления, содержащим персональные данные, определяется в соответствии с действующим в Управлении Приказом «Об утверждении разрешительной системы допуска к персональным данным»ологическому, технологическому и атомному надзору».

6.2.2. Для получения доступа к персональным данным сотрудником пишется заявление на имя руководителя Управления. По решению руководителя сотрудник вносится в список лиц, допущенных к работе с персональными данными.

6.2.3. Каждый сотрудник Управления должен иметь право доступа только к тем персональным данным, которые необходимы ему для выполнения трудовых обязанностей. Необоснованное служебной необходимостью ознакомление сотрудников с персональными данными не допускается.

6.2.4. Передача персональных данных возможна только с согласия субъекта или в случаях, прямо предусмотренных законодательством. При передаче ПДн оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные в коммерческих целях без письменного согласия субъекта ПДн;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

6.3. Технология обработки персональных данных

6.3.1. Процесс обработки персональных данных предусматривает:

- знание государственным гражданским служащим требований нормативно – методических документов по защите персональных данных;
- наличие необходимых условий в помещении для работы с персональными данными, при которых исключается бесконтрольное получение защищаемой информации. Список помещений, в которых ведётся обработка персональных данных, содержится в Приказе «Об утверждении Перечня помещений, в которых размещаются информационные системы персональных данных и осуществляется обработка персональных данных»;
- воспитательную и разъяснительную работу с сотрудниками по предупреждению утраты ценных сведений при работе с персональными данными;
- своевременное выявление нарушения требований разрешительной системы доступа государственными служащими Управления.

6.4. Организация технического обслуживания оборудования, используемого для обработки защищаемой информации.

6.4.1. Оборудование, предназначенное для обработки персональных данных, должно эксплуатироваться в условиях (температура, влажность, электромагнитный режим) в соответствии с инструкциями производителя и/или соответствующих нормативных документов. Техническое обслуживание оборудования должно обеспечивать его постоянную работоспособность.

6.4.2. Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 и ПУЭ.

6.4.3. Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

6.4.4. Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно

выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

6.4.5. Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г)

6.5. Организация пропускного и внутриобъектового режима в Управлении

6.5.1. Доступ сотрудников на территорию Управления и во внутренние рабочие помещения, где обрабатывается защищаемая информация, осуществляется с использованием системы контроля управления доступом (СКУД). Доступ сотрудников в защищаемые помещения должен осуществляется с использованием установленной для этих помещений СКУД с обязательной регистрацией входа и выхода.

6.5.2. Для каждого защищаемого помещения должен быть составлен список сотрудников, имеющих право доступа в данное помещение. Список должен своевременно корректироваться по мере увольнения сотрудников Управления, приема на работу новых сотрудников или перевода сотрудника на другую работу. Сотрудники, не указанные в данном списке, не имеют права находиться в защищаемом помещении без сопровождения сотрудника, имеющего право такого доступа, кроме случаев экстренной необходимости при чрезвычайных обстоятельствах. В данном случае с разрешения администрации Управления помещение снимается с охраны и производится доступ в данное помещение в присутствии лица, ответственного за него, или представителя администрации Управления.

6.5.3. Доступ посетителей на территорию Управления осуществляется по предварительной договоренности с конкретным сотрудником Управления, который сообщает в пропускной пункт, необходимые для оформления временного пропуска — ФИО посетителя, день, цель и место визита. Доступ посетителей во внутренние помещения Управления осуществляется только по временным пропускам.

6.5.4. Выдача посетителю временного пропуска возможна при предъявлении им одного из трех типов установленных документов, а именно Паспорта, Водительского удостоверения или Военного билета.

6.5.5. Посетитель обязан предъявить охране временный пропуск, после чего он получает законное право проследовать на территорию Управления. Все посетители регистрируются в пропускном пункте в журнале учета посещений с записью паспортных или иных данных в соответствии с предъявляемым типом документа. Посетители, пришедшие без предварительной договоренности (курьеры и др.), не имеют права доступа во внутренние помещения Управления.

6.5.6. Перед тем как покинуть внутренние помещения Управления, посетитель должен поставить в отделе обеспечения внутриобъектового режима отметку об уходе во временном пропуске. Сдав охране временный пропуск, посетитель получает право покинуть Управление.

6.5.7. Доступ приглашенного технического и обслуживающего персонала осуществляется в соответствии с необходимыми письменными распоряжениями администрации Управления и фиксируется в журнале учета посещений. Доступ технического и обслуживающего персонала в защищаемые помещения без сопровождения сотрудника Управления не допускается.

6.5.8. Администрация Управления обязана обеспечить сотрудников удостоверениями. При увольнении сотрудники обязаны сдать удостоверение лицу, ответственному за организацию пропускного режима.

6.5.9. На посту охраны при входе в здание должен находиться список сотрудников, имеющих доступ в помещения Управления, в соответствии с которым осуществляется проход сотрудников в здание по предъявлению паспорта при отсутствии у них удостоверения на право входа. Список должен своевременно корректироваться по мере увольнения сотрудников Управления или приема на работу новых сотрудников.

6.6. Разработка организационно-распорядительной и нормативной документации

6.6.1. В Управлении должны быть разработаны и введены в действие все организационно-распорядительные и иные нормативные документы, на которые имеются ссылки в данном Положении.

6.7. Контроль соблюдения требований по обеспечению безопасности персональных данных

6.7.1. Контроль соблюдения требований по обеспечению безопасности информации в Управлении возлагается на администрацию Управления и специально назначенные проверочные комиссии.

6.7.2. В Управлении должна быть должность, ответственного за обеспечение информационной безопасности (администратора), который осуществляет организацию деятельности по защите информации Управления, установку, настройку и администрирование программных и программно-аппаратных средств защиты информации, контроль за выполнением требований по обеспечению безопасности информации.

6.8. Технические (программные и аппаратные) меры

6.8.1. Технические меры предполагают обеспечение защиты персональных данных от утечки по техническим каналам, а также от несанкционированного доступа.

6.8.2. Обеспечение рабочих мест сотрудников, обрабатывающих персональные данные:

- АРМ сотрудников Управления должны быть оборудованы необходимыми программными или программно-аппаратными средствами защиты персональных данных — система парольной защиты, средства защиты информации от НСД, средства антивирусной защиты, криптографические средства (при необходимости), и т.п. Работа со средствами защиты должна быть описана в организационно-распорядительных документах Управления. Все средства защиты должны быть учтены в «Журнале учёта средств защиты информации»;
- сотрудники обязаны использовать технические и программно-аппаратные средства защиты информации, установленные на их рабочих местах и/или использующиеся совместно со средствами обработки, передачи информации и средствами связи;
- не допускается передача персональных данных по открытым каналам связи без использования специальных технических и программных средств защиты (кроме случаев передачи обезличенных или общедоступных ПДн);
- в Управлении должно проводиться обучение сотрудников правилам работы с используемыми техническими и программно-аппаратными средствами защиты информации;
- все, используемые в Управлении технические и программно-аппаратные средства защиты информации должны быть сертифицированы в установленном порядке;
- на АРМ пользователей должно быть установлено только прикладное программное обеспечение (ПО), необходимое пользователю для выполнения им своих трудовых обязанностей. Неиспользуемое пользователем ПО АРМ должно быть отключено или удалено. Установку нового ПО на АРМ и обновление ПО должен осуществлять только системный администратор или сотрудники службы, осуществляющие обслуживание и техническое сопровождение СВТ Управления;
- установка и настройка программно-аппаратных средств защиты информации Управления осуществляется ответственным за информационную безопасность. Доступ к конфигурации программно-аппаратных средств защиты информации для иных пользователей, кроме ответственного лица, должен быть блокирован;
- АРМ должно эксплуатироваться тем сотрудником, за которым оно закреплено. Этот сотрудник несет персональную ответственность за работу своего АРМ и выполнение требований данного Положения по безопасности для своего АРМ;
- должно проводиться своевременное обновление ПО АРМ;

- при наличии подключений к сетям общего пользования должны использоваться системы обнаружения вторжений (атак) и средства анализа и контроля трафика;
- должно быть обеспечено в обязательном порядке наличие источников бесперебойного питания для сетевого и серверного оборудования Управления и, по возможности, для АРМ пользователей.

6.9. Организация учёта носителей персональных данных

6.9.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

6.9.2. Учёт выдаваемых носителей персональных данных ведётся в «Журнале учёта носителей персональных данных». Учёт осуществляется лицом, назначенным ответственным за безопасность персональных данных, если нормативными документами Управления не предусмотрено иного. Сотрудники Управления получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

6.9.3. Запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

6.10. Организация учёта средств защиты информации

6.10.1. Все используемые в Управлении средства защиты подлежат учёту. Каждому экземпляру средства защиты присваивается уникальный номер. На программно-аппаратных средствах защиты данный номер указывается на корпусе изделия. На программных СЗИ – на упаковке.

6.10.2. Учёт средств защиты информации ведётся в «Журнале учёта СЗИ». Учёт осуществляется лицом, назначенным ответственным за безопасность персональных данных, если нормативными документами Управления не предусмотрено иного.

6.11. Контроль доступа пользователей к АРМ и ресурсам сети Управления:

6.11.1. В компьютерной вычислительной сети Управления должны обеспечиваться: идентификация, аутентификация, авторизация, управление доступом, контроль целостности, регистрация, включая:

- функционирование системы парольной защиты АРМ и КВС Управления;
- контроль доступа пользователей к ресурсам АРМ и/или КВС Управления;
- непротиворечивая и прозрачная административно-техническая поддержка задач управления доступом к ресурсам АРМ и/или КВС Управления.

6.11.2. Назначение/лишение полномочий по доступу сотрудников к ресурсам АРМ и/или сети санкционируется руководителем структурного подразделения Управления, несущего персональную ответственность за обеспечение безопасности информации в данном подразделении.

6.11.3. Системный администратор не должен иметь служебных полномочий (а при возможности и технических средств) по настройке параметров системы, влияющих на полномочия пользователей по доступу к информации. Однако он должен иметь право добавить в систему нового пользователя без полномочий по доступу к информации, а также удалить из системы такого пользователя.

6.11.4. Ответственный за информационную безопасность должен иметь служебные полномочия и технические возможности по контролю действий соответствующих системных администраторов (без вмешательства в их действия) и пользователей, а также полномочия (а при возможности и технические средства) по настройке для каждого пользователя параметров системы, которые определяют права доступа к информации.

6.11.5. Ответственный за информационную безопасность не должен иметь права добавить нового пользователя, а также удалить из него существующего пользователя.

6.11.6. Права доступа пользователей к ресурсам КВС Управления назначаются ответственным за информационную безопасность в соответствии с «Матрицей доступа».

6.11.7. Для каждого пользователя заводится отдельная учетная запись.

6.11.8. Учетные записи пользователей делятся на 3 категории: администраторы безопасности, администраторы и пользователи.

Администраторы:

- учетная запись используется сотрудниками службы, осуществляющей поддержку функционирования оборудования КВС Управления и средств ее защиты;
- администраторы имеют доступ ко всем штатным средствам настройки программно-аппаратного комплекса КВС Управления;
- администраторы не имеют права доступа к системным журналам, политикам аудита штатного ПО и СЗИ.

Пользователи:

- учетная запись используется всеми сотрудниками, АРМ которых подключены к КВС Управления;
- пользователи имеют право на использование ПО, установленного на АРМ;

- пользователи не имеют права установки дополнительного ПО без согласования с ответственным за информационную безопасность и системным администратором.

Администраторы безопасности:

- учетная запись используется ответственным за информационную безопасность;
- администраторы безопасности имеют доступ ко всем штатным средствам настройки СЗИ Управления;
- администраторы безопасности имеют права доступа к системным журналам, политикам аудита штатного ПО и СЗИ.

6.11.9. Учетные записи сотрудников, которые прекратили работу в Управлении, должны блокироваться. Удаление таких учетных записей должно осуществляться не ранее, чем через 6 месяцев.

6.11.10. Доступ пользователей к АРМ и КВС Управления осуществляется с использованием средств парольной защиты, в соответствии с инструкцией по организации парольной защиты.

6.12. Мониторинг системы защиты информации

6.12.1. Мониторинг СЗИ должен проводиться ответственным за информационную безопасность с целью обнаружения и регистрации отклонений защитных мер от требований обеспечения безопасности информации и оценки полноты реализации требований данного Положения.

6.12.2. Основной целью мониторинга СЗИ является оперативное и постоянное наблюдение, сбор, анализ и обработка данных, необходимых для решения следующих задач:

- контроль за реализацией положений нормативных актов по обеспечению безопасности информации Управления;
- выявление нештатных (или злоумышленных) действий в КВС Управления ;
- выявление потенциальных нарушений безопасности информации.

6.12.3. Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

6.12.4. В СЗИ должен вестись журнал регистрации действий пользователей. Журнал ведется в электронной форме, при необходимости, с использованием штатных средств ОС.

6.12.5. Должна осуществляться регистрация попыток входа пользователей в систему.

Регистрируются следующие параметры:

- дата и время попытки;

- результат попытки входа (успешная, неуспешная);
- идентификатор пользователя, предъявленный при попытке;
- пароль, предъявленный при неуспешной попытке.

6.12.6. Должна осуществляться регистрация попыток доступа к защищаемым файлам.

Регистрируются следующие параметры:

- дата и время попытки доступа;
- результат попытки (успешная, неуспешная);
- идентификатор пользователя — субъекта доступа.

6.12.7. Действия пользователей с полномочиями администраторов также должны подвергаться регистрации. Следующие действия администраторов должны протоколироваться:

- создание, модификация, удаление объектов;
- модификация прав доступа и привилегий пользователей;
- модификация правил доступа к информационным ресурсам;
- запуск (остановка) сетевых сервисов;
- изменение параметров аудита.

6.12.8. События, дополнительно подлежащие регистрации, устанавливаются отдельно для различных пользователей, групп пользователей, информационных ресурсов.

6.12.9. Журнал регистрации должен быть защищен от несанкционированного доступа и изменений.

Должно осуществляться резервное копирование данных журнала регистрации.

Должно быть настроено оперативное оповещение ответственного за информационную безопасность при регистрации критических событий нарушения безопасности.

Ответственный за информационную безопасность должен регулярно просматривать и анализировать данные журнала регистрации.

6.13. Антивирусная защита

6.13.1. Антивирусная защита информационных систем персональных данных производится согласно документу «Инструкция по организации антивирусной защиты ИСПДн».

6.14. Межсетевое экранирование

6.14.1. Подключение к сети Интернет должно осуществляться по выделенному каналу, защищенному межсетевым экраном (МЭ).

6.14.2. МЭ администрируется ответственным за информационную безопасность локально или удаленно (только из КВС Управления с АРМ ответственного за информационную безопасность).

6.14.3. Должна обеспечиваться регистрация загрузки, инициализации системы и остановки работы МЭ.

6.14.4. Межсетевой экран должен быть корректно настроен, чтобы обеспечивать:

- фильтрацию трафика, поступающего со стороны внешней сети на сетевом, транспортном и прикладном уровне;
- трансляцию сетевых адресов при взаимодействии с внешней сетью;
- противодействие попыткам определения топологии КВС Управления, активности оборудования, запущенных сетевых служб;
- противодействие атакам типа «отказ в обслуживании»;
- блокировку иных дестабилизирующих воздействий со стороны внешней сети;
- регистрацию попыток подключения со стороны внешней сети и регистрацию этих данных в своем журнале аудита.

6.14.5. МЭ должен содержать средства контроля целостности своей программной и информационной части.

6.14.6. МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление заданных свойств.

6.14.7. МЭ должен обеспечивать достаточную пропускную способность и отказоустойчивость.

6.14.8. Межсетевое экранирование должно применяться при организации защиты периметра КС и серверного сегмента (внутренних серверов).

6.15. Электронная почта, web-сервер

6.15.1. Ресурсы сети Интернет в Управлении могут использоваться для ведения деловой переписки, получения и распространения информации, связанной с деятельностью Управления (путем создания информационных web-сайтов), информационно-аналитической работы в интересах Управления, обмена почтовыми сообщениями, обусловленного служебной необходимостью. Иное использование ресурсов сети Интернет, решение о котором не принято руководством Управления в установленном порядке, должно рассматриваться как нарушение безопасности информации.

6.15.2. При взаимодействии с сетью Интернет обязательно должны применяться соответствующие сертифицированные средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации (СКЗИ) и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

6.15.3. Запрещается передавать ПДн через открытые соединения с сетью Интернет, в том числе по электронной почте без шифрования такой информации (за исключением случаев передачи обезличенных или общедоступных ПДн).

6.16. Криптографическая защита

6.16.1. Обработка персональных данных высокой категории должна вестись с использованием криптографических средств.

6.16.2. Средства криптографической защиты информации:

- должны допускать встраивание в действующую технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным ПО на уровне обработки запросов на криптографические преобразования и выдачи результатов;
- должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- должны быть реализованы на основе алгоритмов, соответствующих национальным стандартам РФ, условиям договора с контрагентом и (или) стандартам Управления;
- должны иметь строгий регламент использования ключей, предполагающий контроль со стороны ответственного за информационную безопасность за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);
- не должны содержать требований к ЭВМ по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
- не должны требовать дополнительной защиты от утечки по ПЭМИН.

6.16.3. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения.

6.16.4. Безопасность процессов изготовления ключевых документов СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

6.16.5. Внутренний порядок применения СКЗИ определяется руководством Управления и должен включать:

- порядок ввода в действие;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой системой;
- порядок обращения с носителями ключевой информации.

7. Ответственность

7.1. Все сотрудники Управления, допущенные в установленном порядке к работе с защищаемой информацией, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности такой информации и соблюдение правил работы с ней, установленных данным Положением и иными организационно-распорядительными документами Управления, разработанными на его основе.

7.2. Ответственность за доведение требований настоящего Положения до сотрудников Управления и обеспечение мероприятий по их реализации несет руководство Управления.

7.3. Все сотрудники Управления обязаны неукоснительно соблюдать относящиеся к ним требования настоящего Положения.

7.4. Отказ соблюдать настоящее Положение может подвергнуть защищаемую информацию Управления недопустимому риску потери целостности, доступности, актуальности или конфиденциальности при ее хранении, обработке или передаче.

7.5. Нарушения сотрудниками Управления положений, инструкций, руководств и иных организационно-распорядительных документов, поддерживающих данное Положение, будут рассматриваться руководством Управления в административном порядке и нарушители будут привлекаться к ответственности в установленном действующим законодательством порядке.

8. Порядок проведения разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации

8.1. По каждому невыполнению предписанных мероприятий по защите ПДн для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

8.2. Для проведения расследования назначается комиссия с привлечением ответственного за информационную безопасность.

8.3. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению.

8.4. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

9. Порядок приостановки предоставления доступа к персональным данным пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных

9.1. По каждому невыполнению предписанных мероприятий по защите персональных данных проводится расследование.

9.2. Доступ к хранилищу и системе обработки персональных данных закрывается ответственным за информационную безопасность вплоть до выяснения обстоятельств нарушения порядка предоставления данных и устранения причин невыполнения предписанных мероприятий по защите персональных данных.

9.3. После окончания расследования и устранении причин утечки информации руководитель комиссии по расследованию принимает решение об открытии доступа к хранилищу ПДн и системам обработки персональных данных.

10. Законодательная и нормативная база

Конституция Российской Федерации от 12.12.1993 г.;

Федеральный закон Российской Федерации от № 149-ФЗ 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации № 152-ФЗ от 27.07.2006 г. «О персональных данных»;

Федеральный закон Российской Федерации от 25.07.2011 г. «О внесении изменений в Федеральный закон «О персональных данных»;

Постановление Правительства Российской Федерации № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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