Приложение № 1
к приказу Департамента социальной защиты
населения Ивановской области

от 03.06.2015 № 216 - о.д.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн)

Термины и определения

Автоматизированная система	- Система, состоящая из работников (лиц, замещающих должности государственной гражданской службы в Департаменте социальной защиты населения Ивановской области) и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Администратор безопасности информации	- Должностное лицо (работник), ответственный за защиту информации, он же может быть ответственным за обеспечение безопасности персональных данных в информационной системе (работник, назначенный приказом руководителя), ответственный за защиту информационных систем персональных данных от несанкционированного доступа к информации
Администратор информационной системы	- Администратор автоматизированной системы, администратор локальной вычислительной сети, администратор баз данных, администратор информационного ресурса - ответственный за функционирование информационной системы персональных данных в установленном штатном режиме работы (работники назначенные приказом руководителя)
Блокирование персональных данных	- Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Обладатель информации (информационного ресурса)	- Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Структурное подразделение Департамента социальной защиты населения Ивановской области, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Обладатель устанавливает в пределах своей компетенции режим и правила обработки информации, зашиты информационного ресурса, доступа к информационному ресурсу, условия копирования и тиражирования информационного ресурса (в распоряжении на создание информационного ресурса или в виде отдельных регламентов)
Доступ к информации	- Возможность получения информации и ее использования
Информационная система персональных данных (ИСПДн)	- Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Инцидент информационной	- Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми

безопасности	связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности (отказ в обслуживании, сбор информации, несанкционированный доступ и т.д.)
Контролируемая зона	- Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей организации, а также транспортных, технических и иных материальных средств
Конфиденциальность персональных данных	- Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания
Несанкционированный доступ (несанкционированные действия)	- Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам
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 (в настоящем Положении – Департамент социальной защиты населения Ивановской области.
Организационно-распорядительная документация ИСПДн	- Документация, регламентирующая деятельность работников в области защиты конфиденциальной информации и персональных данных, а также требования к ИСПДн в соответствии с требованиями законодательства Российской Федерации
Персональные данные	- Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	- Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Распространение персональных данных	- Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Руководящие документы по безопасности информации	- Нормативно-правовые и методические документы ФСТЭК России и ФСБ России, регулирующие деятельность в области защиты информации
Технические средства, позволяющие осуществлять обработку персональных данных	- Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

	документов и другие 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 информационной системе
Субъект доступа (субъект)	- Лицо или процесс, действия которого регламентируются правилами разграничения доступа
Угроза безопасности персональных данных	- Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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

Перечень сокращений

АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
ЗИ	- защита информации
ИБ	- информационная безопасность
ИР	- информационный ресурс
ИС	- информационная система
ИСПДн	- информационная система персональных данных
ИТ	- информационная технология
МЭ	- межсетевой экран
НСД	- несанкционированный доступ
ОС	- операционная система
ПДн	- персональные данные
ПО	- программное обеспечение
Положение	- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн
СВТ	- средство вычислительной техники
СЗИ	- средство защиты информации
СЗПДн	- система защиты персональных данных
СКЗИ	- средство криптографической защиты информации
СТР-К	- «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282
ТС	- техническое средство
ФСБ	- Федеральная служба безопасности
ФСТЭК	- Федеральная служба по техническому и экспортному контролю

1. Общие положения

Настоящее Положение регламентирует вопросы обеспечения безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) и иной, охраняемой законами Российской Федерации информации в Департаменте социальной защиты населения Ивановской области (далее также – Учреждение) и определяет порядок организации работ по созданию и эксплуатации системы защиты персональных данных (СЗПДн) и иной охраняемой информации.

Настоящее Положение разработано на основании следующих основных нормативных правовых актов и документов в области обеспечения безопасности информации и ПДн:

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

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

- постановление Правительства Российской Федераций от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

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

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрирован в Минюсте России 31 мая 2013 г. № 28608);

- приказ ФСТЭК России 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» (Зарегистрирован в Минюсте России 14 мая 2013 г. № 28375);

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282.

Действие настоящего Положения не распространяется на вопросы, связанные с обработкой ПДн, осуществляемой без использования средств автоматизации. Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения определяются в отдельном документе с учетом требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства Российской Федерации от 15.09.2008 № 687.

2. Порядок организации и проведения работ по обеспечению безопасности информации и ПДн при их обработке в информационных системах и ИСПДн

Под организацией работ по обеспечению безопасности информации и ПДн при их обработке в информационных системах (ИС) и ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИС и ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности информации и ПДн в ИС и ИСПДн, восстановление нормального

функционирования ИС и ИСПДн после нейтрализации угрозы с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Организация работ по защите информации и ПДн предусматривает формирование:

- перечня информации и ПДн, обрабатываемых в информационной системе;

- порядка классификации ИС как ИСПДн;

- порядка разработки, ввода в действие и эксплуатации ИС и ИСПДн в части реализации мероприятий по обеспечению безопасности информации и ПДн;

- порядка взаимодействия между ответственными за обеспечение безопасности информации и ПДн и эксплуатирующими подразделениями (пользователями) по вопросам обеспечения безопасности информации и ПДн;

- порядка привлечения структурных подразделений Учрежения и специализированных сторонних организаций к разработке и эксплуатации СЗПДн, их задачи и функции на различных стадиях создания и эксплуатации ИС и ИСПДн в соответствии с требованиями Руководящих документов по безопасности с учетом механизмов, предусмотренных Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

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

- порядка контроля обеспечения требуемого уровня защищенности информации и ПДн.

Согласование подключений сторонних организаций к сети Учреждения осуществляется после согласования схемы подключения, подписания договора на использование ИР между Учреждением и сторонней организацией и соглашения о взаимодействии между такой сторонней организацией и Учреждением.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности информации и ПДн при их обработке в ИС и ИСПДн ответственным за обеспечение безопасности информации и ПДн соответствующим приказом начальника Департамента социальной защиты населения Ивановской области назначается должностное лицо (работник) – Администратор безопасности информации.

Непосредственно исполнение работ по защите информации (ПДн) в ИС (ИСПДн) с использованием средств автоматизации возлагается на начальников структурных подразделений Учреждения, ответственных за развитие и использование (эксплуатацию) ИСПДн.

Для проведения классификации ИСПДн соответствующим приказом начальника Департамента социальной защиты населения Ивановской области назначается специальная внутренняя комиссия (рабочая группа). В состав этой комиссии (группы) включаются представители структурных подразделений - обладателей информационных ресурсов.

Для придания необходимого статуса рабочей группе могут издаваться соответствующие распоряжения начальника Учреждения, в которых, в частности, даются указания всем начальникам структурных подразделений об оказании содействия и необходимой помощи в работе комиссии (рабочей группе) при проведении работ. Для оказания помощи на время работы группы в подразделениях начальниками этих структурных подразделений выделяются работники, владеющие детальной информацией по вопросам обработки информации и ПДн в данных подразделениях.

Проведение обследования ИС (ИСПДн), разработка и реализация СЗПДн могут осуществляться как работниками Учреждения, так и на договорной основе с другими специализированными организациями, имеющими соответствующие лицензии на деятельность по технической защите конфиденциальной информации в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Научно-техническое и методическое руководство, непосредственная организация работ по созданию (модернизации) СЗПДн и контроль за эффективностью использования предусмотренных мер возлагается на специалиста по информационной безопасности.

В случае разработки СЗПДн или ее отдельных компонентов специализированными организациями специалист по информационной безопасности (Администратор безопасности информации) отвечает за организацию и проведение мероприятий по защите информации.

Разработка, внедрение и эксплуатация СЗПДн осуществляются во взаимодействии разработчика с Администратором безопасности информации.

Контроль за реализацией проектных решений возлагается на начальника Департамента социальной защиты населения Ивановской области.

2.1. Порядок определения защищаемой информации и классификации ИС (ИСПДн)

Внутренней комиссией (рабочей группой), образованной приказом начальника Учреждения, для каждой ИС (ИСПДн) определяется перечень информации (ПДн), уточняются цели и основание обработки информации (ПДн), а также срок хранения и условия прекращения обработки.

Целью классификации ИС (ИСПДн) является определение по её результатам перечня обоснованных организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности информации (ПДн) с учётом особенностей конкретной ИС (ИСПДн).

Классификация может проводиться на этапе создания ИС (ИСПДн) или в ходе её эксплуатации (для ранее введенной в эксплуатацию и (или) модернизируемой ИС (ИСПДн)).

Классификация ИС (ИСПДн) осуществляется в соответствии с требованиями, установленными постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России 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».

Классификация ИС (ИСПДн) проводится внутренней комиссией (рабочей группой) и включает в себя следующие этапы:

- сбор и анализ исходных данных по ИС (ИСПДн);

- присвоение ИС (ИСПДн) соответствующего класса и его документальное оформление.

При проведении классификации ИС (ИСПДн) внутренней комиссией (рабочей группой) определяется:

- заданные Учреждением характеристики безопасности информации (ПДн), обрабатываемых в ИС (ИСПДн);

- структура ИС (ИСПДн);

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

- режим обработки информации (ПДн);

- режим разграничения прав доступа пользователей ИС (ИСПДн);

- местонахождение технических средств ИС (ИСПДн).

В случае выделения в составе ИС (ИСПДн) подсистем, каждая из которых является ИС (ИСПДн), ИС (ИСПДн) в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем, если данные ИС (ИСПДн) не разделены между собой МЭ.

Предложения комиссии (рабочей группы) по отнесению ИС (ИСПДн) к определенному классу согласовываются с начальником Учреждения.

Результаты классификации АС оформляются актом, утверждаемым начальником Учреждения, в соответствии с Приложением № 1 к Специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР-К), утвержденным приказом Гостехкомиссии России от 30.08.2002 № 282.

Сформированные по результатам классификации материалы являются неотъемлемой частью организационно-распорядительной документации ИС (ИСПДн) и относятся к информации конфиденциального характера. Оригиналы организационно-распорядительной документации ИС (ИСПДн) хранятся у лица, ответственного за организацию работ по защите информации (ПДн).

Класс ИС (ИСПДн) может быть пересмотрен комиссией (рабочей группой) в установленном порядке в следующих случаях:

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

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности информации (ПДн) при их обработке в ИС (ИСПДн).

2.2. Порядок разработки, ввода в действие и эксплуатации СЗИ

Для обеспечения защиты информации, содержащейся в ИС (ИСПДн), проводятся следующие мероприятия:
- формирование требований к защите информации, содержащейся в ИС (ИСПДн);
- разработка системы защиты информации ИС (ИСПДн);
- внедрение системы защиты информации ИС (ИСПДн);
- аттестация ИС (ИСПДн) и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной ИС (ИСПДн);
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС (ИСПДн) или после принятия решения об окончании обработки информации.

2.3. Порядок привлечения структурных подразделений и специализированных сторонних организаций к разработке и эксплуатации ИС (ИСПДн), их задачи и функции на различных стадиях создания и эксплуатации ИС (ИСПДн)

Для организации и обеспечения безопасности информации (ПДн) при их обработке в ИС (ИСПДн) лицом, ответственным за обеспечение безопасности информации (ПДн)

соответствующим приказом начальника Учреждения назначается должностное лицо (работник) – Администратор безопасности информации.

Администратор безопасности информации обеспечивает методическое руководство, разработку требований к мерам защиты ИС (ИСПДн) и контроль за эффективностью использования предусмотренных мер защиты информации.

Администратор безопасности информации обеспечивает подготовку предложений по совершенствованию и реализации положений Политики информационной безопасности ИС (ИСПДн) и контролирует выполнение установленных требований в структурных подразделениях Учреждения.

Администратор безопасности информации осуществляет следующие основные функции:

- разрабатывает предложения по определению класса защищенности объектов ИС (ИСПДн) и автоматизированной системы (АС);

- участвует в организации работ по выявлению актуальных угроз безопасности информации (ПДн);

- осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите информации (ПДн) и разработке технического (частного технического) задания на создание СЗИ(ПДн);

- согласовывает выбор конкретных средств обработки информации (ПДн), технических и программных средств защиты;

- осуществляет контроль реализации проектных решений на создание СЗИ(ПДн);

- участвует в организации работ по оценке соответствия ИС (ИСПДн) предъявляемым требованиям по обеспечению безопасности информации (ПДн);

- участвует в организации разработки организационно-распорядительной документации по защите информации в ИС (ИСПДн);

- проводит контроль требуемого уровня обеспечения защищенности информации (ПДн) при эксплуатации СЗИ(ПДн), в том числе контроль соблюдения условий использования СЗИ(ПДн);

- участвует в организации обучения должностных лиц (работников) – пользователей ИС (ИСПДн), ответственных за эксплуатацию СЗИ(ПДн), по направлению обеспечения безопасности информации (ПДн);

- участвует в организации охраны и физической защиты помещений Учреждения, в которых размещаются средства обработки информации (ПДн), исключающих несанкционированный доступ к техническим средствам ИС (ИСПДн), их хищение и нарушение работоспособности, хищение носителей информации;

- оказывает методическую помощь должностным лицам (работникам) Учреждения.

Администратор безопасности информации разрабатывает правила работы с информацией, техническими средствами и правила использования информации (ПДн) в соответствии с возможностями, функциями, предназначением и степени защищенности этих средств, ресурсов и требованиям к защите и доступности информации (ПДн), осуществляет предоставление ИТ - сервисов всем структурным подразделениям Учреждения, отвечает за их целостность и доступность, обеспечивает разграничение доступа к информации (ПДн_ в процессе их использования, контроль над ходом информационных процессов.

Привлечение для разработки СЗИ(ПДн) или ее отдельных компонентов сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными и организационно-распорядительными документами ФСТЭК России и ФСБ России.

В случае привлечения для обеспечения безопасности информации (ПДн) сторонних специализированных организаций в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» рекомендуется выполнение следующих условий:

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

- оформление соглашения о неразглашении конфиденциальных сведений;

- проведение инструктажа исполнителей работ по вопросам ИБ;

- другие условия, устанавливаемые соответствующими нормативными и организационно-распорядительными документами.

При привлечении сторонних специализированных организаций работникам следует учитывать следующие функции в техническом задании:

а) формирование требований к защите информации, содержащейся в информационной системе:

- уточнение перечня информации (ПДн), подлежащих защите;

- определение условий расположения ИС (ИСПДн) относительно границ контролируемой зоны;

- определение конфигурации и топологии ИС (ИСПДн) в целом, и ее отдельных компонент, физические, функциональные и технологические связи как внутри ИС (ИСПДн), так и с другими системами различного назначения;

- определение технических средств и систем, включаемых в состав ИС (ИСПДн), условий их расположения, общесистемных и прикладных программных средств;

- определение режимов обработки информации (ПДн) в ИС (ИСПДн);

- разработка предложений по уточнению класса защищенности ИС (ИСПДн);

- уточнение степени участия работников в обработке информации (ПДн), характера их взаимодействия между собой;

- определение (уточнение) угроз безопасности информации (ПДн) с учётом конкретных условий функционирования ИС (ИСПДн), разработка проекта частной модели угроз;

- участие в разработке (согласовании) конкретных требований по защите информации (ПДн) и разработке технического (частного технического) задания на создание СЗИ(ПДн).

б) разработка системы защиты информации информационной системы (ИСПДн):

- разработка технического проекта на создание СЗИ(ПДн) в соответствии с требованиями руководящих документов ФСТЭК России и ФСБ России;

- монтажные работы в соответствии с проектной документацией;

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

- организация сертификации по требованиям безопасности информации программных СЗИ в случае, когда на рынке отсутствуют требуемые сертифицированные СЗИ;

- разработка разрешительной системы доступа пользователей к информации (ПДн), обрабатываемым в ИС (ИСПДн);

- разработка (в согласованном объеме) эксплуатационной документации на СЗИ(ПДн).

в) внедрение системы защиты информации:

- установка СЗИ;

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

- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;

- оценка соответствия ИС (ИСПДн) требованиям безопасности информации (ПДн).

3. Основные требования и правила по обеспечению безопасности информации (ПДн) при их обработке в ИС (ИСПДн)

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

Основными направлениями защиты информации (ПДн) являются:

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

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

Основными мерами защиты информации (ПДн) являются:

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

- ограничение доступа пользователей в помещения, в которых размещены технические средства (ТС), позволяющие осуществлять обработку информации (ПДн), а также в которых хранятся машинные носители информации;

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

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа (НСД) и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение машинных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование ТС, дублирование массивов и носителей информации;

- использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;

- использование защищенных каналов связи;

- размещение ТС, позволяющих осуществлять обработку информации (ПДн) в пределах охраняемой территории;

- использование ТС, удовлетворяющих требованиям стандартов по электромагнитной совместимости, безопасности, санитарным нормам, предъявляемым к видеодисплейным терминалам;

- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах охраняемой территории;

- обеспечение развязки цепей электропитания ТС с помощью защитных фильтров, блокирующих (подавляющих) информационный сигнал;

- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных ТС и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация;

- размещение дисплеев и других средств отображения информации, исключающее её несанкционированный просмотр;

- организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку информации (ПДн);

- предотвращение внедрения в ИС (ИСПДн) вредоносных программ (программ-вирусов) и программных закладок.

Для обеспечения безопасности информации (ПДн) от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД в зависимости от класса ИС (ИСПДн), заданных характеристик безопасности обрабатываемой информации (ПДн), угроз безопасности информации (ПДн), структуры ИС (ИСПДн), наличия межсетевого взаимодействия и режимов обработки информации (ПДн) в рамках СЗИ от НСД реализуются функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Перечень мер по защите информации от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи применяются по решению начальника Учреждения.

Применяемые СЗИ учитываются в Журнале учета СЗИ. В случае проведения аттестации ИС (ИСПДн), учёт применяемых технических СЗИ ведется в документе «Технический паспорт ИС (ИСПДн)» в соответствии с требованиями СТР-К.

3.1. Требования по организации разрешительной системы доступа пользователей к обрабатываемой в ИС (ИСПДн) информации

Данный раздел Положения регламентирует порядок взаимодействия подразделений Учреждения по обеспечению безопасности информации (ПДн) при организации разрешительной системы доступа к сервисам и ресурсам ИС (ИСПДн).

Разрешительная система доступа к обрабатываемой в ИС (ИСПДн) информации предусматривает установление единого порядка обращения со сведениями, содержащими

защищаемую информацию (ПДн) и их носителями, определяет степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности информации (ПДн) и включает:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;

- определение порядка изменения правил доступа к защищаемой информации;

- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

- контроль функционирования разрешительной системы доступа и расследование фактов неправомерного доступа лиц к защищаемой информации, в случае выявления таковых;

- оценку эффективности проводимых мер по исключению утечки информации;

- организацию деятельности должностных лиц, ответственных за подготовку предложений о внесении изменений в должностные обязанности и иные документы, определяющие задачи и функции работников ИС (ИСПДн);

- разработку внутренних организационно-распорядительных документов, определяющих порядок реализации и функционирования разрешительной системы доступа.

Основные условия правомерного доступа работников Учреждения к обрабатываемой в ИС (ИСПДн) информации включают в себя:

- подписание работником Учреждения обязательства о неразглашении конфиденциальной информации;

- наличие у работника Учреждения оформленного в установленном порядке права доступа к информации (ПДн), обрабатываемым в ИС (ИСПДн);

- наличие утвержденных в соответствии с трудовым законодательством Российской Федерации, должностных (функциональных) обязанностей работника, определяющих круг его задач и объем необходимой для их решения информации.

Лица, доступ которых к информации (ПДн), обрабатываемым в ИС (ИСПДн), необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующей информации (ПДн) на основании Списка должностей работников с указанием методов управления доступом, типа доступа и правил доступа, утвержденного начальником Учреждения.

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

В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками.

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от

имени системных учетных записей.

К внутренним пользователям в целях настоящего документа, относятся должностные лица (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС (ИСПДн) в соответствии с утвержденными должностными регламентами (инструкциями) и которым в ИС (ИСПДн) присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ИСПДн) информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами Учреждения и которым в ИС (ИСПДн) также присвоены учетные записи.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

Аутентификация пользователя осуществляется с использованием паролей.

В ИС (ИСПДн) должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

При регистрации и назначении прав доступа пользователей ИС (ИСПДн) Учреждения выполняются следующие требования:

- каждому пользователю присваивается уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать;

- учётные записи всех пользователей привязываются к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты ИС (ИСПДн);

- при регистрации пользователей проводится проверка соответствия уровня доступа возложенным на пользователя задачам (вмененным обязанностям);

- назначенные пользователю права доступа документируются;

- пользователь знакомится под роспись с предоставленными ему правами доступа и порядком его осуществления;

- в ИС (ИСПДн) предусматривается разрешение доступа к сервисам только аутентифицированным пользователям;

- при внесении нового пользователя разрабатывается и обновляется формальный список всех пользователей, зарегистрированных для работы в ИС (ИСПДн);

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

- администраторами ИС (ИСПДн) проводится удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы недоступны другим пользователям.

Контроль выполнения требований разрешительной системы доступа к информации (ПДн) возлагается на Администратора безопасности информации.

Доступ к ИР ИС (ИСПДн) сторонних организаций (правоохранительных органов, судебных органов, органов статистики, органов исполнительной и законодательной власти субъектов Российской Федерации) регламентируется законодательством Российской Федерации, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

Порядок доступа к ИР ИС (ИСПДн) сторонних организаций, выполняющих работы на договорной основе, определяется в договоре на выполнение работ (оказание услуг) в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Обязательным условием договора является заключение соглашения об обеспечении безопасности персональных данных и их конфиденциальности.

Использование дополнительных типов устройств, необходимых для использования в информационной системе возможно, только после утверждения начальником Учреждения перечня типов устройств, подлежащих идентификации и аутентификации, до начала информационного обмена.

3.2. Требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены средства ИС (ИСПДн)

Данный раздел Положения содержит общие требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, в которых размещены ИС (ИСПДн):

1. Организуется контроль доступа работников и посетителей в помещения Учреждения, в которых установлены ТС ИС (ИСПДн) и осуществляется обработка информации (ПДн), а также хранятся машинные носители информации (ПДн).

2. Доступ работников структурных подразделений Учреждения в помещения, в которых осуществляется обработка информации (ПДн), организовывается на основании списков (перечней), утверждаемых начальником Учреждения. Доступ других работников Учреждения и посетителей в эти помещения осуществляется в сопровождении ответственных должностных лиц.

При этом время и дата их посещения и выхода протоколируются подразделением по охране объекта в специальном журнале учета посетителей или с применением ТС контроля физического доступа.

3. Для защиты помещений, в которых расположены ТС ИС (ИСПДн), принимаются меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

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

5. Обеспечивается размещение устройств вывода информации средств вычислительной техники, дисплеев АРМ ИС (ИСПДн) таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей охраняемую информацию (ПДн).

6. Работникам Учреждения запрещается подключать к сети неучтенные машинные носители информации.

3.3. Правила обеспечения безопасности информации (ПДн) при использовании машинных носителей информации

3.3.1. Правила обращения с машинными носителями информации

В информационной системе допускается использование только учтённых, установленным порядком, съемных носителей информации.

К машинным носителям информации относятся: флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства.

При этом должны соблюдаться установленные правила управления доступом к объектам доступа, методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа в соответствии с функциональными обязанностями (решаемыми задачами).

При обращении с машинными носителями информации выполняются следующие основные правила:

- машинные носители информации учитываются и выдаются пользователям под роспись и защищены;

- машинные носители информации, срок эксплуатации которых истек, уничтожаются установленным порядком;

- для выноса машинных носителей информации за пределы объектов Учреждения дается специальное разрешение, а факт выноса фиксируется;

- все машинные носители информации хранятся в безопасном месте в соответствии с требованиями по их эксплуатации;

- мониторинг за использованием машинных носителей информации осуществляется постоянно руководителями структурных подразделений, в которых установлены ресурсы ИС (ИСПДн), Администратором безопасности информации и Администратором информационной системы.

Администратор информационной системы обеспечивает запрет запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с машинным носителем информации.

Ответственным за хранение, учет и выдачу машинных носителей информации (ПДн) является Администратор безопасности информации.

3.3.2. Порядок учёта носителей информации

Все находящиеся на хранении и в обращении машинные носители информации поэкземплярно учитываются в Журнале учета машинных носителей конфиденциальной информации и персональных данных.

Учёту подлежат:

- машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинные носители информации, встроенные в корпус средств вычислительной техники

(накопители на жёстких дисках).

Учёт машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учёта, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учёт встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учёта в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учёта машинных носителей информации или журналы материально-технического учёта с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учёту в журналах учёта подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съёмные жесткие диски).

Каждый носитель, с записанной на нём информацией (ПДн), имеет этикетку, на которой указывается метка машинного носителя и гриф.

Пользователи ИС (ИСПДн) для выполнения работ получают учтённый машинный носитель информации от ответственного работника Учреждения. При получении делаются соответствующие записи в Журнале учёта.

После окончания работ пользователь ИС (ИСПДн) сдает машинный носитель информации ответственному работнику Учреждения для хранения, о чем делается соответствующая запись в Журнале учёта.

При наличии личного сейфа у пользователя ИС (ИСПДн) допускается хранение учтённых машинных носителей информации в личных сейфах (металлических шкафах), опечатанных печатью пользователя ИС (ИСПДн).

Хранение машинных носителей информации (ПДн) осуществляется в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на машинном носителе информации (ПДн) хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

3.3.3. Порядок доступа к машинным носителям информации

Порядок доступа к машинным носителям информации в Учреждении заключается в определении должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

- съёмным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры,

звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жёстких дисках);

- предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

3.3.4. Порядок уничтожения машинных носителей информации

Уничтожение (стирание) информации на машинных носителях информации обеспечивается при их передаче между пользователями, в сторонние организации для ремонта или утилизации и должно исключать возможность восстановления защищаемой информации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съёмных и несъёмных машинных носителях информации.

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

Уничтожение машинных носителей информации (ПДн) осуществляется комиссией по уничтожению, назначенной начальником Учреждения.

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

Бумажные носители данных уничтожаются через термическую обработку (сжигание) или с использованием специальных устройств - шредеров.

Перед утилизацией оборудования, участвующего в обработке информации (ПДн), Администратором информационной системы осуществляется проверка всех его компонентов, включая машинные носители информации (жёсткие диски) на отсутствие защищаемой информации (ПДн) и лицензированного программного обеспечения (ПО).

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

3.4. Порядок и правила использования паролей пользователей

Организационное и техническое обеспечение смены, прекращения действия паролей в ИС (ИСПДн), процессов генерации и использования возлагается в пределах своих полномочий на Администратора безопасности информации и Администратора информационной системы, сопровождающего механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

При использовании паролей в ИС (ИСПДн) выполняются следующие правила:

- пароли обязаны меняться с установленной периодичностью в соответствии с требованиями, установленными в Департаменте социальной защиты населения Ивановской области;

- пароль имеет не менее 6 символов и содержит буквенные и цифровые символы;

- обязательно применение индивидуальных паролей;

- применение групповых паролей не допускается;

- при создании пароля пользователя администратором предусматривается его автоматическое изменение самим пользователем после первого же его входа в ИС (ИСПДн);

- для предотвращения повторного использования паролей ведется их учёт (запись) за предыдущие 12 месяцев;

- при вводе пароль не выдается на монитор компьютера в явном виде;

- пароли могут храниться только на АРМ владельца пароля в зашифрованном виде с использованием стойких алгоритмов шифрования. Файл с паролями хранится отдельно от системных приложений;

- рекомендуется использование возможностей операционной системы (ОС) по контролю за периодичностью смены (не реже 1 раза в 3 месяц), составу символов и недопущению повторений паролей.

Контроль за действиями пользователей ИС (ИСПДн) при работе с паролями возлагается на Администратора безопасности информации в пределах своих полномочий.

При использовании паролей запрещается:

- использовать в качестве пароля свои имя, фамилию, дату рождения, имена родственников, кличку собаки и т. п., равно как и обычные слова;

- использовать в качестве пароля русское слово, введенное при нахождении клавиатуры в латинском регистре;

- использовать в качестве пароля легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ), а также общепринятые сокращения;

- использовать в качестве пароля «пустой» пароль, имя входа в систему, а также выбирать пароли, которые уже использовались ранее;

- использовать один и тот же пароль при загрузке АРМ и при работе в ИС (ИСПДн);

- записывать пароль на неучтённых бумажных носителях информации;

- разглашать кому бы то ни было свои персональные пароли доступа.

В ИС (ИСПДн) должно обеспечиваться автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем трех неуспешных попыток входа в информационную систему (доступа к информационной системе) в течение трех минут с возможностью разблокирования только Администратором информационной системы.

В ИС (ИСПДн) должно обеспечиваться блокирование сеанса доступа пользователя после пяти минут его бездействия (неактивности) в ИС (ИСПДн) или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (ИСПДн) (без выхода из информационной системы).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИС (ИСПДн) сохраняется до прохождения им повторной идентификации и аутентификации.

Администратор безопасности информации совместно с Администратором информационной системы обеспечивают в ИС (ИСПДн) визуальное предупреждение пользователя в виде сообщения («окна») при его входе в ИС (до процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные обладателем ИС (ИСПДн) правила и ограничения на работу с информацией.

До пользователей ИС (ИСПДн) под роспись доводятся требования по организации парольной защиты с проставлением собственноручно подписи в листе ознакомления с соответствующей документированной процедурой и ответственность за использование паролей, не соответствующих установленным требованиям, а также за разглашение парольной информации.

3.5. Обязанности работников, при возникновении инцидентов информационной безопасности

Настоящий раздел регламентирует взаимодействие подразделений Учреждений при возникновении нештатных ситуаций.

При возникновении инцидентов ИБ работник, обнаруживший инцидент, немедленно ставит в известность своего непосредственного руководителя, Администратора безопасности информации или Администратора информационной системы.

Администратор безопасности информации или Администратора информационной системы проводят предварительный анализ ситуации.

По факту возникновения инцидента ИБ проводится выяснение причин его возникновения.

Результаты расследования фиксируются в акте. К акту прилагаются (при наличии) поясняющие материалы (копии экрана, распечатка журнала событий и др.). Акт предоставляется начальнику Учреждения.

3.6. Требования к резервированию информационных ресурсов

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

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

При организации резервирования ИР обеспечивается выполнение следующих требований:

- резервные копии ИР и инструкции по их восстановлению хранятся в специально выделенном месте, территориально отдаленном от места хранения основной копии информации;

- к резервным копиям применяется комплекс физических и организационных мер защиты;

- носители, на которые осуществляется резервное копирование, регулярно проверяются на отсутствие сбоев;

- применяемая система резервного копирования обеспечивает производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью;

- предусмотрены регулярная проверка процедур восстановления и практический тренинг работников по восстановлению данных.

Резервное копирование информации осуществляется Администратором информационной системы в соответствии с графиком резервного копирования. Допускается осуществление резервного копирования в автоматизированном режиме.

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

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

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

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

Восстановление данных из резервной копии производится Администратором информационной системы на основании заявки начальника структурного подразделения - обладателя ИР, согласованной с Администратором безопасности информации. Заявка может предоставляться в электронной форме.

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

3.7. Правила защиты ИС (ИСПДн) от вредоносных программ

При использовании в ИС (ИСПДн) средств антивирусной защиты и защиты от вредоносных программ выполняются следующие организационные меры:

- использование машинных носителей информации (ПДн) пользователя ИС (ИСПДн) на других компьютерах только с механической защитой от записи;

- запрет на использование неучтенных машинных носителей информации (ПДн) при работе в ИС (ИСПДн);

- запрет на передачу машинных носителей информации (ПДн) посторонним лицам;

- запрет на запуск программ с внешних съёмных носителей информации при работе в ИС (ИСПДн);

- запрет на несанкционированное использование отчуждаемых носителей информации (оптических дисков, флэш-карт и т. п.);

- использование в ИС (ИСПДн) только дистрибутивов программных продуктов, приобретенных у официальных дилеров фирм-разработчиков этих продуктов;

- обязательная проверка всех программных продуктов;

- проверка всех программных файлов и файлов документов, полученных по электронной почте, специальными антивирусными средствами;

- систематическая проверка содержимого дисков файловых хранилищ обновленными версиями антивирусных программ;

- контроль и обновление списка разрешенных ссылок на веб-ресурсы сети «Интернет».

Ответственность за эксплуатацию средств антивирусной защиты и защиты от вредоносных программ возлагается:

- на Администратора информационной системы в части наличия антивирусного ПО на клиентских рабочих станциях и использования данного ПО пользователями;

- на Администратора безопасности информации в части централизованного управления СЗИ(ПДн).

3.8. Требования по обеспечению безопасности при работе в информационно – телекоммуникационных сетях

Доступ к информационно – телекоммуникационным сетям, в т.ч. «Интернет», предоставляется пользователям исключительно в целях повышения эффективности выполнения ими своих служебных обязанностей.

Организация доступа пользователей ИСПДн к информационно – телекоммуникационным сетям и сети «Интернет» осуществляется Администратором информационной системы на основании мотивированного запроса руководителя структурного подразделения Учреждения, согласованного с Администратором безопасности информации.

Установка дополнительного оборудования и ПО для осуществления доступа пользователей ИС (ИСПДн) осуществляется в порядке, установленным настоящим Положением для внесения изменений в ПО и аппаратные средства Учреждения.

Администратор безопасности информации и Администратор информационной системы обеспечивают защиту информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Использование удаленного доступа к информационной системе запрещено.

В отдельных случаях по решению начальника Учреждения, в случае служебной необходимости и наличия технической возможности может быть обеспечен удаленный доступ к информационной системе, но при этом должна быть обеспечена защита требуемого вида доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) которая должна включать:

- установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ИС (ИСПДн);

- ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС (ИСПДн), для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа.

- предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС (ИСПДн);

- контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС (ИСПДн) до начала информационного взаимодействия

с информационной системой (передачи защищаемой информации).

Использование технологий беспроводного доступа к информационной системе запрещено.

В отдельных случаях по решению начальника Учреждения, в случае служебной необходимости и наличия технической возможности может быть организован беспроводный доступ пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), но при этом дополнительно должны быть обеспечены регламентация и контроль использования технологий беспроводного доступа, направленные на защиту информации в ИС (ИСПДн).

Регламентация и контроль использования технологий беспроводного доступа должны включать:

- ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИС (ИСПДн), для решения которых такой доступ необходим;
- предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
- контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС (ИСПДн) до начала информационного взаимодействия с информационной системой.

Запрещается использование подключений к сети «Интернет» и каналов связи, использование которых не согласовано с Администратором безопасности информации.

Пользователи ИС (ИСПДн) могут использовать сеть «Интернет» в качестве:

- транспортной среды при обмене информацией между несколькими территориально разнесенными элементами ИС (ИСПДн) или другими ИС (ИСПДн) (транспортная задача);

- средства предоставления открытой общедоступной информации, содержащейся в ИР Учреждения, внешнему абоненту (портальная задача);

- средства получения необходимой пользователям ИС (ИСПДн) информации, содержащейся в ИР сети «Интернет» или других корпоративных сетей (информационная задача).

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

При работе с ресурсами сети «Интернет» запрещается:

- разглашение конфиденциальной информации, ставшей известной работнику Учреждения, в связи с исполнением служебных обязанностей либо иным путем;

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

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в сети «Интернет», а также размещение ссылок на вышеуказанную информацию;

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

- использование анонимных прокси-серверов;

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

Вся информация о ресурсах, посещаемых работниками Учреждения, протоколируется.

Администратор информационной системы обязан проводить анализ использования ресурсов сети «Интернет» и в случае необходимости представлять отчет об использовании «Интернет-ресурсов» работниками Администратору безопасности информации.

В случае обнаружения значительных отклонений в параметрах работы средств обеспечения доступа к ресурсам сети «Интернет» от среднестатистических значений немедленно сообщается Администратору безопасности информации для принятия последующих решений.

Руководители подразделений вправе запросить у Администратора безопасности информации отчет об использовании ресурсов сети «Интернет» работниками своего подразделения.

При нарушении работником Учреждения правил работы в сети «Интернет» либо возникновении нештатных ситуаций доступ к ресурсам сети «Интернет» блокируется Администратором информационной системы с последующим уведомлением Администратора безопасности информации.

Электронная почта в Учреждении является средством коммуникации, распределения информации и управления процессами в производственных целях: повышения эффективности труда работников Учреждения и экономии ресурсов.

Корпоративная (внутренняя) электронная почта Учреждения предназначена исключительно для использования в служебных целях.

Использование личной почты в служебных целях запрещено.

Организацией и обеспечением порядка работы электронной почты в Учреждении занимается Администратор информационной системы. Ответственность за использование электронной почты возлагается на работников и руководителей подразделений в рамках их должностных обязанностей.

При работе с корпоративной электронной почтой Учреждения пользователь учитывает следующие принципиальные положения:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

- внутренняя электронная почта, организованная с применением средств криптографической защиты, является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации.

Передача информации ограниченного доступа осуществляется только в зашифрованном или в обезличенном виде.

3.9. Правила использования ПО и аппаратных средств ИС (ИСПДн)

Настоящий раздел регламентирует взаимодействие подразделений Учреждения по обеспечению безопасности информации при проведении модификаций ПО, технического обслуживания и ремонта средств вычислительной техники (СВТ) ИС (ИСПДн).

3.9.1. Права на внесение изменений в ПО и аппаратные средства ИС (ИСПДн)

Все изменения конфигурации ТС и программных средств рабочих станций (АРМ) и серверов ИС (ИСПДн), обрабатывающих защищаемую информацию (ПДн), производятся только на основании заявок начальников структурных подразделений, согласованных с Администратором безопасности информации.

Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (рабочих станций, серверов) и телекоммуникационного оборудования, обрабатывающего информацию (ПДн), предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – Администратору информационной системы;

- в отношении программно-аппаратных СЗИ - Администратору безопасности информации и Администратору информационной системы;

- в отношении программно-аппаратных средств телекоммуникаций – Администратору информационной системы.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций (АРМ) и серверов кем-либо, кроме уполномоченных работников, запрещено.

3.9.2. Порядок внесения изменений в ПО и аппаратные средства ИС (ИСПДн)

Для внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций ИС (ИСПДн) начальником структурного подразделения, в котором вносятся изменения, подается заявка на имя Администратора информационной системы, которая им рассматривается и утверждается по согласованию с Администратором безопасности информации.

При необходимости планового проведения изменений (обновлений версий) ПО, заявка выпускается руководителем структурного подразделения и, после согласования с Администратором безопасности информации, направляется Администратору информационной системы.

В заявках могут быть указаны следующие виды необходимых изменений в составе программных и аппаратных средств рабочих станций и серверов подразделения:

- установка в подразделении новой рабочей станции (АРМ) или сервера;

- замена рабочей станции (АРМ) или сервера подразделения;

- изъятие рабочей станции (АРМ) или сервера подразделения;

- добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера подразделения;

- замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера подразделения;

- изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;

- установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);

- обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке указываются условные наименования развернутых рабочих станций (АРМ) и серверов в соответствии с их паспортами. Программные средства указываются в соответствии с перечнем программных средств алгоритмов и программ, которые используются в ИС (ИСПДн).

Администратор безопасности информации при согласовании заявки учитывает возможность совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях (АРМ) или серверах в соответствии с требованиями по безопасности.

После этого заявка передается Администратору информационной системы для непосредственного исполнения работ по внесению изменений в конфигурацию рабочих станций (АРМ) или серверов ИС (ИСПДн).

Начальник структурного подразделения, в котором установлены аппаратно-программные средства, подлежащие модернизации, допускает Администратора информационной системы и Администратора безопасности информации к внесению изменений в состав аппаратных средств и ПО.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором информационной системы.

Если рабочая станция (АРМ) или сервер обрабатывают защищаемую информацию (ПДн), то установка, снятие, и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется Администратором информационной системы под контролем Администратора безопасности информации. Работы производятся в присутствии пользователя данной рабочей станции.

Подготовка модификаций ПО защищенных серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в фонд алгоритмов и программ и другие необходимые действия производится Администратором информационной системы.

Установка или обновление ИС (ИСПДн) проводится в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Модификация ПО на сервере осуществляется Администратором информационной системы по согласованию с Администратором безопасности информации.

После установки модифицированных модулей на сервер Администратор безопасности информации в присутствии Администратора информационной системы устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью специальных программных средств, прошедших оценку соответствия).

После проведения модификации ПО на рабочих станциях Администратор информационной системы проводит антивирусный контроль.

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

Все добавляемые программные и аппаратные компоненты предварительно проверяются на работоспособность, контроль наличия проверок работоспособности осуществляет Администратор безопасности информации.

После установки (обновления) ПО Администратор информационной системы, а при использовании специализированных СЗИ от НСД - Администратор безопасности информации производят настройку средств управления доступом к данному программному средству и проверяют работоспособность ПО и правильность настройки СЗИ.

После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), обрабатывающей ПДн, ее системный блок закрывается Администратором информационной системы на ключ (при наличии штатных механических замков) и опечатывается (пломбируется, защищается специальной наклейкой) с возможностью постоянного визуального контроля за ее целостностью Администратором безопасности информации.

Администратор безопасности информации проводит периодический контроль за опечатыванием узлов и блоков ИС (ИСПДн).

На обратной стороне заявки делается отметка о выполнении и исполненная заявка хранится вместе с паспортом данной рабочей станции (сервера).

При изъятии рабочей станции (сервера), обрабатывающей защищаемую информацию (ПДн), из состава рабочих станций (серверов) структурного подразделения ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как Администратор безопасности информации снимет с данной рабочей станции (сервера) СЗИ и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется Актом об уничтожении конфиденциальной информации (персональных данных) после затирания остаточной информации, хранившейся на диске компьютера.

Оригиналы заявок (документов), на основании которых производились изменения в составе ТС или программных средств рабочих станций с отметками о внесении изменений в состав программно-аппаратных средств хранятся вместе с оригиналами паспортов рабочих станций (серверов). Они могут быть использованы:

- для восстановления конфигурации рабочих станций (серверов) после аварий;

- для контроля правомерности установки на конкретной рабочей станции (сервере) средств для решения соответствующих задач при разборе конфликтных ситуаций;

- для проверки правильности установки и настройки СЗИ рабочих станций (серверов).

3.10. Требования по обеспечению безопасности при применении средств криптографической защиты информации

Для защиты информации, не содержащей сведений, составляющих государственную тайну, при применении средств криптографической защиты информации (СКЗИ) соблюдаются нормативные требования. Криптографическая защита в ИС (ИСПДн) Учреждения создаётся на основе сертифицированных СКЗИ, встраивание которых в ИС (ИСПДн) происходит с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

В Учреждении выделяются должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ. Вопросы обеспечения функционирования и безопасности СКЗИ отражаются в специально разработанных документах в соответствии с требованиями регуляторов в области защиты информации, утвержденных начальником Учреждения, с учетом эксплуатационной документации на СКЗИ.

К работе с СКЗИ решением начальника Учреждения допускаются работники, обладающие знаниями: эксплуатационной документации, о правилах эксплуатации и правилах пользования, прошедшие обучение работе с СКЗИ.

Ответственное должностное лицо, уполномоченное на руководство заявленными видами деятельности со средствами СКЗИ (Ответственный пользователь СКЗИ), имеет представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и СЗИ.

Охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), обеспечивают безопасность информации, СКЗИ и криптоключей, сводят к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

Порядок допуска в помещения определяется внутренним документом Учреждения.

В зависимости от установленных уровней защищенности ПДн необходимо выполнить:

- оснащение помещений входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;
- утвердить правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- организовать режим обеспечения безопасности помещений, в которых размещена ИС (ИСПДн), препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами,

препятствующими НСД в помещения. Эти помещения имеют прочные входные двери, на которые устанавливаются надежные замки.

Для хранения криптоключей, нормативной и эксплуатационной документации, инсталлирующих криптосредство носителей, помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей хранятся в сейфе ответственного лица, назначаемого начальником Учреждения. Порядок охраны помещений предусматривает периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ. Системные блоки АРМ с СКЗИ оборудуются средствами контроля их вскрытия.

3.11. Регистрация событий безопасности

Для реагирования на события безопасности в информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности.

События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС (ИСПДн). Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС (ИСПДн).

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Администратором информационной системы исходя из возможностей реализации угроз безопасности информации и фиксируется в Журнале учета мероприятий по контролю режима защиты конфиденциальной информации (ПДн) и выполнения обязательных процедур.

Сбор, запись и хранение информации о событиях безопасности должен предусматривать:

- возможность выбора Администратором безопасности информации событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности;

- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);

- хранение информации о событиях безопасности.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

- реагирование на сбои при регистрации событий безопасности путем изменения

администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

Администратор безопасности информации и Администратор информационной системы осуществляют мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагируют на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) проводиться для всех событий, подлежащих регистрации, и с периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в ИС (ИСПДн).

В случае выявления признаков ИБ в ИС (ИСПДн) осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Администратор информационной системы контролирует синхронизацию системного времени. Применение внутренних системных часов ИС (ИСПДн) необходимо для получения меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС (ИСПДн).

Информация о событиях безопасности подлежит защите и обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только Администратору безопасности информации и Администратору информационной системы.

4. Порядок организации внутреннего обучения работников правилам и мерам защиты ПДн

Решение основных вопросов обеспечения защиты информации (ПДн) предусматривает соответствующую подготовку работников. Проведение обучения работников Учреждения позволяет организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности информации (ПДн) при их обработке в ИС (ИСПДн) и реализовать установленный комплекс организационных и технических мер по защите информации (ПДн).

Систему внутреннего обучения работников в области защиты информации (ПДн) составляет:

- проведение инструктажа пользователей ИС (ИСПДн);

- самостоятельное изучение работниками Учреждения необходимых для работы документов, средств и продуктов;

- проведение курсов повышения квалификации работников в области защиты персональных данных.

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

- правил использования СЗИ;

- содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности информации (ПДн) при их обработке в ИС (ИСПДн);

- основных мероприятий по организации и техническому обеспечению безопасности информации (ПДн) при их обработке в ИС (ИСПДн);

4.1. Проведение инструктажа пользователей ИС (ИСПДн)

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

Инструктаж представляет собой ознакомление работников Учреждения, допущенных к работе в ИС (ИСПДн), с положениями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при ее обработке в ИС (ИСПДн), в том числе и с Инструкцией пользователя ИС (ИСПДн).

Ознакомление с положениями нормативной документации работник Учреждения подтверждает своей личной подписью в журнале инструктажа (обучения), что свидетельствует о прохождении инструктажа (обучения).

Контроль проведения инструктажа и периодическая проверка знаний пользователями ИС (ИСПДн) положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на Администратора безопасности информации и ответственного за организацию обработки персональных данных в Учреждении совместно с начальниками структурных подразделений, использующих ИС (ИСПДн).

Ответственность за непосредственное проведение инструктажа возлагается на начальников структурных подразделений Учреждения.

Работники Учреждения, не прошедшие инструктаж, к работе в ИС (ИСПДн) не допускаются. Инструктаж проводится перед началом работы в ИС (ИСПДн) и вновь принятых на работу работников, а также не реже одного раза в год для всех пользователей ИС (ИСПДн).

Проверка знаний пользователями ИС (ИСПДн) положений законодательства Российской Федерации в области персональных данных и нормативных правовых документов по вопросам обеспечения безопасности информации (ПДн) проводятся: лицом, назначенным ответственным за организацию обработки персональных данных в Учреждении и/или Администратором безопасности информации, не реже одного раза в год, а также в ходе периодического контроля, соблюдения режима безопасности информации (ПДн).

4.2. Самостоятельное изучение

При данном виде подготовки работниками Учреждения, осуществляющими обработку информации (ПДн), самостоятельно изучаются (в части касающейся):

- нормативные правовые документы в области защиты информации (ПДн);

- руководящие и нормативно-методические документы в области обеспечения безопасности информации (ПДн);

- правила (инструкции) по использованию программных и аппаратных СЗИ.

- внутренние положения (локальные акты) Учреждения, устанавливающие порядок обращения с информацией (ПДн) и их защиты.

Время для самостоятельного изучения определяется начальниками структурных подразделений.

5. Ответственность должностных лиц за обеспечение безопасности информации (ПДн), своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ(ПДн)

Ответственность за обеспечение безопасности информации (ПДн) распределяется между должностными лицами Учреждения на основании настоящего Положения.

Ответственность за организацию режима обеспечения безопасности информации (ПДн) возлагается на начальника Учреждения и начальников структурных подразделений.

Ответственность за своевременность и качество формирования требований по защите информации (ПДн), за качество и научно-технический уровень разработки СЗИ(ПДн), а также контроль исполнения правил и требований, направленных на обеспечение безопасности информации (ПДн), возлагается на лицо, ответственное за организацию обработки персональных данных и/или Администратора безопасности информации.

Ответственность за выполнение обязанностей по обеспечению режима безопасности информации (ПДн), несут начальники соответствующих структурных подразделений, эксплуатирующие ИС (ИСПДн).

Средства информатизации, входящие в состав ИС (ИСПДн), закрепляются за ответственными должностными лицами (владельцами). Владельцем средств информатизации может быть начальник структурного подразделения или специально назначаемое должностное лицо. На владельца средств информатизации возлагается ответственность за выполнение установленных мероприятий по защите закрепленных средств информатизации и обрабатываемой ими информации (ПДн).

Должностные лица и работники Учреждения, виновные в нарушении режима защиты информации (ПДн), несут дисциплинарную, гражданскую, административную и уголовную ответственность, предусмотренную законодательством Российской Федерации.

6. Порядок контроля за обеспечением уровня защищенности информации (ПДн) и оценки соответствия ИС (ИСПДн)

Контроль обеспечения требуемого уровня защищенности информации (ПДн) заключается в проверке выполнения требований нормативных документов по защите информации (ПДн), а также в оценке обоснованности и эффективности принятых мер. Мероприятия по контролю защищенности информации (ПДн) могут проводиться как уполномоченными работниками Учреждения, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации. Мероприятия по контролю защищенности информации (ПДн) и оценке соответствия ИС (ИСПДн) включают:

- внутренний контроль режима безопасности информации (ПДн) (оперативный и периодический);

- обследование защищенности информации (ПДн) с привлечением сторонней организации;

- оценку соответствия ИС (ИСПДн) требованиям безопасности информации (ПДн).

6.1. Внутренний контроль режима безопасности информации (ПДн) и оценки соответствия ИС (ИСПДн) требованиям безопасности

Внутренний оперативный контроль соблюдения режима безопасности информации (ПДн) проводится Администратором безопасности информации ежедневно в режиме «реального времени».

Внутренний контроль заключается в анализе защищенности информации (ПДн) посредством используемых в составе ИС (ИСПДн) программных и программно-аппаратных средств (систем) анализа защищенности.

В ходе проведения контроля соблюдения режима безопасности информации ПДн Администратор безопасности информации:

- осуществляет анализ лог-файлов, производимых средствами защиты и другими элементами ИС (ИСПДн) (ОС, прикладные программы);

- просматривает оповещения средств защиты ИС (ИСПДн);

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

Внутренний периодический контроль соблюдения режима безопасности информации (ПДн) (контрольные обследования защищенности ИС (ИСПДн)) организуется лицом, ответственным за организацию обработки персональных данных по планам, ежегодно утверждаемым начальником Учреждения.

По решению начальника Учреждения внутренний контроль может проводиться во внеочередном порядке в случаях выявления нарушений безопасности информации (ПДн) с целью определения причин произошедших нарушений и разработки мер по их устранению.

Внутренний периодический контроль заключается в оценке выполнения требований нормативных (методических, руководящих) документов по обеспечению безопасности информации (ПДн), обрабатываемых в ИС (ИСПДн).

В ходе проведения внутреннего периодического контроля проверяются следующие вопросы:

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

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

- проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки информации (ПДн) и применения СЗИ (сертификатов соответствия и других документов);

- проверка правильности применения СЗИ;

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

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

- знание инструкций по обеспечению безопасности информации пользователями ИС (ИСПДн);

- организация хранения носителей информации (ПДн) и допуска в помещения, в которых размещены средства обработки и осуществляется обработка информации (ПДн);

- прохождение инструктажа пользователей по вопросам обеспечения безопасности информации (ПДн) и выполнение ими установленных требований.

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

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

6.2. Обследование защищенности информации (ПДн) внешней специализированной организацией

Обследование защищенности информации (ПДн) внешней специализированной организацией проводится при создании ИС (ИСПДн) (формирование требований к защите информации, содержащейся в информационной системе) или при доработке (модернизации) СЗИ(ПДн) в случае, если:

- изменился состав или структура ИС (ИСПДн) или технические особенности её построения (состав или структура ПО, ТС обработки информации (ПДн), топологии и т.п.);

- изменился состав угроз безопасности информации (ПДн);

- изменился класс защищённости ИС (ИСПДн).

Обследование защищенности информации (ПДн) внешней специализированной организацией проводится по решению начальника Учреждения.

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

6.3. Порядок оценки соответствия ИС (ИСПДн) требованиям безопасности информации (ПДн)

Оценка соответствия ИС (ИСПДн) требованиям безопасности информации (ПДн) проводится в форме проверки готовности СЗИ к использованию.

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

Для проверки готовности СЗИ к использованию или для проведения аттестации ИС (ИСПДн), привлекается организация, имеющая лицензию ФСТЭК России на право деятельности по технической защите конфиденциальной информации в соответствии с постановлением Правительства Российской Федерации от 03.02.2012 № 79.

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

Аттестация проводится в соответствии с действующими нормативными и методическими документами ФСТЭК России.

Порядок подготовки и проведения аттестации ИС (ИСПДн) определяется в приказах (распоряжениях) начальника Учреждения.