

Министерство труда и социальной защиты Чувашской Республики

УТВЕРЖДАЮ
Министр труда и социальной
защиты Чувашской Республики

С.П. Дмитриев

« 11 » декабря 2015 г.

**Политика информационной безопасности
информационных систем персональных данных
Министерства труда и социальной защиты
Чувашской Республики**

г. Чебоксары

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, 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.

Межсетевой экран – локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанному в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных,

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы 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 невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

- АВС** – антивирусные средства
- АРМ** – автоматизированное рабочее место
- ВТСС** – вспомогательные технические средства и системы
- ИСПДн** – информационная система персональных данных
- КЗ** – контролируемая зона
- ЛВС** – локальная вычислительная сеть
- МЭ** – межсетевой экран
- НСД** – несанкционированный доступ
- ОС** – операционная система
- ПДн** – персональные данные
- ПМВ** – программно-математическое воздействие
- ПО** – программное обеспечение
- ПЭМИН** – побочные электромагнитные излучения и наводки
- САЗ** – система анализа защищенности
- СЗИ** – средства защиты информации
- СЗПДн** – система (подсистема) защиты персональных данных
- СОВ** – система обнаружения вторжений
- ТКУИ** – технические каналы утечки информации
- УБПДн** – угрозы безопасности персональных данных

Введение

Настоящая Политика информационной безопасности ИСПДн Министерства труда и социальной защиты Чувашской Республики (далее - Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Концепции информационной безопасности информационных систем персональных данных Министерства труда и социальной защиты Чувашской Республики (далее - Концепция), и является официальным документом.

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» на основании:

- «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных ФСТЭК России от 15.02.2008;

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных (далее - ПДн) в ИСПДн Министерства труда и социальной защиты Чувашской Республики (далее – Минтруд Чувашии) и подведомственных учреждений.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Министерства труда и подведомственных учреждений от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее - УБПДн) информационной системы.

Безопасность ПДн достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожение данных.

Состав ИСПДн, подлежащих защите, представлен в «Перечне информационных систем персональных данных». Состав объектов защиты представлен в «Перечне персональных данных, содержащихся в программных комплексах, входящих в состав информационной системы персональных данных».

Требования настоящей Политики распространяются на всех сотрудников Минтруда Чувашии и подведомственных учреждений (штатных, временных, работающих по контракту и т.п.), а также сторонних организаций (подрядчики, аудиторы и т.п.).

2. Система защиты персональных данных

2.1. Система защиты персональных данных (далее - СЗПДн), строится на основании:

- акта о результатах проведения внутренней проверки;
- перечня персональных данных, подлежащих защите;
- акта классификации информационной системы персональных данных;
- модели угроз безопасности персональных данных;
- разрешительной системы допуска (матрицы доступа) на информационные системы персональных данных;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Минтруда Чувашии и подведомственных учреждений. На основании анализа актуальных угроз безопасности ПДн, описанных в модели угроз безопасности персональных данных, и актов о результатах проведения внутренних проверок режима защиты персональных данных в Минтруде Чувашии и подведомственных учреждениях, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по защите персональных данных в Минтруде Чувашии и подведомственных учреждениях.

2.2. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевое экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

2.3. В список включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружение вторжений.

2.4. Список используемых технических средств отражается в Плане мероприятий по защите персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены в Минтруде Чувашии - министром либо лицом, ответственным за обеспечение защиты ПДн Минтруда Чувашии, в подведомственном учреждении - директором подведомственного учреждения.

3. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в акте классификации ИСПДн. Функции должны обеспечивать необходимый уровень защищенности от актуальных угроз ИСПДн.

3.1. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

3.2. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Минтруда Чувашии и подведомственных учреждений, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

3.3. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Минтруда Чувашии и подведомственных учреждений.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

3.4. Подсистема межсетевое экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификации администратора меж сетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора меж сетевого экрана в систему (из системы) либо загрузки и инициализации системы;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

3.5. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения (ПО) ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.6. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.7. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Минтруда Чувашии и подведомственных учреждений, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

4. Пользователи ИСПДн

В Концепции определены основные категории пользователей. На основе этих категорий производится типизация пользователей ИСПДн, определяется их уровень доступа и возможности.

В ИСПДн Минтруда Чувашии и подведомственных учреждений можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратора ИСПДн;
- администратора безопасности;
- оператора ИСПДн;
- администратора сети;
- технического специалиста по обслуживанию периферийного оборудования;
- программиста-разработчика ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности отражаются в разрешительной системе допуска (матрице доступа) на информационные системы персональных данных (ИСПДн).

4.1. Администратор ИСПДн - сотрудник отдела информационных технологий и защиты информации Минтруда Чувашии (сотрудник подведомственного учреждения), ответственный за настройку, внедрение и сопровождение ИСПДн. Администратор ИСПДн обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

4.2. Администратор безопасности - сотрудник отдела информационных технологий и защиты информации Минтруда Чувашии (сотрудник подведомственного учреждения), ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор ИСПДн) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других предприятий.

4.3. Оператор ИСПДн - сотрудник Минтруда Чувашии (подведомственного учреждения), осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор ИСПДн не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

4.4. Администратор сети - сотрудник отдела информационных технологий и защиты информации Минтруда Чувашии (сотрудник подведомственного учреждения), ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

- знает, по меньшей мере, одно легальное имя доступа.

4.5. Технический специалист по обслуживанию - сотрудник отдела информационных технологий и защиты информации Минтруда Чувашии (сотрудник подведомственного учреждения), осуществляющий обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- знает, по меньшей мере, одно легальное имя доступа.

4.6. Программист-разработчик (поставщик) прикладного программного обеспечения - сотрудник сторонней лицензированной организации, обеспечивающий его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники оператора, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

5. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Минтруда Чувашии и подведомственных учреждений, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный руководитель подразделения Минтруда Чувашии (подведомственного учреждения), в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Пользователь ИСПДн должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Пользователи ИСПДн Минтруда Чувашии и подведомственных учреждений, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи ИСПДн несут персональную ответственность за сохранность идентификаторов.

Пользователи ИСПДн Минтруда Чувашии и подведомственных учреждений должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Пользователи ИСПДн Минтруда Чувашии и подведомственных учреждений должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи ИСПДн должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Пользователям ИСПДн запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Пользователям ИСПДн запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Минтруда Чувашии и подведомственных учреждений, третьим лицам.

При работе с ПДн в ИСПДн пользователи ИСПДн Минтруда Чувашии и подведомственных учреждений обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн пользователи ИСПДн обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Пользователи ИСПДн Минтруда Чувашии и подведомственных учреждений должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на пользователей ИСПДн, которые нарушили принятые политику и процедуры безопасности ПДн.

Пользователи ИСПДн обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству, а также администратору ИСПДн и администратору безопасности ИСПДн.

6. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция оператора ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

7. Ответственность пользователей ИСПДн Минтруда Чувашии и подведомственных учреждений

В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Администратор ИСПДн и администратор безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях пользователями ИСПДн Минтруда Чувашии и подведомственных учреждений правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных регламентах сотрудников Минтруда Чувашии и подведомственных учреждений, осуществляющих обработку ПДн в ИСПДн.

В должностные регламенты сотрудников Минтруда Чувашии и подведомственных учреждений, осуществляющих обработку ПДн в ИСПДн, должны быть внесены сведения об их ответственности за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

8. Список использованных источников

Федеральные законы и нормативные правовые акты Российской Федерации

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный Закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».
4. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
6. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Нормативно-методические документы ФСТЭК России и ФСБ России

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14.02.2008.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14.02.2008.

9. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные ФСБ России 21.02.2008 № 149/6/6-622.

10. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

11. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

12. Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014.

Отдел информационных технологий и защиты информации Минтруда Чувашии