ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

от 20 мая 2013 г. № 77-ро

г. Архангельск

Об утверждении Политики информационной безопасности информационных систем персональных данных министерства здравоохранения Архангельской области

Во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Утвердить прилагаемую Политику информационной безопасности информационных систем персональных данных министерства здравоохранения Архангельской области;
2. Настоящее распоряжение вступает в силу со дня его подписания.

Министр **Л.И. Меньшикова**

УТВЕРЖДЕНА
распоряжением министерства
здравоохранения
Архангельской области

от 20 мая 2013 г. № 77-пр

ПОЛИТИКА
информационной безопасности информационных систем персональных данных министерства здравоохранения Архангельской области

1. Настоящая Политика информационной безопасности (далее – Политика) министерства здравоохранения Архангельской области (далее – министерство) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных (далее - ПДн) изложенных в Концепции информационной безопасности информационных систем персональных данных министерства здравоохранения Архангельской области.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлений Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к персоналу информационных систем персональных данных (далее - ИСПДн), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн министерства.

2. В настоящем документе используются следующие термины и их определения.

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

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить

конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

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

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;

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;

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;

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;

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 описанным 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;

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;

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированно

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;

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;

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);

3. В настоящей Концепции используются следующие обозначения и сокращения:

АВС – антивирусные средства

АРМ –автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

Министерство – министерство здравоохранения Архангельской области

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

СУБД –система управления базой данных

УБПДн – угрозы безопасности персональных данных

4. Целью настоящей Политики является обеспечение безопасности объектов защиты министерства от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных 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 доступны для авторизованных пользователей. Осуществляется своевременное обнаружение и реагирование на УБПДн.

Осуществляется предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты указывается в Перечне персональных данных, подлежащих защите.

Состав ИСПДн подлежащих защите, указывается в Отчете о результатах проведения внутренней проверки.

Настоящая политика информационной безопасности утверждается министром здравоохранения Архангельской области (далее - министр) и вводится в действие распоряжением министерства.

5. Требования настоящей Политики распространяются на всех сотрудников министерства (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

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

отчета о результатах проведения внутренней проверки;

перечня персональных данных, подлежащих защите;

акта классификации информационной системы персональных данных;

модели угроз безопасности персональных данных;

положения о разграничении прав доступа к обрабатываемым персональным данным;

руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн министерства. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз безопасности персональных данных и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн составляется список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

автоматизированных рабочих мест пользователей;

сервера приложений;

систем управления базами данных;

границы локально-вычислительной сети;

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 межсетевого экранирования;

средства анализа защищенности сети;

средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же 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.

Список используемых средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения вносятся в Список и утверждаются министром или лицом, ответственным за обеспечение защиты ПДн.

7. 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 информационной системы персональных данных.

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 остановки;

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). Так же 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 средств.

2) подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн министерства, 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) подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн министерства.

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.

4) подсистема межсетевого 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 аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного приостановления;

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.

5) подсистема анализа защищенности, обеспечивает выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы реализуется внедрением программных и программно-аппаратных средств.

6) подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы реализуется внедрением программных и программно-аппаратных средств.

7) подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн министерства, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программных или программно-аппаратных комплексов.

8. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории проводится типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн министерства можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

администратора ИСПДн;

администратора безопасности;

оператора АРМ;

администратора сети;

технического специалиста по обслуживанию периферийного оборудования;

программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности отражаются в Положение о разграничении прав доступа к обрабатываемым персональным данным.

1) администратор ИСПДн, сотрудник министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим ПДн.

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.

2) администратор безопасности, сотрудник министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), ответственный за функционирование СЗПДн, включая обслуживание и настройку административный, серверный и клиентский 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 политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

осуществлять аудит средств защиты;

устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений.

3) оператор АРМ, сотрудник министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор АРМ 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) администратор сети, сотрудник министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), 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.

5) технический специалист по обслуживанию, сотрудник министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), осуществляет 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.

6) программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники министерства, так и сотрудники сторонних организаций.

Лицо указанной 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.

9. Все сотрудники министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудники сторонней организации), 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 начальник подразделения, 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.

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

Сотрудники министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации), использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их

утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации) должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

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

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами министерства, третьим лицам.

При работе с ПДн в ИСПДн сотрудники министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации) обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

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

Сотрудники министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудник сторонней организации) 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 сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники 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 структурного подразделения

и/или лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Должностные обязанности пользователей ИСПДн описываются в следующих документах:

инструкция администратора ИСПДн;

инструкция администратора безопасности ИСПДн;

инструкция пользователя ИСПДн;

инструкция пользователя при возникновении внештатных ситуаций.

11. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности 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 сотрудниками министерства (в случаях, когда сотрудникам сторонних организаций при взаимодействии предоставляется доступ к объектам защиты – сотрудниками сторонней организации) – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.