УТВЕРЖДАЮ
главный врач
ГУЗ РКБ им. Н.А. Семашко
_____Л.Ю.Сорокина
«15» 11 2010 г.

Политика информационной безопасности

информационных систем персональных данных
ГУЗ Рязанская клиническая больница им. Н.А. Семашко

Государственное учреждение здравоохранения «Рязанская клиническая больница им. Н.А. Семашко», сокращённое наименование ГУЗ РКБ им. Н.А. Семашко переименовано в Государственное бюджетное учреждение Рязанской области «Клиническая больница им. Н.А. Семашко», сокращённое наименование ГБУ РО «КБ им. Н.А. Семашко».

Основание: приказ Министерства имущественных и земельных отношений Рязанской области и Министерства здравоохранения Рязанской области от 09.11.2011 г. № 708-р/1161, приказ главного врача ГУЗ РКБ им. Н.А. Семашко от 13.12.2011 г. № 380-д «О мероприятиях в связи с изменением наименования учреждения».

Коррекция 01.01.2012 г.

Заместитель главного врача по МР и ГО _____Илларионов И.Г.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

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.

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

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.

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 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.

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, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать 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.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

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.

ТКУ И – технические каналы утечки информации.

УБПДн – угрозы безопасности персональных данных.

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – Политика) ГУЗ Рязанская клиническая больница им. Н.А. Семашко (Далее - Учреждения), разработана на основании рекомендаций для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости; утверждено Министерством здравоохранения и социального развития Российской Федерации и согласованно со ФСТЭК России.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в «Концепции информационной безопасности» ИСПД Учреждения.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

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 в ИСПДн Учреждения.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения 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 должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

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

Состав персональных данных представлен в «Перечне ПДн обрабатываемых в ИСПДн».

Состав ИСПДн подлежащих защите, представлен в «Отчете о результатах обследования системы защиты персональных данных информационной системы персональных данных».

2 ОБЛАСТЬ ДЕЙСТВИЯ

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

3 СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (СЗПДн), строится на основании:

- «Отчета о результатах обследования системы защиты персональных данных ИСПДн»;
- «Перечня сведений конфиденциального характера»;
- «Акта классификации информационной системы персональных данных»;
- «Модели угроз безопасности персональных данных»;
- «Перечня лиц допущенных к обработке ПДн в ИСПДн»;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн описанного в «Модели угроз» и «Отчете о результатах обследования системы защиты персональных данных информационной системы персональных данных», делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

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

- АРМ пользователей;
- Сервер 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;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены 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 обнаружений вторжений.

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 руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

4 ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления логическим доступом;
- регистрации и учета;
- обеспечения целостности;
- антивирусная защита;
- обнаружение вторжений;
- межсетевого взаимодействия.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в «Акте классификации информационной системы персональных данных». Список соответствия функций подсистем СЗПДн классу защищенности представлен в Приложении 1.

4.1 Подсистемы управления логическим доступом.

Подсистема управления логическим доступом предназначена для реализации следующих функций:

- идентификации и проверки подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно – постоянного действия длиной не менее шести буквенно – цифровых символов;
- идентификации терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

Подсистема управления логическим 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.

4.2 Подсистема регистрации и учета.

Подсистема регистрации и учета предназначена для реализации следующих функций:

- регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

- регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатора пользователя, запросившего документ;

- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешны);

- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием её результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

- регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));

- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей.

4.3 Подсистема обеспечения целостности.

Подсистема обеспечения целостности предназначена для выполнения следующих функций:

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;

- физической охраны технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;

- периодического тестирования функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест – программ, имитирующих попытки несанкционированного доступа;

- наличия средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4 Подсистема антивирусной защиты.

Подсистема антивирусной защиты предназначена для выполнения следующих функций:

- должна проводиться автоматическая проверка на наличие вредоносных программ (далее ВП) или последствий программно-математических воздействий (далее ПМВ) при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;

- должны быть реализованы механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;

- должна регулярно выполняться проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью);

- факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП;

- должен быть реализован механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП;

- на всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ;

- должна проводиться проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;

- должны быть реализованы механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;

- должна быть обеспечена возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программных средств защиты, его периодическое обновление и контроль работоспособности.

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

4.5 Подсистема обнаружения вторжений.

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.

4.6 Подсистема межсетевого экранирования.

Подсистема межсетевого взаимодействия предназначена для реализации следующих функций:

- фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

- фильтрация с учетом любых значимых полей сетевых пакетов;

- фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

- фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

- фильтрация с учетом даты и времени;

- аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушивании сети;

- регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

- регистрация и учет запросов на установление виртуальных соединений;

- локальная сигнализация попыток нарушения правил фильтрации;

- идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно – постоянного действия;

- предотвращение доступа не идентификационного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

- идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

- регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация входа из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

- регистрация запуска программ и процессов (заданий, задач);

- регистрация действия администратора межсетевого экрана по изменению правил фильтрации;

- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;

- контроль целостности своей программной и информационной части;

- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;

- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

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

5 ПОЛЬЗОВАТЕЛИ ИСПДн

В «Концепции информационной безопасности» определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

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

- Администратора ИСПДн;

- Администратора информационной безопасности (ИБ) ИСПДн;

- Пользователи АРМ;

- Программист-разработчик ИСПДн.

Данные о группах пользователях должен быть отражен в «Перечне лиц допущенных к обработке ПДн в ИСПДн».

5.1 Администратор ИСПДн.

Администратор ИСПДн, сотрудник Учреждения, 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 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.

5.2 Администратор (ИБ) ИСПДн.

Администратор безопасности, сотрудник 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 ИБ 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 Учреждений.

Возможно совмещение ролей Администратора ИСПДн и Администратора ИБ ИСПДн.

5.3 Пользователи АРМ.

Пользователи АРМ, сотрудники 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. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователи АРМ 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.

5.4 Программист-разработчик ИСПДн.

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие разработку и сопровождение на защищаемом объекте. К данной группе относиться сотрудники Учреждения, ООО «Парус - Рязань», ООО «АКВАМАРИН», ЗАО «Калуга-Астрал».

Лица этой категории:

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

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

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

6 ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

Все сотрудники Учреждения, 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 и «Положением о ПДн, обрабатываемых в автоматизированной ИСПДн», принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Учреждения, 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 Учреждения должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Учреждения 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 Учреждения, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения 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 Учреждения 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 подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7 ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- «Инструкция администратора ИСПДн»;
- «Инструкция администратора информационной безопасности ИСПДн»;
- «Инструкция пользователя ИСПДн».

8 ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ИСПДн УЧРЕЖДЕНИЯ

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 информационной 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 Учреждения – пользователей ИСПДн 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 Положениях о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Учреждения.

Необходимо внести в Положения о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

9 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

а) Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;

б) Приказ Федеральной службы по техническому и экспортному контролю № 58 от 5 февраля 2010 года «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;

в) «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 17.11.2007 г. № 781;

г) «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.;

д) «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687;

е) «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512;

ж) Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн;

з) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП);

и) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

Приложение 1 . Требования к системе защиты персональных данных.

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
I	В подсистеме управления доступом:			
1	Идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;	-	-	+
3	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;	-	-	+
4	Контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;	-	-	+
II	В подсистеме регистрации и учета:			
1	Регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;	+	+	+
2	Регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатора пользователя, запросившего документ;	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
3	Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешны);	-	-	+
4	Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием её результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;	-	-	+
5	Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа(терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя(номер));	-	-	+
6	Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);	+	+	+
7	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей.	-	-	+
III	В подсистеме обеспечения целостности:			
1	Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных;	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
2	Физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;	+	+	+
3	Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест – программ, имитирующих попытки несанкционированного доступа;	+	+	+
4	Наличие средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности;	+	+	+
IV	Межсетевое взаимодействие			
1	Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);	+	+	+
2	Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;	+	+	+
3	Фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;	-	+	+
4	Фильтрация с учетом любых значимых полей сетевых пакетов;	-	+	+
5	Фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;	-	-	+
6	Фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;	-	-	+
7	Фильтрация с учетом даты и времени;	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
8	Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушивании сети;	-	-	+
9	Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);	-	+	+
10	Регистрация и учет запросов на установление виртуальных соединений;	-	-	+
11	Локальная сигнализация попыток нарушения правил фильтрации	-	-	+
12	Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно – постоянного действия;	+	+	+
13	Предотвращение доступа не идентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;	-	-	+
14	Идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;	-	-	+
15	Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация входа из системы не проводится в моменты аппаратурного отключения межсетевого экрана);	+	+	+
16	Регистрация запуска программ и процессов (заданий, задач);	-	+	+
17	Регистрация действия администратора межсетевого экрана по изменению правил фильтрации;	-	-	+
18	Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;	-	-	+
19	Контроль целостности своей программной и информационной части;	+	+	+
20	Контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;	-	-	+
21	Восстановление свойств межсетевого экрана после сбоев и отказов оборудова-	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	ния.			
22	Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.	+	+	+
V	Подсистема защиты информации от утечки по техническим каналам.			
1	Использовать технических средств в защищенном информации.	-	-	+
2	Использовать средства защиты информации, прошедших в установленном порядке процедуру оценки соответствия.	-	-	+
3	Размещение объектов защиты в соответствии с предписанием на эксплуатацию.	-	-	+
4	Размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средст в пределах охраняемой зоны	-	-	+
5	Обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал	-	-	+
6	Обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории и информационными цепями, по которым циркулирует защищаемая информация.	-	-	+
7	При наличии функций голосового ввода ПДн в ИСПДн или воспроизведения ПДн акустическими средствами ИСПДн: должны быть реализованы мероприятия по защите акустической (речевой) информации. Мероприятия по защите акустической (речевой) информации заключаются в обеспечении звукоизоляции ограждающих конструкций помещений, в которых расположена ИСПДи, их система вентиляции и кондиционирования, не позволяющей прослушивание акустической (речевой) информации при голосовом вводе ПДи в ИСПДн, либо воспроизведении акустическими средствами ИСПДн.	-	-	+
VI	Подсистема антивирусной защиты и защиты от ПМВ.			
1	Должна проводиться автоматическая проверка на наличие вредоносных про-	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	грамм (далее ВП) или последствий программно-математических воздействий (далее ПМВ) при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.			
2	Должны быть реализованы механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.	+	+	+
3	Должна регулярно выполняться проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью).	+	+	+
4	Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП.	+	+	+
5	Должен быть реализован механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.	+	+	+
6	На всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.	+	+	+
7	Должна проводиться проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.	+	+	+
8	Должны быть реализованы механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.	+	+	+
9	Должна быть обеспечена возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программных средств защиты, его периодическое обновление и контроль работоспособности.	+	+	+

Примечание:

1 Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно – аппаратных средств (систем) анализа защищенности.

Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

2 Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно – аппаратных средств (систем) обнаружения вторжений.

3 Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующие 4 уровню контроля отсутствия не декларированных возможностей.

4 Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн.