

УТВЕРЖДАЮ

Директор Ангарского филиала ФГБУ
«ВСНЦ ЭЧ» СО РАМН
В.С. Рязановский
« 21 » 2012 года



ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

информационных систем персональных данных
Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН

Содержание

Определения	3
Обозначения и сокращения	6
Введение.....	7
1 Общие положения	8
2 Область действия.....	9
3 Система защиты персональных данных	10
4 Требования к подсистемам СЗПДн	11
4.1 Подсистемы управления доступом, регистрации и учета	11
4.2 Подсистема обеспечения целостности.....	11
4.3 Подсистема антивирусной защиты.....	12
4.4 Подсистема межсетевое экранирования	12
4.5 Подсистема анализа защищенности	12
4.6 Подсистема обнаружения вторжений	13
4.7 Подсистема криптографической защиты.....	13
4.8 Защита информации от её утечки по техническим каналам	13
5 Категории субъектов доступа ИСПДн	14
5.1 Сотрудники, не имеющие доступа к ПДн.....	14
5.2 Пользователи ИСПДн, работающие локально с ПДн.....	14
5.3 Пользователи ИСПДн, работающие удаленно с ПДн	14
5.4 Администраторы безопасности сегмента ИСПДн	15
5.5 Администраторы ИСПДн	15
5.6 Администраторы безопасности ИСПДн	15
5.7 Технические специалисты по обслуживанию периферийного оборудования.....	16
5.8 Программисты-разработчики специального ПО ИСПДн	16
6 Требования к персоналу по обеспечению защиты ПДн	17
7 Должностные обязанности пользователей ИСПДн	18
8 Ответственность	19
9 Список использованных источников	20

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, характеризующееся 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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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.

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) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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, аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы с использованием технологии межсетевого взаимодействия. межсетевой экран выполняет функцию межсетевого экранирования.

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.

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 (или без иных), 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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

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.

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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.

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

Обозначения и сокращения

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

УБПДн – угрозы безопасности персональных данных

Введение

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в документе «Концепция информационной безопасности информационных систем персональных данных Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, утвержденным директором Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН от 20.09.2012 г.

Политика разработана в соответствии с требованиями:

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 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»;
- приказа Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных".

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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН.

Общие положения

Целью настоящей политики является обеспечение безопасности автоматизированных рабочих мест ИСПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН 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 объектов защиты представлен в перечне персональных данных, подлежащих защите.

Состав ИСПДн подлежащих защите, представлен в отчете о результатах проведения внутренней проверки или акте обследования информационных систем персональных данных.

Область действия

Требования настоящей политики распространяются на всех сотрудников, обрабатывающих автоматизировано ПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц, обрабатывающих ПДн (подрядчики, аудиторы и т.п.).

Система защиты персональных данных

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

- отчета о результатах проведения внутренней проверки (или акта обследования информационной системы персональных данных);
- перечня персональных данных, подлежащих защите;
- акта классификации информационной системы персональных данных;
- частной модели угроз безопасности персональных данных;
- технического задания на разработку системы защиты персональных данных;
- положения о разграничении прав доступа к обрабатываемым персональным данным или матрице доступа;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН. На основании анализа актуальных угроз безопасности ПДн описанного в модели угроз и отчета о результатах проведения внутренней проверки или акта обследования информационной системы персональных данных, 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 должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- СУБД;
- 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;
- межсетевого экранирования;
- защиты от несанкционированного доступа (непосредственного);
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- анализа защищенности (сканеры уязвимостей).

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 должен включать:

- управление доступом субъектов;
- разграничение доступом пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений;
- анализ защищенности.

Список используемых технических средств отражается в плане мероприятий по обеспечению защиты 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 начальником Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН или лицом, ответственным за обеспечение защиты ПДн.

Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты;
- защита информации от её утечки по техническим каналам.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в акте классификации информационной системы персональных данных. Требования к подсистемам предъявляются в зависимости от класса ИСПДн и актуальных угроз безопасности ПДн. В разделе описаны основные требования к подсистемам, требования к подсистемам уточняются в техническом задании на систему защиты для каждой ИСПДн. Используемые программные, программно-аппаратные, аппаратные средства защиты должны пройти процедуру оценки соответствия.

1.1 Подсистемы управления доступом, регистрации и учета

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.

1.2 Подсистема обеспечения целостности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности ПДн, программных и аппаратных средств ИСПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью программно-аппаратных средств защиты информации путем периодического контроля файлов, каталогов, элементов системного реестра по

контрольным суммам, а также организации резервного копирования обрабатываемых данных и ключевых элементов ИСПДн.

1.3 Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты АРМ пользователей ИСПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- автоматизированное обновление антивирусных баз;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения, прошедшего процедуру оценки соответствия.

1.4 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;
- 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 обеспечения;
- 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 на границе защищаемой сети или на каждом защищаемом автоматизированном рабочем месте программно-аппаратных комплексов межсетевого экранирования, прошедших процедуру оценки соответствия.

1.5 Подсистема анализа защищенности

Подсистема анализа защищенности используется для распределенных ИСПДн, подключенных к сетям международного информационного обмена и должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем безопасности персональных данных для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами, прошедшими процедуру оценки соответствия.

1.6 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений используется для ИСПДн, подключенных к сетям международного информационного обмена, и 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, прошедшими процедуру оценки соответствия.

1.7 Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программных или программно-аппаратных комплексов, прошедших процедуру оценки соответствия.

1.8 Защита информации от её утечки по техническим каналам

Защита информации от её утечки по техническим каналам осуществляется для ИСПДн класса защищенности К2 путем использования средств вычислительной техники, удовлетворяющих требования национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники

Защита информации от её утечки по техническим каналам осуществляется для ИСПДн класса защищенности К1 на основании актуальных угроз безопасности ПДн, определенных в Частной модели угроз.

Категории субъектов доступа 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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН можно выделить следующие группы пользователей, участвующих в обработке ПДн:

- Пользователи ИСПДн, работающие локально с ПДн;
- Пользователи ИСПДн, работающие удаленно с ПДн;
- Администраторы безопасности сегмента ИСПДн;
- Администраторы ИСПДн;
- Администраторы безопасности ИСПДн;
- Технические специалисты по обслуживанию периферийного оборудования;
- Программист-разработчик специального ПО ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должен быть отражен в матрице доступа к обрабатываемым персональным данным или технологическом процессе.

1.9 Сотрудники, не имеющие доступа к ПДн

К данной категории относятся сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, не имеющие доступа к ПДн и обладающие следующим уровнем доступа и знаний:

- имеют доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;
- располагают фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;
- располагают именами и могут вести выявление паролей зарегистрированных пользователей;
- могут изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

1.10 Пользователи ИСПДн, работающие локально с ПДн

Пользователи ИСПДн, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, осуществляющие обработку ПДн без применения технологии удаленного доступа. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователи данной категории не имеют полномочий для управления подсистемами СЗПДн.

Пользователи ИСПДн, работающие локально с ПДн обладают следующим уровнем доступа и знаний:

- всеми возможностями предыдущей категории нарушителей;
- знают по меньшей мере одно легальное имя доступа;
- обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагают конфиденциальными данными, к которым имеют доступ.

1.11 Пользователи ИСПДн, работающие удаленно с ПДн

Пользователи ИСПДн, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, осуществляющие обработку ПДн с применением технологии удаленного доступа. Обработка

ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователи данной категории не имеют полномочий для управления подсистемами СЗПДн.

Пользователи ИСПДн, работающие удаленно с ПДн обладают следующим уровнем доступа и знаний:

- всеми возможностями предыдущих категорий нарушителей;
- располагают информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной систем, через которую они осуществляют доступ, и составе технических средств ИСПДн;
- имеют возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

1.12 Администраторы безопасности сегмента ИСПДн

Администраторы безопасности сегмента ИСПДн, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, ответственные за функционирование сегмента СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администраторы безопасности сегмента ИСПДн обладают следующим уровнем доступа и знаний:

- всеми возможностями предыдущих категорий нарушителей;
- обладают полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;
- обладают полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;
- имеют доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;
- имеют доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;
- обладают правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

1.13 Администраторы ИСПДн

Системные администраторы, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, ответственные за функционирование программной и аппаратной части ИСПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Системные администраторы обладают следующим уровнем доступа и знаний:

- всеми возможностями предыдущих категорий нарушителей;
- обладают полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладают полной информацией о технических средствах и конфигурации ИСПДн;
- имеют доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладают правами конфигурирования и административной настройки технических средств ИСПДн.

1.14 Администраторы безопасности ИСПДн

Администраторы безопасности, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, ответственный за функционирование системы защиты ИСПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администраторы безопасности обладают следующим уровнем доступа и знаний:

- всеми возможностями предыдущих категорий нарушителей;

- обладают полной информацией об ИСПДн;
- имеют 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).

1.15 Технические специалисты по обслуживанию периферийного оборудования

Технические специалисты по обслуживанию периферийного оборудования, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН или подрядных организаций, занимающиеся техническим обслуживанием компьютерной техники и сетевого оборудования. Технические специалисты по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и СЗПДн

Технические специалисты по обслуживанию периферийного оборудования обладают следующим уровнем доступа и знаний:

- обладают возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;
- могут располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

1.16 Программисты-разработчики специального ПО ИСПДн

Программисты-разработчики специального ПО ИСПДн, сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН или подрядных организаций, разрабатывающие специальное программное обеспечение для обработки ПДн.

Программисты-разработчики специального ПО ИСПДн обладают следующим уровнем доступа и знаний:

- 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.

Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, 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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, 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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН 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 также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН 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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН 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, ответственному за обработку и защиту ПДн.

Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- инструкция администратора ИСПДн;
- инструкция администратора безопасности ИСПДн;
- инструкция пользователя ИСПДн;
- инструкция резервирования и восстановления персональных данных, ПО, СЗИ;
- инструкция по организации антивирусной защиты в ИСПДн;
- инструкция по эксплуатации СЗИ.

Ответственность

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 Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН – 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 положении по обработке и защите персональных данных в информационной системе Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН.

Необходимо внести в положение об обработке и защиты ПДн Ангарского филиала ФГБУ «ВСНЦ ЭЧ» СО РАМН, 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.

Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая политика являются:

1. 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.
2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства РФ от 17.11.2007 г. № 781;
3. 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.;
4. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.;
6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	K3	K2	K1
I	В подсистеме управления доступом:			
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам);	+	+	+
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;	+	+	+
4	Реализовать контроль доступа субъектов к защищаемым ресурсам;	+	+	+
5	Для обеспечения идентификации пользователей должны использоваться средства защиты информации, прошедшие процедуру оценки защищенности;	+	+	Не ниже 5-го класса защищенности СВТ
6	При наличии подключения ИСПДн к сетям общего пользования должно при- меняться межсетевое экранирование с использованием средств защиты инфор- мации, прошедших процедуру оценки защищенности;	+	+	Не ниже 3-го уровня защищенности
7	Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для раз- ных классов необходимо использовать МЭ, прошедшие процедуру оценки за- щищенности.	+	+	Не ниже 3-го уровня защищенности
II	В подсистеме регистрации и учета:			
1	Осуществлять регистрацию входа (выхода) пользователя в систему (из систе- мы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;	+	+	+

2	Осуществлять регистрацию выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);	-	-	+
3	Осуществлять регистрацию 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, неуспешный);	-	-	+
4	Осуществлять регистрацию 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 ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;	-	-	+
5	Осуществлять регистрацию 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 ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер));	-	-	+
6	Проводить учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;	+	+	+
7	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации;	-	-	+
23	Для обеспечения регистрации и учета действий пользователей должны использоваться средства защиты информации, прошедшие процедуру оценки защищенности;	+	+	Не ниже 5-го класса защищенности СВТ
24	Для регистрации действий пользователя и администратора в системе межсетевой	+	+	Не ниже 3-го

	вого экранирования должны использоваться средства защиты информации, прошедшие процедуру оценки защищенности;			уровня защищенности
25	Для регистрации действий пользователя и администратора в средстве защиты от ПМВ, должны использоваться средства защиты информации, прошедшие процедуру оценки защищенности.	-	-	Не ниже 4-го уровня контроля на отсуствие НДВ
III	В подсистеме обеспечения целостности:			
1	Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;	+	+	+
2	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;	+	+	+
3	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;	+	+	+
4	Должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;	+	+	+
5	Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования с использованием контрольных сумм;	+	+	+
6	Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;	+	+	+
7	Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;	+	+	+

8	Проводить резервное копирование ПДн на отчуждаемые носители информации;	+	+	+	+
IV	В подсистеме антивирусной защиты:				
1	Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;	+	+	+	+
2	Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;	+	+	+	+
3	Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с ус-танавливаемой периодичностью) проверка на предмет наличия в них ВП;	+	+	+	+
4	Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;	+	+	+	+
5	Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и при-кладных программ или программных средств, содержащих ВП;	+	+	+	+
6	Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП;	+	+	+	+
7	Для обеспечения защиты информации от ПМВ должны использоваться антиви-русные средства, прошедшие процедуру оценки защищенности.	+	+	+	Не ниже 4-го уровня контроля на отсутствие НДВ
V	Контроль отсутствия НДВ в ПО СЗИ				
1	Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в обще-системное и прикладное программное обеспечение – ПО), должен быть обеспе-чен соответствующий уровень контроля отсутствия в нем НДВ (не деклариро-ванных возможностей).	-	-	-	Не ниже 4-го уровня контроля на отсутствие НДВ

VI	Обнаружение вторжений в ИСПДн				Не ниже 4-го уровня контроля на отсутствие НДВ
1	Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ);	-			-
2	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа;	-			-
3	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий.	-			-
VII	Защита ИСПДн от ПЭМИН				
1	Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ Р 50628-93, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96).	-			+
VIII	Оценка соответствия ИСПДн требованиям безопасности ПДн				
1	Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации;	+			+