муниципальное автономное общеобразовательное учреждение
муниципального образования город Краснодар средняя общеобразовательная школа № 84
имени Героя Российской Федерации Яцкова Игоря Владимировича
ул. Сормовская,199, г. Краснодар, 350088 тел/факс.(861)236-10-39

МАОУ СОШ № 84

Подписан: МАОУ СОШ № 84
DN: OID.1.2.840.113549.1.9.2=2312045272-231201001-000303758213, E=buh-sosh84@yandex.ru, ИНН=002312045272, СНИЛС=00284943035, ОГРН=1032307160247, T=Директор МАОУ СОШ № 84, STREET="УЛ СОРМОВСКАЯ, ДОМ 199", L=Краснодар, S=23 Краснодарский край, C=RU, G=Ирина Александровна, SN=Устинова, CN=МАОУ СОШ № 84
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2021.04.03 22:29:50+03'00'
Foxit Reader Версия: 10.1.1

УТВЕРЖДАЮ
МАОУ СОШ № 84
_____ И.А. Устинова

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Краснодар

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.

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

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

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.

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 – электрический сигнал, 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 (ст.3 п.9 № 152-ФЗ).

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 (ст.3 п.5 № 152-ФЗ).

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 (ПП №687 от 15.09.08).

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующими 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 (ст.3 п.8 № 152-ФЗ).

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение персональных данных (ст.3 п.3 № 152-ФЗ).

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 (ст.3 п.12 № 152-ФЗ).

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 (ст.3 п.2 № 152-ФЗ).

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 и другая информация (ст.3 п.1 № 152-ФЗ).

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.

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.

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 (ст.3 п.4 № 152-ФЗ).

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

Специальные категории персональных данных – персональные данные, касающиеся расовой и 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.

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.

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 (ст.3 п.11 № 152-ФЗ).

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 – государственное образовательное учреждение города Москвы.

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

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – Политика) МБОУ гимназии № 36 (Далее – Учреждение) 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:

– «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного директором ФСТЭК от 05.01.2010 г. № 58;

– «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 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 объектов защиты представлен в Перечне персональных данных, подлежащих защите.

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

Эта Политика информационной безопасности была утверждена директором МБОУ гимназии № 36 и введена в действие приказом № 101-В от 01.09.2012.

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 проведения внутренней проверки;

– Перечня персональных данных, подлежащих защите;

– Акта классификации информационной системы персональных данных;

– Модели угроз безопасности персональных данных;

– Положения о разграничении прав доступа к обрабатываемым персональным данным;

– Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, 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;

– сервера приложений;

– СУБД;

– граница ЛВС;

– каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

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

– антивирусные средства для рабочих станций пользователей и серверов;

– средства 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;

– обеспечение целостности данных;

– обнаружение вторжений.

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 руководителем Учреждение или лицом, ответственным за обеспечение защиты ПДн.

4 ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

СЗПДн включает в себя следующие подсистемы:

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

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

4.1 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, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрация выдачи печатных (графических) материалов на бумажный носитель;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

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

4.2 Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Учреждения, а так же средств защиты, при случайной или намеренной модификации.

Подсистема обеспечения целостности и доступности предназначена для реализации следующих функций:

– резервное копирование обрабатываемых данных;

– обеспечение целостности программных средств защиты персональных данных, обрабатываемой информации, а так же неизменность программной среды;

– периодическое тестирование функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа;

– наличие средств восстановления системы защиты персональных данных.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, проверкой при загрузке системы контрольных сумм компонентов средств защиты информации, ведением двух копий программных компонент средств защиты информации и их периодическим обновлением и контролем работоспособности, а так же резервированием ключевых элементов ИСПДн.

4.3 Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Учреждения.

Средства антивирусной защиты предназначены для реализации следующих функций:

– резидентный антивирусный мониторинг;

– антивирусное сканирование;

– скрипт-блокирование;

– централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

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

4.4 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

– фильтрацию 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);

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

– фильтрацию с учетом любых значимых полей сетевых пакетов;

– фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

– фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

– фильтрацию с учетом даты и времени;

– аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;

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

– регистрацию и учет запросов на установление виртуальных соединений;

– локальную сигнализацию попыток нарушения правил фильтрации;

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

– предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

– идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

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

– регистрацию запуска программ и процессов (заданий, задач);

– регистрацию 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 регистрации, процесса идентификации и аутентификации запросов, 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.

4.5 Подсистема анализа защищенности

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

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

4.6 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 обнаружения вторжений.

4.7 Подсистема криптографической защиты

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

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

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 безопасности;
- Оператора АРМ;
- Администратора сети;
- Технического специалиста по обслуживанию периферийного оборудования;
- Программист-разработчик ИСПДн.

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

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 БЕЗОПАСНОСТИ

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 безопасности уполномочен:

– реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты;

– устанавливать доверительные отношения своей защищенной сети с сетями других Учреждение.

5.3 Оператор АРМ

Оператор АРМ, сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

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

– располагает конфиденциальными данными, к которым имеет доступ.

5.4 Администратор сети

Администратор сети, сотрудник Учреждения, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

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

– обладает частью информации о технических средствах и конфигурации ИСПДн;

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

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

5.5 Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

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

– обладает частью информации о технических средствах и конфигурации ИСПДн;

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

5.6 Программист-разработчик ИСПДн

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

Лицо этой категории:

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

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

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

6 ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

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

Сотрудники Учреждение 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 Учреждение, 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 Учреждение 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 безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

8 ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ИСПДН УЧРЕЖДЕНИЕ

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего 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 Учреждение – 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 Учреждение, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Учреждение.

Необходимо внести в Положения о подразделениях Учреждение, 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:

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

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

– «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.;

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

– «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.

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

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

– 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)

– «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденное директором ФСТЭК от 05.01.2010 г. № 58

ПРИЛОЖЕНИЕ 1

к Политике информационной безопасности

Таблица 1 Соответствие функций подсистем СЗПДн классу защищенности

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
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, узлов ИСПДн, каналов связи, внешних устройств по их логическим именам.	-	-	При многопользовательском режиме
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам.	-	-	При многопользовательском режиме
4	Реализовать контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.	-	-	При многопользовательском режиме и разных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
II	В подсистеме регистрации и учета:			
5	Осуществлять регистрацию входа (выхода) пользователя в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются:			
	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;	При однопользовательском режиме	При однопользовательском режиме	-
	Дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);	При многопользовательском режиме и равных правах доступа	При многопользовательском режиме и равных правах доступа	При однопользовательском и многопользовательском режимах обработки и равных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
6	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;	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	-
	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.	-	-	При многопользовательском режиме и разных правах доступа
7	Проводить учет всех защищаемых носителей информации с помощью их маркировки:			
	С занесением учетных данных в журнал учета;	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском режиме

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	С занесением учетных данных в журнал учета с пометкой об их выдаче (приеме);	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме
8	Проводить дублирующий учет защищаемых носителей информации.	-	-	При однопользовательском и многопользовательском режимах и равных правах доступа
9	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);	-	-	При однопользовательском режиме
	Дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего	-	-	При многопользовательском режиме

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	документ.			
10	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).	-	-	При многопользовательском режиме
11	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.	-	-	При многопользовательском режиме
12	Осуществлять регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам,	-	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	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)).			
13	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации.	-	-	+
III	В подсистеме обеспечения целостности:			
14	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) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа	При однопользовательском и многопользовательском режимах и равных правах доступа

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	При загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме и разных правах доступа	При многопользовательском режиме обработки и разных правах доступа
15	Осуществлять физическую охрану технических средств информационной системы (устройств и носителей информации), предусматривающую постоянное наличие охраны территории и здания.	-	-	При однопользовательском и многопользовательском режимах и равных правах доступа
16	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающую контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации.	+	+	При многопользовательском режиме обработки и разных правах доступа
17	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и пользователей ИСПДн с помощью тест-программ, имитирующих попытки НСД.	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
18	Должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.	+	+	+
I V	Требования к средствам межсетевого экранирования при подключении ИСПДн к сетям международного информационного обмена			
19	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).	+	+	+
20	Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.	-	+	+
21	Фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов.	-	+	+
22	Фильтрация с учетом любых значимых полей сетевых пакетов; регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации).	-	+	+
23	Фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	отправителя и получателя.			
24	Фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя.	-	-	+
25	Фильтрацию с учетом даты и времени.	-	-	+
26	Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети.	-	-	+
27	Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия.	+	+	+
28	Идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации.	-	-	+
29	Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана).	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
30	Регистрация запуска программ и процессов (заданий, задач).	-	+	+
31	Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации).	-	-	+
32	Регистрация и учет запросов на установление виртуальных соединений	-	-	+
33	Регистрация действий администратора межсетевого экрана по изменению правил фильтрации.	-	-	+
34	Локальная сигнализация попыток нарушения правил фильтрации.	-	-	+
35	Предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась.	-	-	+
36	Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.	-	-	+
37	Контроль целостности своей программной и информационной части; фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой	+	+	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	сетевых устройств.			
38	Контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.	-	-	+
39	Восстановление свойств межсетевого экрана после сбоев и отказов оборудования.	+	+	+
40	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	При применении в ИСПДн функции голосового ввода ПДн в ИС или функции воспроизведения информации акустическими средствами ИС			
41	Реализовать организационные и технические меры для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при	-	-	+

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
	голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.			
VI	Требования к программному обеспечению средств защиты информации и средствам вычислительной техники			
42	Применять программное обеспечение средств защиты информации, соответствующее 4 уровню контроля отсутствия недекларированных возможностей.	-	-	+
43	Использовать средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.	-	+	-

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