Приложение

УТВЕРЖДЕНО
Приказом №0007-З от 15.08.2016г.

Политика
информационной безопасности информационных систем персональных данных Главного управления спорта Смоленской области

г.Смоленск
2016

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

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

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

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

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

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

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

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

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

Доступ к информации - возможность получения информации и ее использования.

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

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

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

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

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

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

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

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

Контролируемая зона- пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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

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

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

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

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

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

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

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

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных

или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Угрозы безопасности персональных данных- совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных- действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

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 СВТ - средства вычислительной техники **СЗИ** - средства защиты информации
СиЗИ ПДн - система (подсистема) защиты персональных данных **СОВ** - система обнаружения вторжений **ТКУ И** - технические каналы утечки информации **УБПДн** - угрозы безопасности персональных данных

ВВЕДЕНИЕ

Политика информационной безопасности разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПДн Главного управления спорта Смоленской области (далее- Управление).

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение
безопасности персональных данных в ИСПДн Управления.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Управления 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 Обследования.

2. Область действия

Субъектами настоящей Политики информационной безопасности являются все лица, вовлеченные в организационные и технологические (бизнес) процессы сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачу), обезличивания, блокирования, уничтожения персональных данных, обрабатываемых ИСПДн Управления.

3. Система защиты персональных данных

Система защиты персональных данных (СиЗИ ПДн), строится на основании:

- отчета о результатах проведения Обследования;
- 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 Управления. На основании анализа актуальных угроз безопасности ПДн описанного в Частной модели угроз и Отчета о результатах проведения Обследования, 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, СиЗИ ПДн 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 программным обеспечением 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 начальником Управления или лицом, ответственным за обеспечение защиты ПДн.

4. Требования к подсистемам СиЗИ ПДн

СиЗИ ПДн может включать в себя следующие подсистемы:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема антивирусной защиты;
- подсистема межсетевого экранирования;
- подсистема аудита безопасности;
- подсистема обнаружения вторжений;
- подсистема криптографической защиты;
- подсистема управления процессами обеспечения безопасности;
- подсистема защиты информации от утечки по техническим каналам. Подсистемы СиЗИ ПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

4.1. Подсистема управления доступом

Подсистема управления доступом предназначена для управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного идентификатора). Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленного идентификатора с перечнем зарегистрированных) и аутентификации (подтверждение подлинности) с защитой от раскрытия пароля.

Подсистема управления доступом включает в себя:

- подсистему контроля и управления доступом в помещения;
- подсистему физической защиты;
- подсистему контроля доступа и разграничения полномочий пользователей.

Подсистема контроля и управления доступом в помещения

Контроль и управление доступом в помещения осуществляется с использованием совокупности организационных мероприятий и средств физической защиты - систем инженерно-технических средств охраны объектов.

Подсистема контроля доступа в помещения (ПКДП) должна обеспечивать выполнение следующих основных функций:

- поддержание дверей в запертом состоянии;
- распознавание «своих» и обеспечение им свободного передвижения;

- распознавание «чужих» и сигнализация о нарушении прав доступа.

Подсистема Физической защиты

Физическая защита объектов осуществляется с целью своевременного обнаружения фактов несанкционированного проникновения на охраняемую территорию, в выделенные помещения, а также для обеспечения сохранности средств информатизации.

Физическая защита охраняемых территорий, помещений и средств осуществляется путем реализации организационных мер (пропускной режим, дислокация, тактика действий подразделений охраны) в сочетании с построением- систем инженерно-технических средств охраны, предотвращающими проникновение в здания, выделенные помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации и исключающими нахождение внутри контролируемой (охраняемой) зоны средств технической разведки.

Основными задачами физической защиты объектов являются:

- реализация организационных и инженерно-технических мер на объектах по построению и обеспечению функционирования систем охраны, предусматривающих многорубежность построения (территории, здания, помещения и т.д.) с комплексным применением современных технических средств охраны, видео наблюдения, сбора и обработки информации, обеспечивающих надежное обнаружение фактов несанкционированного проникновения в охраняемую зону, достоверное отображение и объективное документирование событий;
- ограничение доступа посторонних лиц в здания и помещения, где размещены средства вычислительной техники и коммуникации, на которых обрабатывается (хранится, передается) конфиденциальная информация, непосредственно к самим средствам информатизации и коммуникациям.

В целях обеспечения комплексной безопасности информации физической защите подлежат следующие объекты ИСПДн:

- помещения, в которых установлены серверы баз данных (электронные архивы) и коммуникационные серверы («серверные») - в случае, когда они устанавливаются в отдельном помещении;
- помещения, в которых хранятся носители информации («хранилища»);
- узлы связи;
- коммуникации ИСПДн;
- системы электропитания (автономные источники электропитания).

Помещения ИСПДн должны размещаться в охраняемых зонах, а его «серверные» - в специально приспособленных для этого зонах ограниченного доступа. Доступ в эти помещения должен быть ограничен и строго дифференцирован по выполняемым функциям персонала.

Обслуживание «серверной» обеспечивается персоналом подразделения защиты информации (специалистами подразделений, осуществляющих эксплуатацию серверов, ответственными за обеспечение безопасности) совместно с выделенными для этих целей специалистами подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи, электропитания, кондиционирования и т.п.

Помещение «серверной», не требующее постоянного присутствия обслуживающего персонала, оборудуется техническими средствами охраны в соответствии с категорией охраняемого объекта и степенью конфиденциальности обрабатываемой и хранимой информации.

Информация баз данных (электронных архивов) должна дублироваться и одна из копий должна быть помещена в хранилище носителей информации, обслуживающее ИСПДн.

Хранилища носителей информации должны размещаться в специально приспособленных для этого зонах ограниченного доступа. Они должны быть оборудованы техническими средствами охраны в соответствии со степенью конфиденциальности хранимых в них информационных носителей, и сдаваться под охрану в нерабочее время.

Узлы связи, распределительное и коммуникационное оборудование ИСПДн должны размещаться в пределах контролируемой зоны, или быть защищены от несанкционированного вскрытия техническими средствами охраны.

Электрические установки и кабели, предназначенные для электропитания технических средств (включая трансформаторные подстанции, автономные источники, устройства защиты) должны размещаться в пределах контролируемой зоны.

Подсистема контроля доступа и разграничения полномочий пользователей

Подсистема контроля доступа и разграничения полномочий пользователей (ПКДРП) предназначена для управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа.

ПКДРП обеспечивает выполнение следующих функций:

- идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних устройств компьютеров по логическим именам и (или) адресам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- управление потоками информации с помощью меток конфиденциальности, при этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Реализация функций ПКДРП обеспечивается:

- идентификацией и аутентификацией субъектов доступа;
- контролем доступа субъектов к защищаемым объектам в соответствии с правами и правилами доступа.

В состав ПКДРП могут входить:

Модуль контроля доступа

Функциональное предназначение:

Для ИСПДн **2:3 уровня защищенности ПДн. (при однопользовательском режиме** обработки ПДн)

- идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Для ИСПДн **2:3 уровня защищенности ПДн (при многопользовательском режиме** обработки ПДн и **равных правах** доступа к ним пользователей):

- идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Для ИСПДн **2:3 уровня защищенности ПДн. (при многопользовательском режиме** обработки ПДн и **разных правах** доступа к ним пользователей):

- идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не мене шести буквенно- цифровых символов.

Модули подсистемы контроля доступа и разграничения полномочий пользователей могут реализовываться:

- штатными средствами обработки ПДн (операционных систем, приложений и СУБД).
- специальными программно-техническими средствами или комплексами осуществляющими дополнительные меры по аутентификации и контролю доступа.

Модули подсистемы контроля доступа и разграничения полномочий пользователей могут размещаться:

на уровне АРМ ИСПДн:

- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн;

на уровне серверов ЛВС ИСПЛн:

- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

4.2. Подсистема регистрации и учета

Подсистема регистрации и учета предназначена для сбора и накопления сведений о событиях, происходящих в ИСПДн.

Данная подсистема не используется непосредственно для предотвращения нарушений безопасности, она необходима для обнаружения, записи и анализа событий, связанных с обеспечением безопасности информации.

Подсистема регистрации и учета обеспечивает выполнение следующих функций:

- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн;
- регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача может сопровождаться автоматической маркировкой каждого листа (страницы) документа, его последовательным номером и учетными реквизитами ИСПДн с указанием на последнем листе документа общего количества листов (страниц);
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий);
- регистрация попыток доступа программных средств к защищаемым файлам.

В параметрах регистрации могут быть указаны:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей
- доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление и т.п.);
- регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- регистрация изменений полномочий субъектов доступа и статуса объектов доступа;
- автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом.

Маркировка должна отражать уровень конфиденциальности объекта:

- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
- сигнализация попыток нарушения защиты.

Функции подсистемы регистрации и учета могут реализовываться в ИСПДн модулем регистрации и учета и организационными мерами:

Модуль регистрации и учета

Функциональное предназначение:
Для ИСПДн **2:3 уровня защищенности ПДн (при однопользовательском режиме** обработки ПДн):

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова, регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета.

Для ИСПДн **2:3 уровня защищенности ПДн (при многопользовательском режиме** обработки ПДн и **равных правах** доступа к ним пользователей):

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета.

Для ИСПДн **2:3 уровня защищенности ПДн (при многопользовательском режиме** обработки ПДн и **разных правах** доступа к ним пользователей):

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

Модули подсистемы регистрации и учета могут быть реализованы:

1) Штатными средствами обработки ПДн (операционных систем, приложений и СУБД).
2) Специальными программно-техническими средствами или комплексами, осуществляющими дополнительные меры по регистрации и учету.

Модули подсистемы регистрации и учета могут размещаться: *на уровне АРМ ИСПДн:*

- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн;

на уровне серверов ЛВС ИСПДн:

- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

Организационные меры:

- учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- организация нескольких видов учета (дублирующих) защищаемых носителей информации.

4.3. Подсистема обеспечения целостности

Подсистема обеспечения целостности и доступности (ПОЦД) предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) программной среды, в том числе программных средств ИСПДн, обрабатываемых ПДн, обеспечивая при этом защиту от внедрения программных закладок и вирусов.

ПОЦД обеспечивает выполнение следующих функций:

- обеспечение целостности программных средств СиЗИ ИСПДн, а также неизменность программной среды и обрабатываемых ПДн;
- периодическое тестирование всех функций СиЗИ ИСПДн с помощью специальных программных средств не реже одного раза в шесть месяцев.

ПОЦД может быть реализована модулем обеспечения целостности и доступности в сочетании с организационными мерами.

Модуль обеспечения целостности:

Функциональное предназначение:

Для ИСПДн **2:3 уровня защищенности ПДн (при однопользовательском** режиме **обработки ПДн):**

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;
- физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Для ИСПДн **2:3 уровня защищенности ПДн (при многопользовательском** режиме **обработки ПДн и** равных правах **доступа к ним пользователей):**

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;
- физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Для ИСПДн **2:3 уровня защищенности ПДн (при многопользовательском** режиме **обработки ПДн и** разных правах **доступа к ним пользователей):**
- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется 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;
- физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

Модули подсистемы обеспечения целостности и доступности могут быть реализованы:
1) Штатными средствами обработки ПДн (операционных систем, приложений и СУБД);
2) Специальными программно-аппаратными средствами или комплексами осуществляющими дополнительные меры по обеспечению целостности и доступности (системы резервного копирования ПДн, программы подсчета контрольных сумм и т.д.).

Модули подсистемы обеспечения целостности и доступности могут размещаться:

на уровне АРМ ИСПДн:
- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

на уровне серверов ЛВС ИСПДн:
- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

Организационные меры:
- физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается ИСПДн, с помощью технических средств охраны и специального персонала, использование пропускного режима, специальное оборудование помещений ИСПДн;
- должен быть предусмотрен администратор (служба) защиты информации (должностное лицо) ответственное за ведение, нормальное функционирование и контроль работы СиЗИ

ИСПДн Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность ИСПДн;
- должен быть разработан и утвержден регламент проверки целостности и доступности определяющий порядок и сроки проведения проверочных мероприятий.

4.4. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн один раз в месяц.

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.

Функции подсистемы антивирусной защиты реализуются модулем антивирус.

Модуль антивирус

Функциональное предназначение:
- постоянный контроль вирусной активности;
- систематический контроль служебных областей дисков, файлов и папок;
- восстановление зараженных файлов.

Модуль работает в трех режимах:

1. Режим «базисного» уровня защиты;
2. Режим «повышенной бдительности»;
3. Режим ликвидации заражения программным вирусом.

В режиме «базисного уровня» защиты обеспечивается решение следующих задач:
- периодический контроль целостности программного обеспечения и файловой структуры программой-ревизором, а также контроль целостности и оптимизация файловой структуры;
- сегментация дисков и сетевых ресурсов с защищенными от записи разделами;
- использование резидентных средств защиты на узлах ИСПДн;
- использование средств разграничения доступа и блокирования несанкционированного запуска программ;
- периодическое обновление версий используемых антивирусных программ;
- периодическое обновление антивирусных баз;
- контроль передаваемых по линиям связи данных с помощью элементов каталога детекторов.

В режиме «повышенной бдительности» обеспечивается решение следующих задач:
- принудительная проверка всех поступивших носителей информации и программного обеспечения на наличие программных вирусов;
- сплошной входной контроль новых программных средств и файлов с документацией;
- использование резидентных средств защиты и программ-ловушек.

В режиме ликвидации заражения программным вирусом обеспечивается решение следующих задач:
- приостановка выполнения решаемых задач в очаге заражения;
- устранение очага заражения антивирусной программой;
- восстановление исходного состояния файлов с использованием резервных копий и архивов последней контрольной точки перед заражением.

Модуль антивирус реализуется специализированными программными средствами и комплексами и может размещаться:

на уровне АРМ ИСПДн:
- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн; *на уровне серверов ЛВС ИСПДн:*
- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

4.5. Подсистема межсетевого экранирования Подсистема межсетевого экранирования предназначена для реализации следующих функций:
- фильтрации открытого и зашифрованного (закрытого) IP-трафика по заданным параметрам;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом 1P-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 останова;
- 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 не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Функции подсистемы межсетевого экранирования реализуются модулем Межсетевой экран.

Модуль Межсетевой экран

Функциональное предназначение:

Для ИСПДН. **2:3 УРОВНЯ защищенности ПДн:**
- 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);
- идентификация и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- 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);
- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий

администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Межсетевые экраны, которые обеспечивают выполнение указанных выше функций, применяются в распределенных информационных системах 1,2,3 классов при их разделении на отдельные части.

Модули подсистемы межсетевого экранирования реализуются внедрением программно-аппаратных комплексов и могут размещаться: *на уровне АРМ ИСПДн (Персональные межсетевые экраны):*

- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

на уровне серверов ЛВС ИСПДн (Корпоративные межсетевые экраны):

- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

на границах ЛВС ИСПДн (Корпоративные межсетевые экраны):

- активном сетевом оборудовании;
- веб-серверах;
- прокси-серверах и т.д.

4.6. Подсистема анализа защищенности

Подсистема анализа защищенности, реализуется модулем «Анализ защищенности» в распределенных ИСПДн и ИСПДн, подключенных к сетям международного информационного обмена.

Модуль Анализ защищенности

Функциональное предназначение:

- выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

Модули подсистемы анализа защищенности реализуются программными или программно-аппаратными средствами (системами) анализа защищенности и могут размещаться:

на уровне АРМ ИСПДн :

- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

на уровне серверов ЛВС ИСПДн :

- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

на границах ЛВС ИСПДн:

- активном сетевом оборудовании;
- веб-серверах;
- прокси- серверах и т.д.

4.7. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, реализуется модулем Обнаружения вторжений в ИСПДн подключенных к сетям международного информационного обмена.

Модуль Обнаружения вторжений

Функциональное предназначение:

- выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Модули подсистемы обнаружения вторжений реализуются программными или программно-аппаратными средствами (системами) обнаружения вторжений и могут размещаться:

на уровне АРМ ИСПДн :

- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

на уровне серверов ЛВС ИСПДн :

- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

на границах ЛВС ИСПДн:

- активном сетевом оборудовании;
- веб-серверах;
- прокси- серверах и т.д.

4.8. Подсистема криптографической защиты

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

Криптографическая подсистема предназначена для реализации функций криптографического преобразования данных, в том числе:

- генерация и распределение ключевой информации между элементами ИСПДн;
- управление ключевой информацией;
- шифрование/дешифрование информации;
- взаимодействие с подсистемами управления процессами обеспечения безопасности информации, контроля доступа к ресурсам и аудита.

Криптографическая подсистема может быть реализована модулем криптографической защиты.

Модуль криптографической защиты

Функциональное предназначение:

- шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные портативные носители данных (дискеты, usb -носители и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа;
- создание каналов связи, обеспечивающих защиту передаваемой информации;
- принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

- аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
- обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;
- обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя;

Модули подсистемы криптографической защиты реализуются криптографическими программными или программно-аппаратными средствами (системами) и могут размещаться:

на уровне АРМ ИСПДн:
- АРМы пользователей ИСПДн;
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

на уровне серверов ЛВС ИСПДн:
- файловых серверах;
- серверах баз данных;
- серверах приложений;
- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

на границах ЛВС ИСПДн:
- активном сетевом оборудовании;
- веб-серверах;
- прокси- серверах и т.д.

4.9. Подсистема управления процессами обеспечения безопасности

Подсистема управления процессами обеспечения безопасности информации имеет целью обеспечение эффективного функционирования СиЗИ ИСПДн, согласно принятой политике безопасности.

Данная цель достигается совокупностью организационных и технических мероприятий, направленных на эффективное функционирование каждой подсистемы (элемента) СиЗИ ИСПДн, выявление и устранение возможных каналов утечки информации, выработку предложений по повышению эффективности мероприятий по защите информации.

Подсистема управления процессами обеспечения безопасности информации осуществляет управление всеми ресурсами СиЗИ ИСПДн во всех режимах ее работы. При этом основное внимание уделяется организации взаимодействия всех подсистем СиЗИ ИСПДн в процессе контроля прав пользователей по использованию информационных и функциональных ресурсов ИСПДн

На структурном уровне подсистема управления обеспечением безопасности информации пронизывает все сегменты ИСПДн и СиЗИ ИСПДн. Для управления обеспечением безопасности информации (ОБИ) в ИСПДн должны выделяться должностные лица, ответственные за настройку и функционирование элементов СиЗИ ИСПДн и имеющие иерархическую подчиненность в соответствии с масштабами и принадлежностью ИСПДн:
- главный администратор информационной безопасности ИСПДн;
- администраторы информационной безопасности сегментов ИСПДн;
- внештатные ответственные по ОБИ.

Подсистема управления процессами обеспечения безопасности информации обеспечивает:
- работу администраторов информационной безопасности, ответственных за ведение, нормальное функционирование и контроль работы СиЗИ ИСПДн;
- функциональный контроль состояния СиЗИ ИСПДн;

- доведение команд управления администраторов информационной безопасности до подсистем и элементов СиЗИ ИСПДн;
- контроль выполнения команд и функционирования подсистем и средств защиты;
- анализ возможных нарушений информационной безопасности, подготовка предложений по совершенствованию принятых решений по обеспечению безопасности информации;
- взаимодействие с вышестоящими и нижестоящими звеньями управления безопасностью информации.

Реализация функций подсистемы управления процессами обеспечения безопасности информации осуществляется с использованием организационных и технических мероприятий.

Технические мероприятия

Функции управления безопасностью (сервисы), встроенные в специальные локальные, и сетевые средства защиты информации настроены таким образом, чтобы обеспечивалось доведение до АРМ администратора информационной безопасности информации о состоянии средств защиты в СиЗИ ИСПДн и изменении режимов функционирования соответствующих средств защиты, а также доведение управляющих воздействий администратора информационной безопасности СиЗИ ИСПДн.

В состав подсистемы управления процессами обеспечения безопасности информации входят:

Модуль аудита безопасности объектов СиЗИ ИСПДн

Функциональное предназначение:

- контроль состояния СиЗИ ИСПДн;
- регистрация всех обращений к защищаемым ресурсам;
- сигнализация о попытках НСД к защищаемым ресурсам;
- установление подлинности (идентификации) всех лиц, обращающихся к защищаемой информации, программам и техническим средствам.

Модуль управления безопасностью объектов СиЗИ ИСПДн

Функциональное предназначение:

- защита программного обеспечения от несанкционированной модификации;
- управление запуском задач;
- предотвращение несанкционированного использования инструментальных средств;
- блокировка ПЭВМ на время отсутствия пользователя либо при его не опознании;
- первичный ввод и модификация списка зарегистрированных пользователей и их полномочий;
- удаленное администрирование информационной безопасности;
- регистрация пользователей с указанием их полномочий;
- назначение/изменение пароля для аутентификации;
- задание привилегированных пользователей;
- установка временных ограничений для работы пользователей;
- задание уровня детализации журнала аудита;
- задание параметров управления экраном пользователей (гашение экрана через установленный интервал времени при бездействии пользователя).

Модули аудита и управления безопасностью СиЗИ ИСПДн могут реализовываться программно-аппаратными СЗИ, которые размещаются:

<u>на уровне АРМ ИСПЛн:</u>

- АРМы пользователей ИСПДн
- АРМы системных администраторов ИСПДн;
- АРМы администраторов безопасности ИСПДн.

<u>на уровне серверов ЛВС ИСПЛн:</u>

- файловых серверах;
- серверах баз данных;
- серверах приложений;

- серверах электронной почты;
- серверах каталогов;
- серверах печати;
- серверах безопасности и т.д.

на границах ЛВС ИСПДн:
- активном сетевом оборудовании;
- веб-серверах;
- прокси- серверах и т.д.

на уровнях АРМ пользователей, серверов и границах ИСПДн - размещаются соответствующие части распределенной трассы аудита безопасности, а также служебная информация, необходимая для функционирования локальных и сетевых средств защиты информации в пределах данной ЛВС.

на серверах безопасности ИСПДн - храниться защищенная информационная база управления процессами обеспечения безопасности информации, заархивированная трасса аудита безопасности объектов ЛВС, а также служебная информация, необходимая для функционирования всех локальных и сетевых средств защиты информации ИСПДн (ключи генерации паролей, база данных паролей пользователей и т.д.).

В подсистему управления процессами обеспечения безопасности информации также может входить специализированная подсистема формирования и распределения парольной информации, которая обеспечивает управление паролями в ИСПДн.

Организационные мероприятия

Организационными мероприятиями по реализации функций подсистемы управления процессами обеспечения безопасности информации должны являться следующие:
- установление должностных лиц, ответственных за ОБИ, и разработка для них функциональных обязанностей;
- определение перечня защищаемых ресурсов;
- организация разграничения доступа должностных лиц (пользователей и обслуживающего персонала) в ЛВС ИСПДн, к техническим средствам информации;
- определение и ввод полномочий пользователей и программных процессов в СиЗИ ИСПДн;
- организация учета, хранения, уничтожения, ремонта машинных носителей информации и порядка обращения с ними;
- обучение (подготовка) пользователей порядку и правилам работы с программно-аппаратными средствами объекта, порядку использования средств защиты информации;
- организация допуска личного состава к самостоятельной работе.
- настройка и управление средствами защиты;
- определение порядка поставки, закрепления, ввода в эксплуатацию копирования, тиражирования, доработки, восстановления программного обеспечения;
- организация паролирования;
- определение периодичности и порядка смены средств опознавания и разграничения доступа (паролей, личных идентификаторов);
- определение периодичности и порядка использования средств антивирусной защиты;
- анализ возможных каналов утечки информации и выработка предложений по их закрытию;
- определение порядка действий при стихийных бедствиях и внезапном нападении противника;
- организация контроля за состоянием защиты информации и работой пользователей ИСПДн в части соблюдения требований по защите информации.

4.10. Подсистема защиты информации от утечки по техническим каналам

Подсистема защиты информации от утечки по техническим каналам предназначена для противодействия утечкам ПДн по техническим каналам.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, должна осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз

применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, определенные с учетом частной модели угроз.

При применении в информационных системах функции голосового ввода персональных данных в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для ИСПДн 1 класса реализуются методы и способы защиты акустической (речевой) информации. Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами. Величина звукоизоляции может, определяется исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в информационной системе.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн , в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

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 Управления можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратора ИСПДн;
- администратора безопасности ИСПДн;
- пользователь ИСПДн;
- 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, работник ИСПДн Управления, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (пользователя ИСПДн) 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 ИСПДн

Администратор безопасности, работник ИСПДн Управления, ответственный за функционирование СиЗИ ПДн, 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 ЛВС.

5.3. Пользователь ИСПДн

Пользователь ИСПДн, работник Управления, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Пользователь не имеет полномочий для управления подсистемами обработки данных и СиЗИ ПДн.

Пользователь 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. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, работник ИСПДн Управления, 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.

5.5. Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как работники ИСПДн Управления, так и работники 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 работники ИСПДн Управления, 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 работника 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.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СиЗИ ПДн.

Работники ИСПДн Управления, 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.

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

Работники Управления 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.

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

Работникам **запрещается разглашать защищаемую информацию,**
которая стала им известна при работе с информационной системой, третьим лицам.

При работе с ПДн в ИСПДн работники Управления обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

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

Работники Управления 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 работников, которые нарушили принятые политику и процедуры безопасности ПДн.

Работники 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 работников ИСПДн Управления

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 работниками Управления 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 ИСПДн Учреждения, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях работников ИСПДн Управления.

Необходимо внести в Положения о подразделениях ИСПДн Управления, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и работников 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 настоящая Политика являются:

1. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
2. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
5. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

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

8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
10. Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Нормативно-методические документы Федеральной службы безопасности России:

11. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации ФСБ (утверждены руководством 8 Центра ФСБ России 21 февраля 2008г. № 149/54-144);
12. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622).