УТВЕРЖЕНО

Приказом Министерства культуры

Республики Алтай

от «21 »октября 2009 г. №217/1

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МИНИСТЕРСТВА КУЛЬТУРЫ РЕСПУБЛИКИ АЛТАЙ

2009г.

ЛИСТ СОГЛАСОВАНИЯ

Ответственные должностные лица:

Должность ответственного лица	**ФИО**	**Подпись**	**Дата**
Заместитель Министра культуры	Мундусов С.М.		
Программист	Толбин В.С.		

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ.

АВС – антивирусные средства;

ВП – выделенное помещение;

ВТСС – вспомогательные технические средства и системы;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

МЭ – межсетевой экран;

НДВ – не декларированные возможности;

НМД – нормативно-методическая документация;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных:

СОВ – система обнаружения вторжений.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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.

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 к информации - возможность получения информации и ее использования.

Защищаемая информация - информация, являющаяся предметом

собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Информационная система персональных данных - 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 так средств.

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

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.

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

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.

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.

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.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие 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).

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 программу с целью осуществить утечку, изменить, блокировать, уничтожать 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.

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

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

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

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

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

Уничтожение персональных данных - действия, в результате которых 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.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение положения

Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Министерства культуры Республики Алтай (далее по тексту – «Положение») разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Трудовым кодексом РФ, Положением о Министерстве культуры Республики Алтай (далее по тексту – «Организация»).

Положение устанавливает порядок организации и проведения работ по обеспечению безопасности ПДн в ИСПДн Организации на протяжении всего жизненного цикла ИСПДн.

1.2 Нормативно-методическая документация по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн

При организации и проведении работ по обеспечению безопасности ПДн необходимо руководствоваться следующими нормативными и методическими документами:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- «Положение об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных» (утв. постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781).
- Совместный приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.).
- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.).
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.).
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.).
- «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» (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622).
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144).

2. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАНОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн. Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в информационной системе информационные технологии.

2.1 Организационные мероприятия

Организационные меры по защите ПДн включают в себя следующие мероприятия:

2.1.1 Определение перечня персональных данных, обрабатываемых на предприятии.

В первую очередь, необходимо установить перечень персональных данных (ПДн) физических лиц, которые обрабатываются на предприятии.

2.1.2 Определение цели обработки персональных данных.

Затем нужно определить цели обработки персональных данных: трудовые отношения с работниками; оформление пропусков для входа на территорию предприятия; договор оказания услуг и т.п.

2.1.3 Определение сроков обработки и хранения ПДн.

Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых ПДн подлежат уничтожению. Установить перечень ПДн, по которым цели обработки достигнуты.

Для целей, указанных в п.п. 2.1.1-2.1.3 формируется и утверждается «Перечень ПДн» (Форма в Приложении 1).

2.1.4 Определение ответственных за обеспечение безопасности ПДн.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн руководством Организации назначается структурное подразделение (или должностное лицо), ответственное за обеспечение безопасности ПДн. Для каждого вида ПДн может быть назначен свой ответственный за обеспечение безопасности ПДн.

2.1.5 Определение круга лиц, допущенных к обработке персональных данных.

Для этой цели формируется «Перечень лиц, допущенных к обработке ПДн» (Форма в Приложении 1).

2.1.6 Организация доступа в помещения, где осуществляется обработка ПДн.

Должна осуществляться физическая охрана помещений ИСПДн.

Доступ в помещения, где обрабатываются ПДн, лицам, не допущенным к обработке ПДн, должен быть по возможности запрещен. В случае невозможности запретить доступ в помещения, необходимо исключить возможность несанкционированного доступа к техническим средствам обработки ПДн, хищение и нарушение работоспособности, хищение носителей информации.

2.1.7 Обучение сотрудников.

Не реже одного раза в год необходимо проводить обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними. Также проводится обучение сотрудников

Организации, допущенных к обработке ПДн, правилам обработки ПДн, в соответствии с утвержденными требованиями.

2.1.8 Установление персональной ответственности за нарушения правил обработки ПДн.

В должностные инструкции сотрудников, допущенных к обработке ПДн, должны быть внесены изменения в части персональной ответственности за нарушение правил обработки ПДн.

2.1.9 Учет применяемых технических средств защиты персональных данных.

Для этой цели формируется «Паспорт ИСПДн» (Форма в Приложении 1).

2.1.10 Учет носителей персональных данных.

В обязательном порядке должен проводиться учет всех защищаемых носителей персональных данных.

2.1.11 Разработка организационно – распорядительных документов (далее ОРД).

Необходимо разработать пакет ОРД, которые будут регламентировать весь процесс получения, обработки, хранения, передачи и защиты персональных данных. Набор ОРД приведен в разделе 2.5.

2.2 Технические мероприятия

Технические меры защиты ПДн предполагают использование программно - аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов предприятия.

2.2.1 Требования к техническим и программным средствам.

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

2.2.2 Необходимость создания СЗПДн

Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности ПДн для ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности ПДн для данной ИСПДн.

2.3 Создание СЗПДн

Рекомендуются следующие стадии создания СЗПДн:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на создание СЗПДн;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также о соответствия ИСПДн требованиям безопасности информации.

2.3.1 Предпроектная стадия

2.3.1.1 На предпроектной стадии по обследованию ИСПДн выполняются следующие мероприятия:

1) Устанавливается необходимость обработки ПДн в ИСПДн.
2) Определяется перечень ПДн, подлежащих защите.
3) Определяются условия расположения ИСПДн относительно границ контролируемой зоны.

4) Определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения.
5) Определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке.
6) Определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах.
7) Уточняется степень участия персонала в обработке ПДн, характер их взаимодействия между собой.
8) Определяются (уточняются) угрозы безопасности ПДн к конкретным условиям функционирования (разработка Частной модели угроз ПДн).
9) Определяется класс ИСПДн.

Классификация ИСПДн проводится в соответствии с порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

2.3.1.2 По результатам предпроектного обследования на основе методического документа «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.), с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности ПДн (оформляется документ «Требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн»), включаемые в техническое (частное техническое) задание на разработку СЗПДн.

2.3.1.3 Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;
- класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

2.3.2 Стадия проектирования

На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

1) Разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн.
2) Разработка раздела технического проекта на ИСПДн в части защиты информации.
3) Строительно-монтажные работы в соответствии с проектной документацией.

4) Использование серийно выпускаемых технических средств обработки, передачи и хранения информации.

5) Разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями.

6) Использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка.

7) Сертификация по требованиям безопасности информации программных средств защиты информации, в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации.

8) Разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации.

9) Определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности ПДн.

10) Разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов).

2.3.3 Стадия ввода в действие

2.3.3.1 На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:

1) Генерация пакетов прикладных программ в комплексе с программными средствами защиты информации.
2) Опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн.
3) Приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

4) Организация охраны и физической защиты помещений ИСПДн, и исключающих несанкционированный доступ к техническим средствам ИСПДн, хищение и нарушение работоспособности, хищение носителей информации.
5) Оценка соответствия ИСПДн требованиям безопасности ПДн.

2.3.3.2 Оценка соответствия ИСПДн по требованиям безопасности ПДн проводится:

- для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация по требованиям безопасности информации);
- для ИСПДн 3 класса - декларирование соответствия требованиям безопасности информации (оформляется документ «Декларация соответствия ИСПДн, требованиям по обеспечению безопасности ПДн»);
- для ИСПДн 4 класса оценка соответствия проводится по решению руководства Организации.

2.4 Лицензирование

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» для проведения мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн 1, 2 классов и в распределенных информационных системах 3 класса Организация должна получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке.

2.5 Организационно-распорядительная документация

2.5.1 Перечень ОРД, разрабатываемой в Организации.

В рамках реализации мер по обеспечению безопасности ПДн в Организации

должны быть разработаны следующие документы:

1) Положение об обработке персональных данных (для каждого вида ПДн).
2) Регламент взаимодействия с субъектами персональных данных.
3) Регламент взаимодействия с уполномоченными органами.
4) Регламент взаимодействия при передаче персональных данных третьим лицам.
5) Регламент контроля режима обработки персональных данных.
6) Регламент обеспечения режима обработки персональных данных.
7) Инструкции администраторов СЗИ, обеспечивающих безопасность персональных данных.
8) Инструкции пользователей ИСПДн по работе с персональными данными и СЗИ.
9) Раздел должностных инструкций персонала в части обеспечения безопасности ПДн при их обработке.
10) Типовые формы согласия субъектов на обработку персональных данных.

2.5.2 Требования к содержанию ОРД.

При разработке «Положения об обработке ПДн» и Типовых форм согласия субъектов ПДн желательно руководствоваться примерными формами, предлагаемыми Роскомнадзором.

Типовая форма письменного согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
3) цель обработки персональных данных;
4) перечень персональных данных, на обработку которых дается согласие

субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
6) срок, в течение которого действует согласие, а также порядок его отзыва.

3. ИСПОЛНИТЕЛЬ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общее руководство работами по обеспечению безопасности ПДн осуществляет руководитель Организации.

Для организации работ по обеспечению безопасности ПДн руководителем Организации назначаются должностные лица, ответственные за следующие направления:

- Методическое руководство и контроль за эффективностью предусмотренных мер защиты информации;
- Научно-техническое руководство и непосредственную организацию работ по созданию (модернизации) СЗПДн.

3.1 Привлечение сторонних организаций

Разработка СЗПДн может осуществляться как подразделением Организации, так и другими специализированными организациями, имеющими лицензии ФСТЭК России на соответствующий вид деятельности.

В случае разработки СЗПДн или ее отдельных компонентов специализированными организациями руководством Организации определяются подразделения (или отдельные специалисты), ответственные за организацию и проведение мероприятий по защите ПДн.

Разработка и внедрение СЗПДн осуществляется во взаимодействии разработчика с ответственным подразделением, которое осуществляет методическое руководство и участвует в разработке конкретных требований по защите персональных данных, аналитическом обосновании необходимости создания СЗПДн, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможных каналов утечки информации или воздействий на неё и предупреждению

утечки и нарушения целостности ПДн, в аттестации ИСПДн.

4. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

4.1 Модернизация СЗПДн

Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменился состав угроз безопасности ПДн в ИСПДн;
- изменился класс ИСПДн.

Для определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и класса ИСПДн. Проверка проводится силами подразделения (должностного лица), ответственного за обеспечение безопасности ПДн. Результаты проверки оформляются актом и утверждаются руководством.

4.2 Контроль за соблюдением условий использования СЗИ

Необходимо проводить периодический (не реже одного раза в год) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

4.3 Разбирательства

Разбирательство и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей персональных данных.

- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.
- нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

По окончании проведения разбирательства необходимо провести разработку (доработку) и принятие мер по предотвращению повторения подобных нарушений.

ПРИЛОЖЕНИЕ 1

ТИПОВЫЕ ФОРМЫ ЭКСПЛУАТАЦИОННЫХ И ТЕХНИЧЕСКИХ ДОКУМЕНТОВ ПО ПДН

Перечень ПДн

Перечень ИСПДн

Перечень лиц, допущенных к обработке ПДн

Акт классификации ИСПДн

Паспорт ИСПДн

Декларация соответствия ИСПДн требованиям по обеспечению безопасности ПДн