Министерство культуры Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский государственный институт искусств имени Загира Исмагилова»

УТВЕРЖДЕН
приказом ректора
от «29» 12 2016 г. № 188

ПРИНЯТ
Ученым советом
от «29» 12 2016 г.
протокол № 5

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В УФИМСКОМ ГОСУДАРСТВЕННОМ ИНСТИТУТЕ ИСКУССТВ ИМЕНИ ЗАГИРА ИСМАГИЛОВА

г. Уфа, 2016

Предисловие

1. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Уфимском государственном институте искусств имени Загира Исмагилова

РАЗРАБОТАНО начальником кадрово- организационной службы _____
Л.Ф. Султановой

2. Положение по организации и проведению работ по обеспечению безовасности персональных данных при их обработке в информационных системах персональных данных в Уфимском государственном институте искусств имени Загира Исмагилова

СОГЛАСОВАНО

Проректор по учебной и воспитательной работе _____ (подпись) А.А. Хасбиуллина

Юрист _____ (подпись) А.А. Тимерханова

Председатель Первичной профсоюзной организации работников _____ (подпись) Г.Г. Назиуллина

СОДЕРЖАНИЕ

1 Назначение и область применения

1.1. Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.2. Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский государственный институт искусств имени Загира Исмагилова» (далее – Институт).

1.3. Положение является локальным нормативным актом Института. Требования Положения обязательны для выполнения всеми работниками, которые допущены к обработке персональных данных.

2 Термины и сокращения

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

Доступ 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 таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы 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 посторонних 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.

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

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

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

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

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

Средство 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.

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

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

3 Общие положения

3.1 Необходимость проведения мероприятий по защите персональных данных в Институте определяется:

Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

Все работники, обрабатывающие ПДн и обеспечивающие защиту ПДн должны быть ознакомлены с настоящим Положением под роспись.

4 Нормативные ссылки

4.1. Настоящее Положение разработано в соответствии с правовыми актами РФ:

Федеральным Законом от 27.07.2006 №152-ФЗ «О персональных данных»;

Федеральным Законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

«Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной заместителем директора ФСТЭК России 15.02.2008;

«Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утвержденной заместителем директора ФСТЭК России 15.02.2008;

Приказом ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5 Персональные данные, подлежащие защите

5.1. Персональные данные, подлежащие защите, утверждаются приказом ректора в виде «Перечня персональных данных, обрабатываемых в Институте».

5.2. Изменения, дополнения перечня персональных данных, обрабатываемых в Институте, осуществляются на основании информации, предоставляемой руководителями подразделений, сотрудники которых обрабатывают ПДн при выполнении должностных обязанностей.

5.3. Персональные данные, подлежащие защите в Институте, обрабатываются в информационных системах персональных данных (ИСПДн), а также без использования средств автоматизации.

6 Организационная система обеспечения безопасности ПДн

6.1. В состав организационной системы обеспечения безопасности ПДн Института входят:

ректор;

лицо, ответственное за организацию обработки ПДн;

администратор безопасности ИСПДн;

сотрудники, которым предоставлен доступ к ПДн (пользователи ИСПДн).

6.2. Руководство и контроль за обеспечением безопасности ПДн при обработке в ИСПДн, организацию работ по разработке документации по защите ПДн, разработке СЗПДн, по проведению организационных и технических мероприятий по защите ПДн осуществляет ректор.

6.3. Из состава сотрудников назначается администратор безопасности ИСПДн. Права и обязанности работника, ответственного за защиту информации (администратора безопасности) определяются инструкцией (Приложение 1) или включаются в его должностные обязанности.

6.4. Сотрудники, которым предоставлен доступ к ПДн в рамках обработки без использования средств автоматизации, непосредственно реализуют организационные меры по обеспечению сохранности носителей ПДн и выполнения процедур по соблюдению требований законодательства.

6.5. Пользователи ИСПДн непосредственно реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации и инструкции пользователя ИСПДн (Приложение 2).

7 Защита ПДн при обработке без использования средств автоматизации

7.1. Требования к обеспечению безопасности персональных данных при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.2. Порядок обработки ПДн без использования средств автоматизации устанавливается Положением об обработке персональных данных в Институте.

7.3. Данный вид обработки ПДн (а также состав ПДн и перечень лиц, допущенных к обработке) указывается в Перечне обрабатываемых персональных данных и Перечне подразделений и должностных лиц, допущенных к работе с персональными данными.

7.4. Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

определением мест хранения персональных;

обеспечением раздельного хранения персональных данных;

соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

7.5. Носители ПДн подлежат уничтожению по достижении целей обработки и/или в случае утраты необходимости в их хранении.

7.6. В случаях истечения срока хранения (архивного хранения) носителей ПДн осуществляется уничтожение и/или обезличивание ПДн при наличии такой возможности в порядке, предусмотренном Положением об обработке персональных данных в Институте.

8 Защита ПДн при обработке в информационных системах персональных данных

8.1. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

определение уровня защищенности ИСПДн;

определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе модели угроз;

разработку на основе модели угроз и модели нарушителя системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем;

описание системы защиты персональных данных;

установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

учет лиц, допущенных к работе с персональными данными в информационной системе;

контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.2. Определение уровня защищенности ИСПДн и моделирование угроз безопасности ПДн

8.2.1 Уровень защищенности ИСПДн (далее – УЗ ИСПДн) определяется в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8.2.2 Определение уровня защищенности ИСПДн проводит Комиссия, состав которой утверждается приказом ректора Института.

8.2.3 Определение уровня защищенности ИСПДн проводится на этапе создания ИСПДн и для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн с целью определения организационных и технических мер, необходимых для обеспечения безопасности ПДн.

8.2.4 Результаты определения уровня защищенности ИСПДн должны утверждаться Актом.

8.2.5 Все имеющиеся и вводимые в эксплуатацию ИСПДн вносятся в перечень ИСПДн Института.

8.2.6 Модель угроз безопасности персональных данных при их обработке в специальных информационных системах персональных данных разрабатывается с использованием методических документов ФСТЭК России и (или) ФСБ России. Результаты определения и оценки актуальных угроз безопасности ПДн при их обработке в ИСПДн Института утверждаются Приказом ректора Института.

8.2.7 Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн.

8.2.8 Модель угроз безопасности ПДн должна периодически

пересматриваться в соответствии с «Планом внутренних проверок состояния защиты ПДн».

8.2.9 Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется в случае изменения:

технологических процессов обработки ПДн;

состава средств защиты информации в ИСПДн;

характеристик ИСПДн, влияющих на уровень защищенности (наличие подключений к сетям общего пользования, тип ИСПДн и т.д.).

8.2.10 При необходимости применения (в случае передачи ПДн по незащищенным каналам связи) средств криптографической защиты информации для ИСПДн разрабатывается Модель нарушителя безопасности персональных данных. Модель нарушителя разрабатывается на основе «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных» ФСБ России. На основе разработанной модели нарушителя для ИСПДн определяется уровень криптографической защиты ПДн, которому должны соответствовать применяемые средства криптографической защиты.

8.3 Требования к обеспечению безопасности ПДн при их обработке в ИСПДн

8.3.1 Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

8.3.2 Требования к СЗПДн разрабатываются на основе модели угроз и модели нарушителя и должны обеспечивать нейтрализацию предполагаемых актуальных угроз, выявленных по результатам моделирования. Требования формируются на основании методов и способов защиты информации для соответствующего УЗ ИСПДн, задаваемых требованиями нормативных документов по защите ПДн ФСТЭК России и ФСБ России.

8.3.3 В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – машинные носители персональных данных);

- регистрация событий безопасности; антивирусная защита;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;
- защита среды виртуализации; защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

8.3.4 Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8.3.5 Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 4 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

8.3.6 Разрешительная система допуска пользователей к информационным ресурсам

8.3.6.1 Разграничение доступа к информационным ресурсам, содержащим ПДн, должно осуществляться на основании «Перечня должностных лиц, допущенных к работе с персональными данными» в Институте.

8.3.7 Регистрация действий пользователей

8.3.7.1 Регистрация действий пользователей должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

8.3.7.2 Подлежат обязательной регистрации следующие операции, осуществляемые в ИСПДн:

регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;

регистрация выдачи печатных (графических) документов на бумажный носитель;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа.

8.3.8 Обеспечение безопасности при хранении носителей информации ПДн

8.3.8.1 Подлежат учету следующие защищаемые носители ПДн:

накопители на жестких магнитных дисках, установленные в серверы ИСПДн;

накопители на жестких магнитных дисках, установленные в АРМ, на которых предусмотрено хранение ПДн;

накопители для хранения резервных копий;

внешние носители ПД (дискеты, компакт-диски, flash-накопители), на которых технологией обработки ПДн разрешается хранение или передача ПДн.

8.3.8.2 Учет защищаемых носителей информации должен осуществляться в Журналах учета материальных носителей ПДн в соответствии с порядком, предусмотренным Положением «Об обработке персональных данных Института».

8.3.8.3 Обязанность по ведению учета электронных носителей ПДн возлагается на администратора ИСПДн.

В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых носителей информации необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с носителей информации должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя.

8.3.8.4 По факту уничтожения носителя ПДн должен составляться соответствующий Акт, в порядке, предусмотренном Положением «Об обработке персональных данных в Институте».

8.3.9 Резервирование технических средств, дублирование массивов и носителей информации

8.3.9.1 Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при их случайной или намеренной модификации, должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

8.3.9.2 Для обеспечения целостности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

8.3.10 Использование средств защиты информации

При использовании средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией;

– проведение обучения лиц, использующих средства защиты информации, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 3. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 4;

– контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– периодическое тестирование средств защиты в соответствии с эксплуатационной документацией на СЗИ. Форма журнала проведения периодического тестирования СЗИ приведена в Приложении 5;

– разбирательство и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению целостности, конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

8.3.11 Использование защищенных каналов связи

8.3.11.1 При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты;

– централизованное управление системой защиты персональных данных информационной системы.

– 8.3.11.2 Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена дополнительно должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена данных;

– управление доступом к защищаемым персональным данным информационной сети;

– использование атрибутов безопасности.

8.3.11.3 Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

8.3.11.4 Защита каналов связи реализуется следующими организационно-техническими способами:

– Размещение линий связи и сетевого оборудования в пределах контролируемой зоны (КЗ);

– Использование волоконно-оптических линий связи, затрудняющих или исключающих возможность перехвата передаваемой информации;

– Использование средств криптографической защиты.

8.3.12 Физическая защита помещений и технических средств

8.3.12.1 Размещение ИСПДн и охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.3.12.2 В Институте приказом ректора утверждается перечень лиц, имеющих право доступа в Помещения.

8.3.12.3 Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) Института.

8.3.12.4 Границами КЗ могут являться:

- периметр охраняемой территории Института;
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;
- стены помещений Института.

8.3.12.5 В состав КЗ должны входить:

- помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;
- помещения, в которых проходят кабельные линии связи ИСПДн;
- помещения, в которых хранятся бумажные носители ПДн (архивы, помещения работников Института).

8.3.12.6 Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

8.3.12.7 Доступ посторонних лиц (посетителей, сотрудников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников Института.

8.3.12.8 Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8.3.12.9 Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

8.3.12.10 В нерабочее время доступ в контролируемую зону должен быть исключен следующими мерами:

- организация и обеспечение контроля доступа в помещения сотрудников и посетителей в рабочие дни с 09.00 до 18.00.
- организация и обеспечение охраны помещений в рабочие дни с 18.00 до 10.00 следующего дня, а также в выходные и праздничные дни.

- не допускать проникновения и пребывания посторонних лиц в помещениях в рабочие дни с 18.00 до 10.00 следующего дня, а также в выходные и праздничные дни. При необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом.
- внос и вынос материальных ценностей в помещения и из помещений осуществляется только в присутствии ответственного лица.
- на всех остекленных проемах первого этажа должна быть установлена охранная сигнализация;
- двери в помещения контролируемой зоны должны быть оснащены замками и охранной сигнализацией;
- хранение ключей осуществляется в настенном шкафу в комнате охранников с выдачей под роспись работникам в случае необходимости.

8.3.13 Использование средств антивирусной защиты

8.3.13.1 Средства антивирусной защиты предназначены для реализации следующих функций:

- антивирусное сканирование;
- блокирование вредоносных программ;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

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

8.3.13.3 Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять специалистов сектора информационных технологий.

8.4 Порядок разработки, ввода в действие и эксплуатации СЗПДн

8.4.1 Требования по защите ПДн для каждой ИСПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

8.4.2 Требования должны формироваться на основании положений руководящих документов ФСТЭК России и ФСБ России, перечень которых приведен в п. 4.1.

8.4.3 Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн, проводятся следующие мероприятия:

- обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн;
- проектирование и реализация ИСПДн и СЗПДн в её составе;
- ввод в действие СЗПДн, включающее опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

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

– изменился состав обрабатываемых ПДн;

– изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился класс ИСПДн.

8.5 Порядок оценки соответствия ИСПДн требованиям безопасности ПДн

8.5.1 Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде внутренней оценки соответствия или добровольной аттестации на соответствие требованиям безопасности информации.

8.5.2 Для ИСПДн, оценка соответствия которых проводится в виде внутренней оценки соответствия, необходимо выполнять следующие требования:

– оценка соответствия осуществляется на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии;

– в случае проведения оценки на основе собственных доказательств Институт самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу;

– результаты оценки соответствия должны содержать:

1) наименование и местонахождение ИСПДн;
2) информацию об объекте подтверждения соответствия, класс ИСПДн;
3) наименование документов, на соответствие требованиям которых оценивается ИСПДн;
4) сведения о принятых мерах по обеспечению соответствия ИСПДн необходимым требованиям;
5) сведения о документах, послуживших основанием для подтверждения соответствия ИСПДн требованиям;
6) срок действия оценки соответствия и условия повторной оценки.

8.5.3 Добровольная аттестация ИСПДн на соответствие требованиям безопасности информации проводится в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденным председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации аккредитуются ФСТЭК России с выдачей лицензии на проведение работ по аттестации объектов информатизации.

Аттестационные испытания проводятся в соответствии с разработанной Программой и методикой проведения аттестационных испытаний. По результатам испытаний оформляются заключение с подтверждающими протоколами, а также, в случае положительного заключения, выдается аттестат соответствия.

9 Требования к персоналу по обеспечению защиты ПДн

9.1 При вступлении в должность нового сотрудника лицо, ответственное за организацию обработки ПДн, обязано организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн (Положением об обработке персональных данных в Институте, настоящим Положением). Администратор обучает навыкам выполнения процедур, необходимых для работы в ИСПДн Института и выполнения требований по защите ПДн и знакомит под роспись с Инструкцией пользователям информационных систем персональных данных.

9.2 Сотрудники должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки персональных данных, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

9.3 Сотрудники должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн в момент заключения трудового договора с Институтом.

10 Контроль состояния защиты ПДн

10.1 Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

10.2 Контроль состояния защиты ПДн должен осуществляться ежегодно в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных. Форма журнала учета проведения мероприятий приведена в Приложении 6.

10.3 Проведение контроля состояния защиты включает в себя мероприятия по оценке:

– соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

10.4 Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

10.5 В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

10.6 Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

11 Порядок внесения изменений

11.1 Настоящее Положение пересматривается по мере необходимости и в случае изменения законодательства в области защиты ПДн.

11.2 Все изменения отражаются в Листе изменений.

11.3 Измененное Положение утверждается в установленном порядке.