ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНО
приказом управления культуры и архивного дела
Тамбовской области
от «16» мая 2017 г. № 103

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе управления культуры и архивного дела Тамбовской области

2017

Содержание

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе управления культуры и архивного дела Тамбовской области (далее – Положение) устанавливает порядок организации и проведения работ по защите информации, содержащей персональные данные, на объектах информатизации управления культуры и архивного дела Тамбовской области (далее – Управление) как в период их создания, так и в процессе повседневной эксплуатации.

1.2. Настоящее Положение определяет:

– перечень мероприятий по защите персональных данных;

– порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации;

– порядок контроля защиты персональных данных, обучения персонала практике работы в информационной системе (далее – ИС);

– правила антивирусной и парольной защиты, обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИС;

– порядок контроля соблюдения условий использования средств защиты информации;

– порядок проверки электронного журнала обращений к ресурсам информационной системы;

– порядок охраны и допуска посторонних лиц в помещения ИС.

1.3. Требования настоящего Положения являются обязательными для исполнения отделами Управления, в которых обрабатываются персональные данные, а также отделами Управления, организациями, учреждениями и предприятиями, выполняющими работы по защите персональных данных в Управлении.

2. Термины и сокращения

В настоящем документе используются следующие термины и сокращения:

– **персональные данные (ПДн)** – любая информация, относящаяся к определённому 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;

– **информационная система (ИС)** – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения различных задач;

– **информационная система персональных данных (ИСПДн)** – совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации;

– **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;

– **конфиденциальность персональных данных** – обязательное для соблюдения пользователем ИС или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

– **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;

– **пользователь ИС** – лицо (сотрудник Управления), участвующее в функционировании ИС или использующее результаты её функционирования;

– **криптосредства** – криптографические (шифровальные) средства для обеспечения безопасности персональных данных;

– **пользователь криптосредства** – пользователь ИС, использующий при обработке (передаче) персональных данных криптосредство;

– **инсайдер** – любое лицо, потенциально имеющее доступ к конфиденциальной информации (например, персональным данным) в силу служебного положения или родственных связей;

– **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;

– **несанкционированный доступ (несанкционированные действия) (НСД)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

– **объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений и объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

– **система защиты информации** – проводимые мероприятия по защите информации и средства защиты информации (в том числе криптографические, средства защиты от несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства и системы), а также используемые информационные технологии;

– **аттестация объектов информатизации** – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации;

– **контролируемая зона (КЗ) –** пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств;

– **основные технические средства и системы (ОТСС) –** технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации;

– **вспомогательные технические средства и системы (ВТСС) –** технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях;

– **технический канал утечки информации** – совокупность носителей информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

3. Нормативно-методическая документация

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»;

– постановление Правительства РФ от 21 марта 2012 № 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»;

– приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– постановление Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказ ФСТЭК от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

– Указ Президента от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (утв. приказом Гостехкомиссии России от 30 августа 2002 № 282);

– приказ ФСБ России от 10 июля 2014 г. № 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»;

– руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992г.).

4. Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в ИС

Под организацией обеспечения безопасности персональных данных при их обработке в ИС 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 персональных данных.

Обеспечение безопасности персональных данных осуществляется путём выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

4.1. Организационные мероприятия

Организационные мероприятия по защите персональных данных включают в себя:

4.1.1. Определение перечня персональных данных, обрабатываемых в ИС

Устанавливается наличие и состав персональных данных, которые обрабатываются в Управлении.

4.1.2. Определение цели обработки персональных данных

Обработка персональных данных осуществляется Управлением в следующих целях:

– организация кадрового учета Управления для обеспечения соблюдения требований действующих нормативно-правовых актов;

– реализация обязательств в рамках трудовых правоотношений (на основании заключенных с сотрудниками Управления контрактов и действующих нормативно-правовых актов), а также обязательств, связанных с трудовыми правоотношениями, предусмотренными действующим законодательством Российской Федерации;

– регистрация обращений граждан.

4.1.3. Определение сроков обработки и хранения персональных данных

Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели их обработки, по достижении которых персональные данные подлежат уничтожению.

По результатам анализа информации, обрабатываемой в Управлении, и реализации мероприятий, указанных в п.п. 4.1.1-4.1.3:

– определяется уровень защищенности персональных данных, обрабатываемых в информационной системе Управления, в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– осуществляется классификация ИС в соответствии с требованиями приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– осуществляется классификация автоматизированных систем, обрабатывающих персональные данные, в соответствии с требованиями СТР-К и руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992г.).

4.1.4. Определение ответственных за обеспечение безопасности персональных данных

Ответственный за организацию обработки ПДн, ответственный за обеспечение безопасности ПДн и администратор безопасности ИС определяются приказом начальника Управления.

Ответственный за организацию обработки ПДн определяет цели, содержание и порядок обработки ПДн в Управлении, а также организовывает и контролирует осуществление мероприятий по обеспечению безопасности ПДн при их обработке в ИС, координирует работу ответственного за обеспечение безопасности ПДн и администратора безопасности ИС в Управлении.

Ответственный за обеспечение безопасности ПДн разрабатывает и осуществляет мероприятия по обеспечению безопасности ПДн при их обработке в ИС.

Задачи, функции, обязанности, права и ответственность администратора безопасности ИС определяются данным Положением, а также инструкцией администратора безопасности ИС.

4.1.5. Определение круга лиц, допущенных к обработке персональных данных

Начальниками отделов Управления составляется перечень сотрудников, доступ которых к обрабатываемым в ИС персональным данным необходим для выполнения ими служебных (трудовых) обязанностей. Перечень лиц, допущенных к обработке персональных данных, утверждается начальником Управления.

К обработке персональных данных допускаются сотрудники Управления, подготовленные к работе с информацией, требующей защиты (пользователи ИС).

Ответственным за обеспечение безопасности ПДн разрабатывается разрешительная система доступа данных пользователей к информационным ресурсам ИС.

Права доступа администратору безопасности ИС и пользователям ИС оформляются в виде «Матрицы разграничения доступа к защищаемым ресурсам автоматизированной системы…».

4.1.6. Организация доступа в помещения, где осуществляется обработка персональных данных

Необходимо исключить возможность несанкционированного доступа и пребывания в помещениях, где обрабатываются персональные данные, а также к техническим средствам обработки персональных данных, хищения и нарушения работоспособности технических средств обработки персональных данных, хищения носителей информации.

Порядок охраны помещений ИС, доступа в эти помещения определяется «Порядком доступа в помещения управления культуры и архивного дела Тамбовской области, в которых ведется обработка персональных данных».

4.1.7. Обучение сотрудников

Не реже одного раза в год необходимо проводить обучение пользователей ИС правилам обработки персональных данных в соответствии с действующим законодательством, а также

правилам работы со средствами защиты информации, применяемыми в ИС, в соответствии с документацией (инструкции, руководства и т.п.), прилагаемой к таким средствам защиты информации.

Обучение может проводиться в форме совещаний, обучающих занятий, семинаров, инструктажей, методической помощи и практических занятий на месте. Обучение может проводиться в ходе периодических (плановых) и внеплановых проверок условий обработки персональных данных в ИС на местах.

Первичные инструктажи проводятся с пользователями ИС:

– после проведения аттестационных испытаний ИС и получения Аттестата соответствия по требованиям безопасности ИС;

– при поступлении на работу сотрудника в отдел Управления, в котором происходит обработка персональных данных в ИС.

Ответственным за организацию обучения и оказание методической помощи пользователям ИС в Управлении является ответственный за обеспечение безопасности ПДн.

Для проведения обучающих мероприятий могут привлекаться администратор безопасности ИС, специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИС.

К работе в ИС допускаются только сотрудники, прошедшие первичный инструктаж обеспечения безопасности персональных данных в ИС и показавшие твёрдые теоретические знания и практические навыки.

В целях изучения практических вопросов обеспечения безопасности в реально действующих информационных системах и ознакомления с новыми решениями в области информационной безопасности ответственный за обеспечение безопасности ПДн, администратор безопасности ИС и другие специалисты, обеспечивающие безопасность персональных данных, должны периодически проходить курсы повышения квалификации (переподготовки) в области информационной безопасности.

Кроме того, данные сотрудники должны самостоятельно изучать необходимые для работы документы, а также современные средства защиты информации.

4.1.8. Установление персональной ответственности за нарушения правил обработки персональных данных

В должностные инструкции пользователей ИС должны быть внесены дополнения в части персональной ответственности за нарушение правил обработки персональных данных.

4.1.9. Учёт применяемых технических средств защиты персональных данных

При выборе технических (аппаратных, программных и программно-аппаратных) средств защиты следует использовать сертифицированные средства защиты информации. Перечень используемых средств защиты с указанием их заводского номера, сведений о сертификате соответствия, месте и дате установки приводится в Техническом паспорте автоматизированной системы.

4.1.10. Учёт носителей персональных данных

В обязательном порядке должен быть организован учёт всех защищаемых носителей персональных данных с помощью их маркировки и с занесением учётных данных в Журнал учета машинных носителей информации.

Запрещается несанкционированное использование съёмных носителей информации, содержащей персональные данные, и использование незарегистрированных носителей информации, содержащей персональные данные.

4.1.11. Разработка организационно-распорядительных документов по обеспечению безопасности персональных данных

В рамках реализации мер по обеспечению безопасности персональных данных должны быть разработаны следующие документы:

– Акт определения уровня защищенности ПДн (в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных

данных»);

- Акт классификации для каждой ИС (в соответствии с приказом ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- Акт классификации для каждой АС, в составе которой находится ИС (в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992г.));
- Уведомление об обработке персональных данных;
- Перечень лиц, допущенных к обработке персональных данных (Список постоянных пользователей) для каждой ИС и установленные им права доступа к информационным ресурсам (матрица доступа пользователей к защищаемым информационным ресурсам);
- Технический паспорт на каждую ИС;
- Инструкция администратора безопасности информационной системы;
- Инструкция по работе пользователей ИС;
- Инструкция по организации антивирусной защиты и проведению антивирусного контроля;
- Инструкция по организации парольной защиты;
- Инструкция по архивированию и резервированию персональных данных в ИС;
- Инструкция по ликвидации последствий нештатных ситуаций в ИС;
- Инструкция о порядке предоставления доступа к защищаемым ресурсам ИС;
- Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИС;
- Инструкция о порядке охраны и допуска в помещения ИС;
- Инструкция по применению криптосредств для защиты конфиденциальной информации;
- Журнал регистрации, учёта и выдачи носителей информации, содержащей персональные данные.

Ответственность за организацию разработки организационно-распорядительных документов возлагается на ответственного за организацию обработки ПДн.

4.1.12. Подача Уведомления об обработке персональных данных в Уполномоченный орган по защите прав субъектов персональных данных

Ответственность за своевременную подачу Уведомления об обработке персональных данных в Уполномоченный орган по защите прав субъекта персональных данных возлагается на ответственного за обеспечение безопасности ПДн.

4.2. Технические мероприятия

Технические меры защиты персональных данных предполагают использование программно-аппаратных средств защиты информации (далее – СЗИ). При обработке персональных данных с использованием средств автоматизации применение СЗИ является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Управления.

4.2.1. Требования к техническим и программным средствам

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

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

4.2.2. Необходимость создания системы защиты персональных данных

Создание системы защиты персональных данных (далее – СЗПДн) является необходимым условием обеспечения безопасности персональных данных в том случае, если

существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности персональных данных для ИС соответствующего класса и/или не покрывают всех угроз безопасности персональных данных для данной ИС.

Целью создания СЗПДн является обеспечение защиты информации, содержащей персональные данные, от утечки по техническим каналам и от несанкционированного доступа. Защита осуществляется путём выполнения комплекса организационных и технических мероприятий в соответствии с требованиями государственных стандартов, руководящих и нормативно-методических документов ФСТЭК России, реализуемых в рамках создаваемой СЗПДн.

СЗПДн должна включать:

- организационные меры и технические средства защиты информации;
- средства предотвращения несанкционированного доступа к информации;
- средства предотвращения утечки информации по техническим каналам;
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных;
- используемые в ИС информационные технологии.

Результатом создания СЗПДн является подтверждение соответствия ИС требованиям безопасности персональных данных – аттестация объекта информатизации (ИС) по требованиям безопасности информации.

Аттестация объекта информатизации по требованиям безопасности информации представляет собой комплекс организационно-технических мероприятий, в результате которых подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утверждённые государственными органами обеспечения безопасности информации и контролируемые при аттестации.

Аттестация проводится органом по аттестации в установленном законодательством порядке.

Результатом аттестации объекта информатизации (ИС) является получение «Аттестата соответствия автоматизированной системы Управления требованиям безопасности информации» (далее – Аттестат соответствия).

Владелец аттестованного объекта информатизации несёт ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

4.3. Контроль обеспечения безопасности (защиты) персональных данных при создании СЗПДн

Задачами контроля обеспечения безопасности (защиты) персональных данных являются:

- контроль выполнения требований безопасности персональных данных в ИС;
- координация действия отделов Управления по организации и обеспечению безопасности персональных данных;
- предупреждение, выявление и пресечение выявленных нарушений.

Общее руководство работами по обеспечению безопасности персональных данных осуществляет начальник Управления.

Ответственный за обеспечение безопасности ПДн (администратор безопасности ИС) выполняет:

- анализ состояния и определение требований к защищённости различных ИС;
- выбор методов и средств обеспечения защиты персональных данных;
- разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных;
- администрирование и контроль применения средств защиты информации, а также поддержку функционирования средств, технологий и процессов при обработке персональных

данных;

- разработку требований по обеспечению безопасности персональных данных (создание/модернизацию СЗПДн);
- организацию проведения работ по защите персональных данных;
- контроль выполнения требований по обеспечению безопасности персональных данных и эффективности предусмотренных мер защиты.

Обязанности пользователей ИС определяются их должностными инструкциями, Инструкцией администратора безопасности ИС, Инструкцией пользователей ИС и другими организационно-распорядительными документами, разрабатываемыми в соответствии с настоящим Положением.

Пользователи ИС не имеют права использовать в неслужебных целях информационные ресурсы ИС, обязаны соблюдать конфиденциальность (не разглашать, не допускать распространения) ставшей им известной в связи с исполнением должностных обязанностей информации ограниченного доступа (персональных данных).

4.4. Привлечение сторонних организаций

Разработка и осуществление мероприятий СЗПДн может проводиться как специалистами по защите информации Управления, так и специализированными организациями, имеющими лицензии ФСТЭК России на соответствующий вид деятельности.

В случае разработки СЗПДн или её отдельных компонентов специализированными организациями разработка и внедрение СЗПДн осуществляется при взаимодействии разработчика с ответственным за организацию обработки ПДн Управления и ответственным за обеспечение безопасности ПДн Управления, которые осуществляют методическое руководство и участвуют в:

- разработке конкретных требований по защите ПДн;
- 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 персональных данных;
- аттестации ИС.

5. Контроль защиты персональных данных

Контроль защиты персональных данных в ИС – это комплекс организационных и технических мероприятий, которые осуществляются в целях предупреждения и пресечения возможности получения с помощью технических средств защищаемой информации (персональных данных), выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности ИС.

Периодический контроль защиты персональных данных осуществляется ежегодно ответственным за организацию обработки ПДн в рамках своих полномочий, а также специалистами органа по аттестации ИС в установленном законодательством порядке.

5.1. Задачи и содержание контроля

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите персональных данных в ИС, учёта требований по защите персональных данных в разрабатываемых плановых и распорядительных документах;
- уточнение зон перехвата обрабатываемой в ИС информации, возможных каналов утечки персональных данных, несанкционированного доступа к ним и программно-технических

воздействий на них;

− проверка выполнения установленных норм и требований по защите персональных данных от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите персональных данных;

− проверка выполнения требований по защите ИС от несанкционированного доступа;

− проверка выполнения требований по антивирусной защите ИС;

− проверка знаний сотрудников по вопросам защиты персональных данных и их соответствия требованиям уровня подготовки для конкретного рабочего места;

− оперативное принятие мер по пресечению нарушений требований (норм) защиты персональных данных в ИС;

− разработка предложений по устранению (ослаблению) технических каналов утечки информации, содержащей персональные данные.

Контроль защиты персональных данных проводится с учётом реальных условий по потенциальным техническим каналам утечки информации, содержащей персональные данные, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты персональных данных.

В ходе контроля проверяются:

− соответствие принятых мер по обеспечению безопасности персональных данных требованиям законодательства по безопасности персональных данных;

− своевременность и полнота выполнения требований настоящего Положения и других руководящих документов по защите персональных данных;

− полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки персональных данных, несанкционированного доступа к информации и программно-технических воздействий на персональные данные;

− эффективность применения организационных и технических мероприятий по защите персональных данных.

Кроме того, могут проводиться необходимые измерения и расчёты приглашенными для этих целей специалистами органа по аттестации ИС.

Основными типами контроля являются:

− визуально-оптический контроль;

− контроль эффективности защиты ПДн от утечки по техническим каналам (инструментальный контроль с использованием контрольно-измерительной аппаратуры);

− контроль несанкционированного доступа к персональным данным.

5.2. Виды контроля

Контроль защиты персональных данных осуществляется путём проведения обследования, периодических (плановых) и внеплановых проверок объектов информатизации, обрабатывающих персональные данные. Проверки ИС проводятся силами ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИС и администратора безопасности ИС Управления в рамках их полномочий, с привлечением специалистов органа по аттестации.

Обследование ИС проводится не реже одного раза в год рабочей группой в составе ответственного за организацию обработки ПДн, ответственного за обеспечение безопасности ПДн в ИС, администратора безопасности ИС и специалистов подразделения, в ведении которого находится ИС.

Обследование ИС проводится с целью определения соответствия помещений, технических средств требованиям по защите персональных данных.

В ходе обследования проверяется:

− соответствие категории обследуемой ИС условиям, сложившимся на момент проверки;

− соблюдение организационно-режимных требований к помещениям;

− соответствие выполняемых в ИС мероприятий по защите персональных данных мероприятиям, изложенным в техническом паспорте ИС;

− выполнение требований по защите ИС от несанкционированного доступа;

− выполнение требований по антивирусной защите.

Внеплановые проверки объектов информатизации могут проводиться как по результатам обследования, так и в случае возникновения нештатных ситуаций в ИС.

Периодические плановые проверки проводятся по истечении одного года с даты выдачи Аттестата соответствия или Акта (Заключения) о результатах предыдущей периодической проверки.

В ходе периодических (плановых) и внеплановых проверок ИС проверяется:

− соответствие состава и структуры программно-технических средств, обрабатывающих персональных данных, задокументированному составу и структуре, разрешённым для обработки такой информации;

− путём опроса персонала: доведение до конкретных исполнителей руководящих документов, технологических инструкций, предписаний, актов, заключений; уровень владения персоналом технологией безопасной обработки персональных данных, описанной в этих инструкциях;

− наличие документов, подтверждающих возможность применения технических и программных средств вычислительной техники, средств защиты для обработки персональных данных (сертификатов соответствия и других документов);

− выполнение требований по условиям размещения автоматизированных рабочих мест (далее – АРМ) в рабочих помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к ПДн;

− соответствие уровня полномочий по доступу к персональным данным различных пользователей ИС разрешённым полномочиям;

− знание инструкций по обеспечению безопасности персональных данных пользователями ИС;

− прохождение инструктажа пользователей ИС по вопросам обеспечения безопасности персональных данных и выполнение требований обеспечения безопасности персональных данных пользователями ИС.

Результатом контроля является специальный документ (Акт или Заключение/Акт (протокол) оценки эффективности принятых мер по обеспечению безопасности ПДн), который содержит выводы о состоянии обеспечения безопасности персональных данных и рекомендации по её совершенствованию.

5.3. Результаты контроля

Полученные в ходе контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты персональных данных и выявления нарушений. При обнаружении нарушений норм и требований по защите персональных данных ответственный за обеспечение безопасности ПДн в ИС уведомляет руководителя подразделения, эксплуатирующего ИС, в которой допущены нарушения, для принятия им решения о прекращении обработки персональных данных и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты персональных данных оформляются актами и заносятся в Журнал по учету мероприятий по внутреннему контролю обработки персональных данных и обеспечения защиты персональных данных в ИС.

Невыполнение предписанных мероприятий по защите персональных данных считается предпосылкой к утечке информации (далее – предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по решению ответственного за обеспечение безопасности ПДн проводится расследование.

Для проведения расследования назначается комиссия с привлечением специалистов по защите информации. Комиссия обязана установить:

- факт, имела ли место утечка персональных данных;
- обстоятельства, ей сопутствующие;
- лиц, виновных в нарушении предписанных мероприятий по защите персональных данных;
- причины и условия, способствовавшие нарушению.

По результатам расследования комиссия вырабатывает рекомендации по устранению нарушений и недостатков и их последствий, а также предложения начальнику Управления о привлечении к ответственности виновных лиц.

5.4. Переаттестация объекта информатизации (ИС) по требованиям безопасности информации

Переаттестация объекта информатизации (ИС) по требованиям безопасности информации проводится:

- по истечении срока действия «Аттестата соответствия»;
- при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации (далее – изменения в ИС).

В случае изменений в ИС владелец аттестованного объекта обязан известить об этом орган по аттестации, проводивший аттестацию объекта информатизации, в следующем порядке:

1. Руководитель подразделения, эксплуатирующего ИС, уведомляет о необходимости внесения изменений в ИС ответственного за обеспечение безопасности ПДн.

2. Ответственный за обеспечение безопасности ПДн согласовывает изменения в ИС с органом по аттестации.

Внесение изменений в ИС разрешается по заключению органа по аттестации:

- при условии проведения переаттестации;
- при внесении отметок об изменениях в ИС в технический паспорт на ИС и другие нормативно-методические документы на ИС.

6. Резервное копирование и восстановление информации

Резервное копирование персональных данных применяется для оперативного восстановления данных в случае их утери, искажения, нарушения целостности и т.п. в результате ошибочных действий пользователей ИС, сбоя работоспособности основных технических средств и систем (далее – ОТСС), входящих с состав ИС, средств защиты информации, общесистемного или специального программного обеспечения (далее – ПО), а также вследствие других причин.

Резервное копирование общесистемного, специального ПО и программных средств защиты информации осуществляется в случае отсутствия дистрибутивов на указанное ПО.

Порядок резервного копирования и восстановления информации определяется «Инструкцией по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах управления культуры и архивного дела Тамбовской области».

7. Восстановление работоспособности ОТСС, общесистемного, специального ПО и средств защиты информации в ИС

Ответственность за организацию проведения мероприятий по восстановлению работоспособности ОТСС, общесистемного и специального ПО, а также средств защиты информации в ИС возлагается на администратора безопасности ИС, которые он выполняет самостоятельно в рамках своих полномочий или с привлечением специализированных организаций (органы по аттестации в случае проведения работ в аттестованных по требованиям безопасности информации ИС) в соответствии с «Инструкцией по порядку резервирования и

восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах управления культуры и архивного дела Тамбовской области».

8. Защита от вредоносных программ

Все ИС должны быть защищены от последствий воздействия вредоносных программ средствами антивирусной защиты.

Средства антивирусной защиты, применяемые в ИС, должны быть сертифицированы по безопасности информации для защиты персональных данных установленного ИС класса.

Ответственность за эксплуатацию средств антивирусной защиты возлагается на:

- пользователей ИС в части периодического антивирусного контроля носителей информации с персональными данными;
- администратора безопасности ИС в части установки и администрирования средств антивирусной защиты в ИС, а также контроля их использования пользователями ИС.

Порядок защиты от вредоносных программ определяется «Инструкцией по организации антивирусной защиты и проведению антивирусного контроля на ПЭВМ, входящих в состав информационных систем управления культуры и архивного дела Тамбовской области».

9. Регистрация пользователей ИС и назначение им прав доступа

Регистрацию пользователей ИС и назначение им прав доступа, определённых ответственным за организацию обработки ПДн, а также блокировку учётных записей осуществляет администратор безопасности ИС.

После включения сотрудника Управления в состав постоянных пользователей ИС ему присваивается уникальный идентификатор (имя) пользователя, и он регистрируется как пользователь ИС.

При регистрации пользователя ИС проводится проверка соответствия уровня доступа его должностным обязанностям.

Назначенные пользователю ИС права доступа должны быть отражены в «Матрице разграничения доступа к защищаемым ресурсам автоматизированной системы…», определенной в «Положении о разрешительной системе доступа к информационным ресурсам, программным и техническим средствам автоматизированной системы…».

При изменении должностных обязанностей (увольнении) пользователя ИС его права доступа корректируются (удаляются). Администратором безопасности ИС производится корректировка Матрицы разграничения доступа к защищаемым ресурсам и Перечня лиц, допущенных к обработке ПДн в ИС.

Неиспользуемые учётные записи блокируются (удаляются).

В сочетании с парольной защитой идентификатор пользователя используется для аутентификации пользователя в ИС.

10. Парольная защита

Парольная защита является одним из способов защиты информации от несанкционированного доступа. На компьютерах, обрабатывающих персональные данные, наличие парольной защиты (пароля пользователя) обязательно.

Порядок использования паролей пользователей в ИС определяется «Инструкцией по организации парольной защиты на ПЭВМ, входящих в состав информационных систем управления культуры и архивного дела Тамбовской области».

11. Применение средств криптографической защиты

Необходимость применения средств криптографической защиты (далее – криптосредств) при обработке персональных данных может возникнуть в следующих случаях:

- при передаче персональных данных в среду (носители информации, каналы связи и т.п.), в которой они могут оказаться доступными для несанкционированного доступа;

− в ИС, являющихся многопользовательскими, в которых введено разграничение прав доступа пользователей и возможно наличие инсайдера, если безопасность хранения и обработки не может быть гарантирована другими средствами.

В случае необходимости применения криптосредств при обработке персональных данных безопасность обработки персональных данных обеспечивается:

− соблюдением пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны при выполнении своих служебных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

− точным выполнением пользователями криптосредств требований к обеспечению безопасности персональных данных;

− надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

− своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

− немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Администрирование криптосредств осуществляется ответственным пользователем криптографических средств в информационной системе Управления. Функции, права и обязанности ответственного пользователя криптографических средств в информационной системе Управления определены в «Инструкции ответственного пользователя криптографических средств в информационной системе управления культуры и архивного дела Тамбовской области».

Порядок обеспечения функционирования и безопасности криптосредств, а также права и обязанности сотрудников, эксплуатирующих криптосредства, определяются «Инструкцией по применению криптографических средств для защиты конфиденциальной информации в информационных системах управления культуры и архивного дела Тамбовской области».

12. Обновление общесистемного и прикладного программного обеспечения, техническое обслуживание ИС

Все изменения конфигураций технических и программных средств ПЭВМ должны производиться только на основании заявок ответственного за эксплуатацию конкретной подсистемы ИС (пользователя конкретного АРМ).

Право внесения изменений в конфигурацию аппаратно-программных средств защищённых АРМ предоставляется:

− в отношении системных и прикладных программных средств – ответственному за обеспечение безопасности ПДн с привлечением администратора безопасности ИС, по согласованию с органом по аттестации;

− в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты информации – уполномоченным сотрудникам органа по аттестации ИС.

Изменение конфигурации аппаратно-программных средств ПЭВМ кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, **запрещено**.

Установка, модификация и техническое обслуживание программного обеспечения и аппаратных средств ИС должны проводиться в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем управления культуры и архивного дела Тамбовской области».

13. Порядок контроля соблюдения условий использования средств защиты информации

Средства защиты информации являются важным компонентом обеспечения безопасности персональных данных.

Порядок работы со средствами защиты информации определён в инструкциях (руководствах) по настройке и использованию, прилагаемых к средствам защиты информации, обязательных для исполнения всеми пользователями ИС и администратором безопасности ИС.

Право проверки соблюдения условий использования средств защиты информации имеет администратор безопасности ИС.

Пользователю ИС категорически запрещается:

- производить обработку персональных данных с отключенными средствами защиты информации;
- изменять настройки средств защиты информации.

Контроль за соблюдением условий использования средств защиты информации, обеспечение правильного функционирования и поддержание работоспособности средств защиты информации осуществляет ответственный за безопасность функционирования средств защиты информации, за исключением криптографических, используемых в информационной системе Управления (далее – Ответственный за безопасность функционирования СЗИ), назначаемый приказом начальника Управления. Функции, права и обязанности Ответственного за безопасность функционирования СЗИ определены в «Инструкции ответственного за безопасность функционирования средств защиты информации, за исключением криптографических, используемых в информационной системе управления культуры и архивного дела Тамбовской области».

Ответственному за безопасность функционирования СЗИ запрещается менять настройки программно-аппаратных средств защиты информации, предустановленные сотрудником органа по аттестации при настройке системы защиты информации в ходе аттестации ИС.

14. Порядок проверки электронных журналов обращений к ресурсам ИС

Проверка электронных журналов обращений проводится с целью выявления несанкционированного доступа (далее – НСД) к защищаемой информации в ИС.

Право проверки электронного журнала обращений имеют:

- ответственный за организацию обработки ПДн;
- администратор безопасности ИС;
- ответственный за обеспечение безопасности ПДн в ИС;
- начальник Управления.

На технических средствах ИС, на которых установлены специализированные средства защиты информации типа «Secret Net», «Dallas Lock» и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

Проверке подлежат все электронные журналы ИС.

Проверка должна проводиться не реже, чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

Факты проверок электронных журналов отражаются в Журнале проверок электронных журналов. После каждой проверки ответственный за обеспечение безопасности ПДн в ИС делает соответствующую отметку в журнале и ставит свою подпись.

15. Заключительные положения

Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих персональные данные, и ответственных за обеспечение безопасности персональных данных.

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением о порядке организации и проведения работ по обеспечению безопасности персональных данных в информационной системе управления культуры и архивного дела Тамбовской области

№ п/п	Дата	Должность	Фамилия, имя, отчество	Подпись