АДМИНИСТРАЦИЯ
НАРО-ФОМИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА МОСКОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 28.08.2017 № 2654

г. Наро-Фоминск

Об утверждении Порядка организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской области

В соответствии с действующим законодательством Российской Федерации и руководствуясь Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Уставом Наро-Фоминского муниципального района, **постановляю:**

1. Утвердить Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской области (приложение).
2. Руководителям структурных подразделений и отраслевых функциональных органов Администрации Наро-Фоминского муниципального района Московской области руководствоваться в работе Порядком организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской области.
3. Отделу по работе со СМИ и интернет коммуникациями Администрации Наро-Фоминского муниципального района (Родина И.В.) разместить настоящее постановление на официальном сайте Администрации Наро-Фоминского муниципального района в сети Интернет.
4. Контроль над исполнением настоящего Постановления возложить на Заместителя Руководителя Администрации Наро-Фоминского муниципального района – управляющего делами Е.А. Кузнецову.

И.о. Руководителя Администрации Наро-Фоминского муниципального района **В.П. Никоненко**

029332

УТВЕРЖДЕН
постановлением Администрации
Наро-Фоминского
муниципального района
№ 1654 от «28» 08 2017 г.

Порядок
организации и проведения работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных
Администрации Наро-Фоминского муниципального района Московской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение Порядка

Порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской Области (далее – Порядок) устанавливает порядок организации и проведения работ по защите информации, содержащей персональные данные, на объектах информатизации Администрации Наро-Фоминского муниципального района Московской области (далее - Администрация) как в период их создания, так и в процессе повседневной эксплуатации.

В Порядке определены: перечень мероприятий по защите персональных данных, система управления безопасностью 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 информационных системах персональных данных (далее – ИСПДн); правила антивирусной и парольной защиты, обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн; порядок контроля соблюдения условий использования средств защиты информации; порядок охраны и допуска посторонних лиц в помещения ИСПДн.

Требования настоящего Порядка являются обязательными для исполнения структурными подразделениями Администрации, в которых обрабатываются персональные данные, а также структурными подразделениями Администрации, организациями, учреждениями и предприятиями, выполняющими работы по защите персональных данных в Администрации.

1.2. Термины, определения 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 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;
- объект информатизации – подлежащие защите ИСПДн Администрации;
- пользователь ИСПДн – лицо (сотрудник Администрации), участвующее в функционировании ИСПДн или использующее результаты её функционирования;
- СЗПДн – система защиты персональных данных;
- АРМ – автоматизированное рабочее место;
- АС – автоматизированная система;
- ПО – программное обеспечение;
- ОТСС – основные технические средства и системы, используемые для обработки персональных данных;
- ФСТЭК России – Федеральная служба по техническому и экспортному контролю России;
- криптосредства – криптографические (шифровальные) средства для обеспечения безопасности персональных данных;
- пользователь криптосредства – пользователь ИСПДн, 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;
- 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;
- конфиденциальность персональных данных – обязательное для соблюдения пользователем ИСПДн или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
- технический канал утечки информации – совокупность носителей информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

1.3. 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 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 № 28375);
- «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. № 149/54-144);
- Специальные требования и рекомендации по технической защите конфиденциальной

информации (СТР-К) (утв. приказом Гостехкомиссии России от 30 августа 2002 г.).

2. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН

Под организацией обеспечения безопасности персональных данных 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 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 персональным данным.

2.1. Организационные мероприятия

Организационные мероприятия по защите персональных данных включают в себя:

2.1.1. Определение перечня персональных данных, обрабатываемых в ИСПДн.

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

2.1.2. Определение цели обработки персональных данных.

Определяются цели обработки персональных данных: трудовые отношения с работниками; расчёт субсидий, учёт военнообязанных и граждан, подлежащих призыву, учёт избирателей и т.д.

2.1.3. 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 Администрации Наро-Фоминского муниципального района, и реализации мероприятий, указанных в п.п. 2.1.1-2.1.3, осуществляется классификация автоматизированных систем, обрабатывающих персональные данные, в соответствии с требованиями СТР-К; осуществляется классификация ИСПДн в соответствии с требованиями совместного приказа ФСТЭК России, ФСБ России, Мининформсвязи России «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 13.02.2008 № 55/86/20.

2.1.4. Определение ответственных за обеспечение безопасности персональных данных.

Ответственный за обеспечение безопасности ПДн и администратор безопасности ПДн определяются распоряжением Администрации Наро-Фоминского муниципального района.

Ответственный за обеспечение безопасности ПДн разрабатывает и осуществляет мероприятия (организовывает и контролирует осуществление мероприятий) по обеспечению безопасности ПДн при их обработке в ИСПДн.

Задачи, функции, обязанности, права и ответственность администратора безопасности ПДн определяются данным Порядком, а также Инструкцией администратора безопасности ПДн.

2.1.5. Определение круга лиц, допущенных к обработке персональных данных.

Руководителями структурных подразделений (отделов) составляется список (перечень) сотрудников, доступ которых к обрабатываемым в ИСПДн персональным данным необходим для выполнения служебных (трудовых) обязанностей. Перечень лиц, допущенных к обработке персональных данных, утверждается Руководителем Администрации Наро-Фоминского муниципального района.

К обработке персональных данных допускаются сотрудники Администрации,

подготовленные к работе с информацией, требующей защиты (пользователи ИСПДн).

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

Права доступа администратору безопасности ПДн и пользователям ИСПДн оформляются в виде матрицы доступа к защищаемым информационным ресурсам.

2.1.6. 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 ИСПДн, доступа в эти помещения определяется Инструкцией о порядке охраны и допуска в помещения ИСПДн.

2.1.7. Обучение сотрудников.

Не реже одного раза в год необходимо проводить обучение пользователей ИСПДн правилам обработки персональных данных в соответствии с действующим законодательством, а также правилам работы со средствами защиты информации, применяемыми в ИСПДн, 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 состояния обеспечения безопасности ИСПДн на местах.

Первичные инструктажи проводятся с пользователями ИСПДн:

- после проведения аттестационных испытаний ИСПДн и получения Аттестата соответствия по требованиям безопасности ИСПДн;

- при поступлении на работу сотрудника в структурное подразделение Администрации, в котором происходит обработка персональных данных в ИСПДн.

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

Для проведения обучающих мероприятий могут привлекаться администратор безопасности ПДн, сотрудники отдела муниципальных услуг и информационных технологий Администрации Наро-Фоминского муниципального района, специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн.

К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж обеспечения безопасности персональных данных в ИСПДн 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 ПДн 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.

2.1.8. Установление персональной ответственности за нарушения правил обработки

персональных данных.

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

2.1.9. 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 Формуляре на АРМ.

2.1.10. 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 регистрации, учёта и выдачи носителей информации.

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

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

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

- Акт классификации для каждой ИСПДн (в соответствии с совместным приказом ФСТЭК, ФСБ, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20);
- Акт классификации для каждой АС, в составе которой находится ИСПДн (в соответствии с СТР-К);
- Уведомление об обработке персональных данных;
- Перечень лиц, допущенных к обработке персональных данных (Список постоянных пользователей) для каждой ИСПДн и установленные им права доступа к информационным ресурсам (матрица доступа пользователей к защищаемым информационным ресурсам);
- Технический паспорт на каждую ИСПДн;
- Инструкция администратору безопасности персональных данных;
- Инструкция по работе пользователей ИСПДн;
- Инструкция по организации антивирусной защиты и проведению антивирусного контроля;
- Инструкция по организации парольной защиты;
- Инструкция по архивированию и резервированию персональных данных в ИСПДн;
- Инструкция по ликвидации последствий нештатных ситуаций в ИСПДн;
- Инструкция о порядке предоставления доступа к защищаемым ресурсам ИСПДн;
- Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн;
- Инструкция о порядке охраны и допуска в помещения ИСПДн;
- 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 обеспечение безопасности ПДн.

2.1.12. 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.

2.2. Технические мероприятия

Технические меры защиты персональных данных предполагают использование программно-аппаратных средств защиты информации (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 Администрации.

2.2.1. Требования к техническим и программным средствам.

Технические и программные средства, используемые для обработки персональных данных 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 системы защиты персональных данных.

Создание 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 ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности персональных данных для данной ИСПДн.

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;
    - утечки информации по техническим каналам;
    - программно-технических воздействий на технические средства обработки персональных данных;
- используемые в ИСПДн информационные технологии.

Порядок создания СЗПДн приведён в Приложении к Порядку организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской Области.

Результатом создания СЗПДн является подтверждение соответствия ИСПДн требованиям безопасности персональных данных – аттестация объекта информатизации (ИСПДн) 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 уполномоченным органом на проведение аттестации в установленном законодательством порядке.

Результатом аттестации объекта информатизации (ИСПДн) является получение «Аттестата соответствия требованиям по безопасности информации персональных данных при их обработке в информационной системе персональных данных <наименование ИСПДн>» (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.

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

Задачами контроля обеспечения безопасности (защиты) персональных данных являются:

- контроль выполнения требований безопасности персональных данных в ИСПДн,
- координация действия подразделений Администрации по организации и обеспечению безопасности персональных данных;
- предупреждение, выявление и пресечение выявленных нарушений.

Общее руководство работами по обеспечению безопасности персональных данных осуществляет начальник отдела муниципальных услуг и информационных технологий Администрации Наро-Фоминского муниципального района.

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

- анализ состояния и определяет требования к защищённости различных ИСПДн;
- 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 ИСПДн определяются их должностными инструкциями, Инструкцией администратора безопасности персональных данных, Инструкцией по работе

пользователей ИСПДн и другими организационно-распорядительными документами, разрабатываемыми в соответствии с настоящим Порядком.

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

2.4. Привлечение сторонних организаций

Разработка и осуществление мероприятий СЗПДн может осуществляться как специалистами по защите информации Администрации, 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 во взаимодействии разработчика с ответственным за обеспечение безопасности ПДн, который осуществляет методическое руководство и участвует 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, в аттестации ИСПДн.

3. КОНТРОЛЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Контроль защиты персональных данных в ИСПДн – 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 ИСПДн.

Периодический контроль защиты персональных данных осуществляется ежегодно администратором безопасности ПДн в рамках своих полномочий, а также специалистами органа по аттестации ИСПДн в установленном законодательством порядке.

3.1. Задачи и содержание контроля

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите персональных данных в ИСПДн, учёта требований по защите персональных данных в разрабатываемых плановых и распорядительных документах;
- уточнение зон перехвата обрабатываемой в ИСПДн 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 ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите ИСПДн;
- 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 ИСПДн;

- 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 Порядка 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 приглашёнными для этих целей специалистами органа по аттестации ИСПДн.

Основными типами контроля являются:

- визуально-оптический контроль;
- контроль эффективности защиты ПДн от утечки по техническим каналам;
- контроль несанкционированного доступа к персональным данным.

3.2. Виды контроля

Контроль защиты персональных данных осуществляется путём проведения обследования, периодических (плановых) и внеплановых проверок объектов информатизации, обрабатывающих персональные данные. Проверки ИСПДн проводятся силами администратора безопасности ПДн в рамках его полномочий, с привлечением специалистов отдела муниципальных услуг и информационных технологий Администрации Наро-Фоминского муниципального района и органа по аттестации.

Обследование ИСПДн проводится не реже одного раза в год рабочей группой в составе администратора безопасности ПДн, специалистов отдела муниципальных услуг и информационных технологий Администрации Наро-Фоминского муниципального района и подразделения, в ведении которого находится ИСПДн.

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

В ходе обследования проверяется:

- соответствие категории обследуемой ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-режимных требований к помещениям;
- соответствие выполняемых в ИСПДн мероприятий по защите персональных данных, мероприятиям, изложенным в техническом паспорте ИСПДн;
- выполнение требований по защите ИСПДн 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 ИСПДн.

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 ИСПДн 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;
- проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники, средств защиты для обработки персональных данных (сертификатов соответствия и других документов);
- проверка выполнения требований по условиям размещения 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 ИСПДн разрешённым полномочиям;
- знание инструкций по обеспечению безопасности персональных данных пользователями ИСПДн;
- прохождение инструктажа пользователей ИСПДн по вопросам обеспечения безопасности персональных данных и выполнение требований обеспечения безопасности персональных данных пользователями ИСПДн.

Результатом контроля является специальный документ (Акт или Заключение), который содержит выводы о состоянии обеспечения безопасности персональных данных и рекомендации по её совершенствованию.

При возникновении нештатных ситуаций и нарушении установленного режима обеспечения безопасности персональных данных в ИСПДн ликвидация последствий осуществляется в соответствии с Инструкцией по ликвидации последствий нештатных ситуаций в ИСПДн.

3.3. 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 администратор безопасности ПДн уведомляет руководителя подразделения, эксплуатирующего ИСПДн, 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 либо в соответствующих журналах учёта результатов контроля.

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 Руководителю Администрации Наро-Фоминского муниципального района о привлечении к ответственности виновных лиц.

3.4. Переаттестация органа информатизации (ИСПДн) по требованиям безопасности информации

Переаттестация органа информатизации (ИСПДн) 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 ИСПДн).

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

1. Руководитель подразделения, эксплуатирующего ИСПДн, уведомляет о необходимости внесения изменений в ИСПДн ответственного за обеспечение безопасности ПДн;
2. Ответственный за обеспечение безопасности ПДн согласовывает изменения в ИСПДн с органом по аттестации;

Внесение изменений в ИСПДн разрешается по заключению органа по аттестации:

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

4. 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 ИСПДн, сбоя работоспособности основных технических средств и систем (далее – ОТСС), входящих с состав ИСПДн, средств защиты информации, общесистемного или специального 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 архивированию и резервированию персональных данных.

5. ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ ОТСС, ОБЩЕСИСТЕМНОГО, СПЕЦИАЛЬНОГО ПО И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ИСПДн

Ответственность за организацию проведения мероприятий по восстановлению работоспособности ОТСС, общесистемного и специального ПО, а также средств защиты информации в ИСПДн возлагается на администратора безопасности ПДн, которые он выполняет самостоятельно в рамках своих полномочий или с привлечением специалистов отдела муниципальных услуг и информационных технологий Администрации Наро-Фоминского муниципального района, а также специализированных организаций (органы по аттестации в случае проведения работ в аттестованных по требованиям безопасности информации ИСПДн).

6. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

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

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

Ответственность за эксплуатацию средств антивирусной защиты возлагается на:

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

Порядок защиты от вредоносных программ определяется Инструкцией по организации антивирусной защиты и проведению антивирусного контроля.

7. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДн И НАЗНАЧЕНИЕ ИМ ПРАВ ДОСТУПА

Регистрацию пользователей ИСПДн и назначение им прав доступа, определённых администратором безопасности ПДн, а также блокировку учётных записей осуществляет администратор сети (администратор локальной вычислительной сети Администрации), определяемый распоряжением Администрации Наро-Фоминского муниципального района.

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

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

Назначенные пользователю ИСПДн права доступа должны быть отражены в матрице доступа пользователей к защищаемым ресурсам ИСПДн.

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

Неиспользуемые учётные записи блокируются (удаляются).

Порядок доступа пользователей ИСПДн к выделенным для его работы ресурсам, контроля и удаления учётных записей определяется Инструкцией о порядке предоставления доступа к защищаемым ресурсам ИСПДн.

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

8. 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 ИСПДн определяется Инструкцией по организации парольной защиты на компьютерах, обрабатывающих конфиденциальную информацию.

9. ПРИМЕНЕНИЕ КРИПТОСРЕДСТВ

Необходимость применения криптосредств при обработке персональных данных может возникнуть в следующих случаях:

- при передаче персональных данных в среду (носители информации, каналы связи), в которой они могут оказаться доступными для несанкционированного доступа;
- в ИСПДн, 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 по работе, 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;
- надёжным 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 Администратором сети.

Порядок обеспечения функционирования и безопасности криптосредств, а также Права и обязанности сотрудников, эксплуатирующих криптосредства, определяются Инструкцией по применению криптосредств для защиты конфиденциальной информации.

10. ОБНОВЛЕНИЕ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ИСПДн

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

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

- в отношении системных и прикладных программных средств – администратору безопасности ПДн с привлечением администратора сети, по согласованию с органом по

аттестации;

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

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 ИСПДн должны проводиться в соответствии с Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн.

11. 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 ИСПДн и администратором безопасности ПДн.

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

Пользователю ИСПДн категорически запрещается:

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

Администратору безопасности ПДн запрещается менять настройки программно-аппаратных средств защиты информации, предустановленные сотрудником органа по аттестации при настройке системы защиты информации в ходе аттестации ИСПДн.

Администрирование средств защиты информации осуществляется администратором безопасности ПДн с привлечением администратора сети.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

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

Приложение к Порядку организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Наро-Фоминского муниципального района Московской области

ПОРЯДОК СОЗДАНИЯ СЗПДН

Создание СЗПДн включает следующие стадии:

1. Предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на создание СЗПДн;

2. Стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

3. Стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приёмо-сдаточные испытания средств защиты информации;

4. Подтверждение соответствия ИСПДн требованиям безопасности информации (аттестат соответствия по требованиям безопасности информации).

1. Предпроектная стадия

На предпроектной стадии по обследованию ИСПДн выполняются следующие мероприятия:

- устанавливается необходимость обработки персональных данных в ИСПДн;

- определяется перечень персональных данных, подлежащих защите;

- определяются условия расположения ИСПДн относительно границ контролируемой зоны;

- определяются конфигурация и топология ИСПДн в целом и её отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

- определяются режимы обработки персональных данных в ИСПДн в целом и в отдельных компонентах;

- уточняется степень участия персонала в обработке персональных данных, характер их взаимодействия между собой;

- определяются (уточняются) угрозы безопасности персональных данных в конкретных условиях функционирования;

- определяется класс ИСПДн.

По результатам предпроектного обследования задаются конкретные требования по обеспечению безопасности персональных данных, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

Техническое задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;

- исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

– определение класса ИСПДн;

– ссылку на нормативные документы, с учётом 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. Стадия проектирования

На стадии проектирования и создания СЗПДн проводятся следующие мероприятия:

– разработка задания и проекта на создание (или модернизацию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

– разработка раздела технического проекта на ИСПДн в части защиты информации;

– работы в соответствии с проектной документацией;

– определение серийно выпускаемых технических средств обработки, передачи и хранения информации, подлежащих использованию в ИСПДн;

– разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– определение сертифицированных технических, программных и программно-технических средств защиты информации, подлежащих использованию в ИСПДн;

– сертификация по требованиям безопасности информации программных средств защиты информации, в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

– разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

– определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности персональных данных;

– разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите персональных данных.

3. Стадия ввода в действие

На стадии ввода в действие СЗПДн осуществляются:

– приобретение, установка, настройка технических средств обработки, передачи и хранения информации;

– приобретение, установка, настройка средств защиты информации;

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приёмо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

– организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, хищение и нарушение

работоспособности технических средств ИСПДн, хищение носителей информации;

- оценка соответствия ИСПДн требованиям безопасности персональных данных;

- подтверждение соответствия ИСПДн требованиям безопасности персональных данных (аттестат соответствия требованиям по безопасности информации).