МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 5

П Р И К А З

29.08.2022 г. № Ш5-13-775/2

г. Сургут

О работе с персональными данными граждан

Во исполнение требований Положения об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства РФ от 1 ноября 2012 г. № 1119, Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также прочих нормативных документов по защите информации, решением Управляющего совета школы протокол от 25.08.2022 г. № 8(33), принятым на заседании педагогического совета МБОУ СОШ № 5 протокол от 30.08.2022 г. № 1

ПРИКАЗЫВАЮ:

1. Ввести в действие «Положение о работе с персональными данными граждан (учеников, выпускников МБОУ СОШ №5, их родителей или опекунов) (Приложение 1).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

Подписано электронной подписью
Сертификат: 3A87F1D9FD6BA452E7A054E60B3942E381262401
Владелец: Петкова Наталья Юрьевна
Действителен: 08.10.2021 с по 08.01.2023

Н.Ю. Петкова

Приложение 1
к Приказу от 22.08.2022
№ Ш5-13-775/2

Положение о работе с персональными данными граждан

1. Политика безопасности персональных данных

1.1. Общие положения

1. Настоящее Положение об организации и проведении работ по обеспечению безопасности персональных данных граждан (учеников, выпускников МБОУ СОШ №5, их родителей или опекунов) при их обработке в информационных системах персональных данных МБОУ СОШ №5 (далее – Положение) разработано в соответствии с ч. 1 ст. 23, ст. 24 Конституции Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее ИСПДн) в МБОУ СОШ №5 (далее – Оператор).
2. Перечень сотрудников, допущенных к работе с персональными данными в ИСПДн, определяется приказом Оператора.
3. Ответственность за обеспечение безопасности персональных данных и надлежащего режима работы ИСПДн возлагается на штатного сотрудника Оператора соответствующим приказом.
4. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

1.2. Область применения и цель положения

1. Положение распространяется на Субъектов персональных данных, являющихся детьми дошкольного возраста.
2. Область применения положения:
   а) помещения обработки и хранения персональных данных, принадлежащие организации;
   б) аппаратные и программные средства, обеспечивающие обработку и хранение персональных данных;
   в) хранилища носителей информации, содержащей персональные данные.
3. Цель данного положения:
   а) определение основных принципов построения системы защиты персональных данных Оператора;
   б) определение основных мер защиты и областей ее внедрения для обеспечения выполнения Федерального законодательства, требования и рекомендаций национальных и международных стандартов в области информационной безопасности персональных данных.

1.3. Основные понятия и определения

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

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

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

Уничтожение персональных данных - данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент информационной безопасности – событие, в результате наступления которого произошло разглашение конфиденциальной информации, нарушение работоспособности ИСПДн, внесение несанкционированных изменений, утечка или разглашение персональных данных клиентов и прочих событий, ведущих к нарушению прав и свобод граждан РФ.

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

1.4. Понятие и состав персональных данных

1. В соответствии с пунктом 1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под персональными данными субъекта (далее Персональные данные) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
2. Перечень обрабатываемых персональных данных граждан (не сотрудников Оператора - детей, их родителей или опекунов):
   - фамилия, имя, отчество (в том числе прежние);
   - дата и место рождения;
   - паспортные данные или данные иного документа, удостоверяющего личность и гражданство;
   - адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
   - номера телефонов (мобильного и домашнего);
   - сведения о семейном положении;
   - сведения о номере и серии страхового свидетельства;
   - сведения государственного пенсионного страхования;

- сведения об идентификационном номере налогоплательщика;
- сведения, указанные в оригиналах и копиях приказов по личному составу и материалах к ним;
- сведения о социальных льготах и социальном статусе;
- фотография;
- сведения о состоянии здоровья.

1.5. Методы и способы защиты персональных данных

1. Методы и способы защиты персональных данных определяются в соответствии с Постановлением правительства № 1119 от 01 ноября 2012, Приказом ФСТЭК России № 21 от 18 февраля 2013г., Приказом ФСБ России № 378 от 10 июля 2014 г.
2. Системы защиты персональных данных должны соответствовать требованиям нормативных и руководящих документов ФСТЭК России, ФСБ России.
3. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.
4. Защита персональных данных субъекта осуществляется за счёт Оператора в порядке, установленном федеральным законом.
5. Оператор при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:
    а) шифровальные (криптографические) средства;
    б) антивирусная защита;
    в) анализ защищённости;
    г) управление доступом;
    д) регистрация и учет;
    е) обеспечение целостности;
    ж) разработка нормативно-методических локальных актов, регулирующих защиту персональных данных.

1.6. Цели обеспечения безопасности

Целью обеспечения безопасности являются:

а) организация непрерывного и защищенного процесса обработки, хранения, передачи информации, содержащей персональные данные;
б) защита прав и свобод граждан РФ (не сотрудников Оператора - детей, их родителей или опекунов), предоставляющих Оператору свои персональные данные для обработки и хранения.

1.7. Принципы обеспечения безопасности

1. Информационная безопасность персональных данных:
    а) основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов;
    б) обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер (программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики информационной системы);
    в) должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования;
    г) должна предусматривать контроль эффективности средств защиты.

2. Информационная безопасность персональных данных должна основываться на следующих принципах.

2.1 Принцип системности – системный подход к защите компьютерных систем предполагает необходимость взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления. При обеспечении информационной безопасности информационных систем необходимо учитывать все слабые и наиболее уязвимые места системы, а также характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения распределенной системы и НСД к информации.

2.2 Принцип комплексности – для обеспечения защиты имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов.

2.3 Принцип непрерывности защиты – защита информации - это не разовое мероприятие и не конкретная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный направленный процесс предполагающий принятие соответствующих мер на всех этапах существования информационной системы. Разработка системы защиты должна вестись параллельно обработке самой защищаемой системы.

2.4 Разумная достаточность – важно правильно выбрать тот уровень защиты при котором затраты, риск и размер возможного ущерба были бы приемлемы и не создавали неудобств пользователю.

2.5 Гибкость системы защиты – часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и средства защиты особенно в начальный период их эксплуатации могут оказывать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения уровня варьирования защищенности средство защиты должно обладать определенной гибкостью, особенно если средство необходимо установить на работающую систему, не нарушая процесса её нормального функционирования.

2.6 Принцип простоты применения средств защиты – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

1.8. Организация безопасности. Ответственность

1. За вопросы безопасности персональных данных несут ответственность следующие сотрудники Оператора:
   - Директор.
   - лица, назначенные Оператором из состава сотрудников, ответственные за организацию работ по защите персональных данных;
   - лица, назначенные Оператором из состава сотрудников, и допущенные к средствам обработки информации и хранилищам, содержащим персональные данные;
   - непосредственно Субъект персональных данных отвечает за корректность своих данных, за соблюдение установленного порядка и мер по обеспечению безопасности ПДн и самолично отвечает за разглашение информации конфиденциального характера, ставшей известной ему.
2. Каждый из обозначенных людей (кроме Субъекта) несет ответственность за неразглашение и корректность обработки ПДн в соответствии с Административным и Уголовным Кодексами РФ.

1.9. Организация безопасности. Направления политики обеспечения безопасности

1. Основными направлениями политики информационной безопасности являются:
   а) соблюдение прав и свобод граждан РФ;

б) соблюдение юридических норм РФ;
в) обеспечение безопасности (конфиденциальности) данных;
г) обеспечение непрерывного и корректного процесса обработки персональных данных, сохранение их целостности, корректности и доступности.

1.10. Организация безопасности. Регистрация инцидентов безопасности

1. Любые инциденты безопасности, в которые входят:
   а) факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
   б) факты сбоя или некорректной работы систем обработки информации;
   в) факты сбоя или некорректной работы средств защиты информации;
   г) факты разглашения информации, содержащей ПДн;
   д) факты разглашения информации о методах и способах защиты и обработки информации, содержащей ПДн,

должны сообщаться сотрудниками Оператора ответственному за обеспечение безопасности. По каждому сообщению, ответственный должен регистрировать инцидент, который в дальнейшем должен проходить процедуру расследования Комиссией, назначенной Оператором в соответствии с утвержденным Порядком проведения служебного расследования, нарушений режима информационной безопасности ИСПДн.

1.11. Организация безопасности. Безопасность средств обработки

1. Безопасность средств обработки обеспечивается организационными и техническими средствами. Организационно осуществляется допуск сотрудников и третьих лиц (если того требует бизнес-процесс), при этом минимизируется круг лиц, имеющих доступ. Права доступа к информации назначаются исходя из их необходимости и достаточности.
2. Технически безопасность обеспечивается корректной настройкой средств обработки информации и установкой наложенных средств защиты информации. Все средства защиты информации должны пройти обязательную процедуру оценки соответствия требованиям безопасности ФСТЭК России и ФСБ России.

1.12. Организация безопасности. Безопасность связи

1. Каналы передачи данных должны обеспечивать безопасное соединение узлов сети Оператором. Безопасность может обеспечиваться следующими мерами:
   а) сегментация сети на зоны обработки ПДн и демилитаризированные зоны посредством физического разделения или с помощью VLAN технологий;
   б) максимальное ограничение доступа и набора протоколов и портов зоны обработки ПДн к сетям общего пользования и сетям международного обмена посредством средств межсетевого экранирования;
   в) обеспечение сетей обработки ПДн, имеющих подключение к сетям общего пользования и сетям международного обмена, средствами обнаружения и предотвращения вторжений;
   г) систематический контроль состояния системы защиты средствами активного аудита;
   д) при прохождении каналов связи вне контролируемой зоны необходимо обеспечивать шифрование передаваемой информации на таких участках.

1.13. Организация безопасности. Физическая безопасность

1. Физическая безопасность может обеспечиваться следующими средствами, исходя из достаточности и необходимости того или иного средства:
   а) организация разрешительной системы доступа в помещения хранения и обработки ПДн;
   б) организация физической охраны;

в) использование систем охранной сигнализации;
г) использование систем видеонаблюдения;
д) конструктивное усиление окон, дверей, стен и иных преград для исключения угрозы несанкционированного доступа.

1.14. Квалификация персонала

1. Сотрудники, участвующие в обработке ПДн, должны иметь соответствующее образование и квалификацию, позволяющие им корректно работать со средствами обработки информации. Не разрешается допуск лиц, не прошедших собеседование с руководителем подразделения на предмет проверки знаний по работе с средствами обработки, осуществляющего обработку ПДн.

1.15. Безопасность документов и носителей информации

1. Обработка осуществляется в строгом соответствии с Положением об организации неавтоматизированной обработки персональных данных, обрабатываемых Оператором.
2. Материальные носители информации должны храниться в сейфах или запираемых шкафах.
3. Все электронные носители информации должны быть промаркированы (возможно использование заводской маркировки) и перечислены в журнале учета. Выдача и сдача электронных носителей осуществляется под роспись пользователя носителя.

2. Организация работ по защите персональных данных

2.1 Создание комиссии по организации работ по защите персональных данных

1. Создание комиссии. Для организации работ по защите информации создается комиссия в составе:
   а) председатель комиссии из состава руководства организации;
   б) члены комиссии.
2. Состав лиц комиссии и ее создание оформляется «Приказом о создании комиссии для организации работ по защите персональных данных».
3. В состав комиссии должны входить следующие сотрудники:
   а) ответственный за организацию работ по защите ПДн;
   б) ответственный за обеспечение безопасности ПДн;
   в) ответственный за обеспечение работы систем обработки ПДн.
4. Функциональные обязанности Комиссии. На членов Комиссии возлагаются следующие обязанности:
   а) определения уровня защищенности (классификация) ИСПДн;
   б) визирование организационно-распорядительных документов Оператора в области защиты персональных данных;
   в) согласование проектных документов ИСПДн и СЗПДн;
   г) контроль состава, функций, состояний ИСПДн и СЗПДн;
   д) визирование актов изменения состава, функций, состояний ИСПДн и СЗПДн.

2.2 Сотрудники, ответственные за обработку и обеспечение защиты персональных данных

1. Лица, ответственные за организацию и обеспечение защиты ПДн назначаются из состава сотрудников Оператора. Они могут быть выделены либо как штатные единицы, либо выполнять данные функции дополнительно к основным трудовым обязанностям, и назначаются приказами (или иными внутренними нормативными актами) Оператора.
2. Функциональные обязанности ответственных лиц определяются в строгом соответствии с утвержденными должностными инструкциями.

2.3 Определение перечня персональных данных. Согласие субъекта ПДн на обработку

1. На начальном этапе внедрения новой ИСПДн определяется перечень обрабатываемых ПДн (далее Перечень). Каждый элемент Перечня должен быть элементарным (то есть не должен быть объединением других элементов, например, элемент «ФИО и паспорт» на самом деле состоит из двух элементов списка: ФИО, паспорт) и оформлен в виде пункта документа «Перечень персональных данных, обрабатываемых Оператором» с указанием обоснования и цели обработки и закреплен внутренним нормативным актом «Приказ об утверждении перечня персональных данных».
2. Оператор должен проводить обоснованную обработку ПДн: каждому элементу Перечня должно быть приведено обоснование.
3. Далее определяется форма согласия субъекта на обработку его ПДн.
4. Согласие должно содержать следующие данные:
    а) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
    б) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
    в) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
    г) цель обработки персональных данных;
    д) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
    е) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
    ж) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
    з) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
    и) подпись субъекта персональных данных.

2.4 Уведомление о начале обработки персональных данных в Роскомнадзор России

1. С помощью Перечня определяется необходимость отправки уведомления в Роскомнадзор России. Отправка не требуется если обработка ПДн ведется на одном из следующих основаниях:
    а) обработка в соответствии с трудовым законодательством;
    б) договорные отношения;
    в) обработка общедоступных данных;
    г) обработка только ФИО Субъекта;
    д) сбор данных, собираемых для однократных пропусков.
    е) включенных в ИСПДн, имеющие статус государственных информационных систем персональных данных;
    ж) обработка без использования средств автоматизации.
2. В иных случаях через Портал персональных данных Роскомнадзора России оформляется уведомление в электронном виде.

2.5 Определение списка лиц, имеющих доступ к обработке персональных данных

1. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к

соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

2. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
3. Круг лиц, имеющих доступ к ПДн, должен быть достаточным для выполнения непрерывной и бессбойной обработки персональных данных, и при этом быть максимально ограниченным для снижения рисков утечки информации.
4. Список может представлять собой перечень структурных подразделений, непосредственно собирающих и обрабатывающих персональные данные с обязательным указанием третьих лиц, имеющих доступ к ПДн, либо перечень конкретных лиц, осуществляющих сбор и обработку.
5. Список должен быть утвержден соответствующим приказом и должен содержать следующие данные:
    а) ФИО/должность лица;
    б) ресурс ПДн;
    в) дата получения доступа;
    г) подпись в уведомлении о доступе;
    д) дата прекращения доступа;
    е) подпись в уведомлении о прекращении доступа.

2.6 Определение контролируемой зоны и помещений обработки персональных данных

1. Контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
2. Контролируемая зона может ограничиваться периметром охраняемой территории частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнатой, кабинетом, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться размером больше, чем охраняемая территория, при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.
3. Территория контролируемой зоны определяется Приказом (или иным внутренним нормативным актом) Оператора.
4. Помещениями обработки персональных данных являются все помещения на территории Контролируемой зоны Оператора, в которых содержатся:
    а) системы хранения данных, содержащих ПДн;
    б) системы защиты информации;
    в) станции ввода, обработки, просмотра ПДн.
5. Перечень помещений обработки персональных данных определяется Приказом (или иным внутренним нормативным актом) Оператора.
6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.7 Определение прав доступа лиц, имеющих доступ к обработке персональных данных

1. Права доступа лиц, имеющих доступ к обработке персональных данных, определяются в необходимом и достаточном объеме для осуществления обработки. Предоставление прав реализуется ответственным за обеспечение безопасности персональных данных. Объем необходимых прав определяется ответственным за организацию работ по защите персональных

данных по устному согласованию с руководителем подразделения, осуществляющего обработку ПДн.

2.8 Определение прав доступа лиц, имеющих доступ к сопровождению систем защиты и обработки персональных данных

1. Права доступа лиц, имеющих доступ к сопровождению систем защиты и обработки персональных данных, определяются из соображений разделения ролей обеспечения безопасности персональных данных и обеспечения работы систем обработки персональных данных.
2. Роль обеспечения безопасности (администратор безопасности ПДн) должна реализовывать следующие функции:
    а) аудит доступа (организационный и инструментальный);
    б) назначение прав доступа;
    в) установка и удаление из системы СЗИ;
    г) управление настройками СЗИ.
3. Роль обеспечения работы систем обработки персональных данных (администратор информационной системы) должна реализовывать следующие функции:
    а) установка и удаление средств обработки ПДн;
    б) управление настройками средств обработки ПДн;
    в) установка и удаление вспомогательных средств обработки ПДн и не связанных с обработкой систем;
    г) управление настройками вспомогательных средств обработки ПДн и не связанных с обработкой систем.
4. Права доступа регламентируются соответствующими внутренним нормативным актом: матрицей доступа.

3. Проектирование системы защиты персональных данных

3.1 Определение угроз безопасности персональных данных

1. Определение угроз безопасности персональных данных осуществляется в соответствии с Постановлением правительства №1119 от 01 ноября 2012, Приказом ФСТЭК России № 21 от 18 февраля 2013г. В следствие вышеуказанного требуется разработать «Модель угроз безопасности персональным данным» на каждую ИСПДн.
2. Модель угроз разрабатывается в соответствии с РД «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России. Оценка рисков должна производится как совокупная экспертная оценка специалистов по обеспечению безопасности и специалистов по обеспечению работы систем обработки данных.

3.2 Классификация информационной системы персональных данных

1. Классификация проводится Комиссией (см. п. 2.1).
2. По результатам анализа исходных данных уровень защищенности (класс) информационной системы персональных данных определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами.

3.3 Выбор средств защиты персональных данных

1. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.
2. На территории РФ единственной формой оценки соответствия является сертификация на соответствие требованиям безопасности информации ФСТЭК России и ФСБ России.

3. Выбранные СЗИ должны обеспечивать нейтрализацию всех угроз, выявленных в модели угроз безопасности персональным данным.
4. Перечень внедренных СЗИ и СКЗИ должен быть отражен в журналах, ведущихся ответственным за обеспечение безопасности персональных данных.

3.4 Оценка соответствия системы защиты требованиям по информационной безопасности

1. Оценка соответствия внедренной системы защиты проводится с использованием сертифицированных в системе сертификации ФСТЭК России инструментальных средств с оформлением заключения о готовности системы защиты или проведении аттестационных испытаний с привлечением лицензиата ФСТЭК России.
2. В случае аттестации, при успешных испытаниях выдается официальный Аттестат соответствия ИСПДн требованиям по безопасности информации.

4. Обеспечение безопасности персональных данных

4.1 Информационные ресурсы, содержащие персональные данные

1. Информационные ресурсы, содержащие персональные данные, должны быть обособлены и не пересекаться с информационными ресурсами систем обработки иных систем. Обособление должно обеспечиваться организационными мерами, мерами физической защиты и средствами защиты информации.
2. Информационные ресурсы создаются для обработки, хранения, передачи информации, содержащей ПДн и объединенных одной целью обработки.

4.2 Передача персональных данных

1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.
2. При передаче персональных данных работники Оператора должны соблюдать следующие требования:
    а) Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.
    б) Осуществлять передачу персональных данных субъектов в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.
    в) Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.
    г) Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.3 Хранение и использование персональных данных

1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.
2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях.
3. Хранение персональных данных субъекта может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами.

5. Порядок предоставления доступа к информационным ресурсам, содержащим персональные данные

5.1 Порядок предоставления доступа

1. Порядок предоставления доступа сотрудникам, осуществляющим обработку ПДн, должен быть регламентирован внутренним нормативным актом (см. п. 2.5).
2. Оператором должна быть разработана «Инструкция по учету лиц, допущенных к работе с персональными данными», матрицы доступа на каждую ИСПДн, «Инструкция пользователя по обработке персональных данных».
3. В общем виде порядок доступа новых сотрудников должен осуществляться по следующей схеме:
    а) Принимаемый сотрудник в соответствии с занимаемой должностью и Приказом о списке лиц, имеющих доступ к обработке ПДн (см. п. 2.5) наделяется правом доступа к обработке ПДн.
    б) Сотрудник ознакамливается с «Приказом о списке лиц, имеющих доступ к обработке ПДн», «Обязательством о неразглашении информации конфиденциального характера» Положениями и Инструкциями по работе с персональными данными и ставит отметки об ознакомлении в «Журнале инструктажа персонала».
    в) Сотрудник расписывается в «Журнале учета лиц, имеющих доступ к обработке ПДн», получая доступ к соответствующим информационным ресурсам.

5.2 Порядок прекращения доступа

1. В общем виде порядок прекращения доступа следующий, сотрудник (в связи с увольнением или иным причинам отсутствия необходимости обработки ПДн, используя конкретный информационный ресурс) должен расписаться в «Журнале учета лиц, имеющих доступ к обработке ПДн», указав дату прекращения доступа.

6. Аудит безопасности систем обработки персональных данных

6.1 Виды аудита

1. Аудит безопасности производится ответственным за обеспечение безопасности персональных данных регулярно, а также в ситуациях, требующих проведения расследования инцидента, связанного с нарушением информационной безопасности.
2. Ответственный должен руководствоваться инструкциями и правилами:
    а) Правила парольной защиты.
    б) Правила антивирусной защиты.
    в) Правила обновления общесистемного и прикладного программного обеспечения ИСПДн.
    г) Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн.
    д) Порядок предоставления информации.
    е) Порядок расследования инцидентов безопасности.
    ж) Порядок приостановки предоставления доступа к ПДн в случае обнаружения нарушений порядка их обработки.
    з) Инструкция по организации резервирования и восстановления.
3. Аудит состоит из пассивных и активных мер контроля.

6.2 Протоколирование и пассивный аудит

1. Протоколирование и пассивный аудит предназначены для осуществления контроля за наиболее критичными компонентами сети, включающими в себя серверы приложений, баз данных и

прочие сетевые серверы, межсетевые экраны, рабочие станции управления сетью и т.п. Компоненты этой подсистемы осуществляют протоколирование, централизованный сбор и анализ событий, связанных с безопасностью (включая предоставление доступа, попытки аутентификации, изменение системных политик и пользовательских привилегий, системные сбои и т.п.). Они включают в себя как средства защиты информации, так и встроенные средства, имеющиеся в составе ОС, СУБД, приложений и т.п. осуществляющие обработку ПДн и предназначенные для регистрации событий безопасности. Все данные аудита поступают на выделенный сервер аудита, где осуществляется их хранение и обработка.

2. Подсистема пассивного аудита безопасности выполняет следующие основные функции:
    а) отслеживание событий, влияющих на безопасность системы;
    б) регистрация событий, связанных с безопасностью в журнале аудита;
    в) выявление нарушений безопасности, путем анализа данных журналов аудита ответственным за обеспечение безопасности ПДн в фоновом режиме.
3. Средства протоколирования и аудита должны применяться на всех рубежах защиты в следующем объеме:
    а) На рубеже защиты внешнего периметра должны протоколироваться следующие события:
    – информация о состоянии внешнего маршрутизатора, МЭ, сервера удаленного доступа, модемов;
    – действия внешних пользователей по работе с внутренними информационными ресурсами;
    – действия внутренних пользователей по работе с внешними информационными ресурсами;
    – попытки нарушения правил разграничения доступа на МЭ;
    – действия администраторов МЭ.
    б) На рубеже защиты серверов и рабочих станций средствами подсистем аудита безопасности ОС должно обеспечиваться протоколирование всех системных событий, связанных с безопасностью, включая удачные и неудачные попытки регистрации пользователей в системе, доступ к системным ресурсам, изменение политики аудита и т. п.
    в) На уровне приложений должна обеспечиваться регистрация событий, связанных с их функционированием, средствами этих приложений.
4. Эффективность функционирования системы пассивного аудита безопасности определяется следующими основными свойствами этой системы:
    а) наличие средств аудита, обеспечивающих возможность выборочного контроля любых происходящих в системе событий, связанных с безопасностью;
    б) наличие средств централизованного управления журналами аудита, политикой аудита и централизованного анализа данных аудита по всем контролируемым системам;
    в) непрерывность контроля над критичными компонентами ЛВС во времени.

6.3 Активный аудит

1. Активный аудит безопасности предназначен для автоматического выявления нарушений безопасности критичных компонентов ИСПДн и реагирования на них в режиме реального времени. К числу критичных компонентов ИСПДн, с наибольшей вероятностью подверженных атакам со стороны злоумышленников, относится внешний защищенный шлюз в сеть Интернет, сервер удаленного доступа, серверная группа и рабочие станции управления сетью.
2. Для сбора информации и реагирования на инциденты используются сертифицированные средства анализа защищенности сетей, операционных систем.
3. Анализатор сетевого трафика должен обнаруживать известные типы сетевых атак при подключении к сетям международного обмена.

4. Анализ защищенности должен проводиться путем эмуляции действий возможного злоумышленника по осуществлению удаленных атак, а также средства системного уровня, и предназначенные для анализа параметров конфигурации операционных систем и приложений, выявления уязвимостей, коррекции конфигурационных параметров и контроля изменения состояния операционных систем и приложений.
5. Средства анализа защищенности системного и прикладного уровней предназначены для решения следующих основных задач:
    а) анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей, связанных с их некорректной настройкой, определения уровня защищенности контролируемых систем и соответствия политике безопасности организации;
    б) коррекция конфигурационных параметров операционных систем и приложений;
    в) контроль изменения состояния операционных систем и приложений, осуществляемый на основе мгновенных снимков их параметров и атрибутов файлов.
6. Средства контроля защищенности системного уровня должны выполнять проверки привилегий пользователей, политик управления паролями и регистрационных записей пользователей, параметров подсистемы резервного копирования, командных файлов, параметров системы электронной почты, настройки системных утилит и т.п.

7. Расследование инцидентов информационной безопасности

7.1 Порядок регистрации

1. Источником информации об инциденте информационной безопасности может служить следующее:
    а) сообщения работников, родителей или опекунов детей Оператора, направленные Оператору в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;
    б) уведомления/сообщения органов, осуществляющих контроль или надзор за деятельностью Оператора;
    в) данные, полученные на основании анализа журналов СЗПДн.
2. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).
3. Сотрудник, получивший информацию об инциденте, должен сообщить об этом администратору безопасности ПДн. Администратор безопасности ПДн сообщает об инциденте ответственному за организацию работ по обработке ПДн и начальнику подразделения, в котором случился инцидент.
4. Все инциденты информационной безопасности должны регистрироваться в журнале регистрации нештатных ситуаций. Журнал инцидентов информационной безопасности должен постоянно актуализироваться.

7.2 Порядок разбора

1. Разбором инцидентов информационной безопасности занимается Комиссия, назначаемая в соответствии с Порядком проведения служебного расследования, нарушений режима информационной безопасности ИСПДн.
2. После сбора информации ответственным за обеспечение безопасности по инциденту Комиссия анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания сотрудников и др.).
3. Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

4. По окончании разбора инцидента информационной безопасности комиссией оформляется отчет, в котором указываются основные «контрольные точки» инцидента.
5. Отчет предоставляется директору Оператора. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.
6. После окончания расследования Комиссия принимает решение о наказании виновных лиц и согласовывает решение с директором.

8. Предоставление информации по обращению субъекта персональных данных

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
    а) подтверждение факта обработки персональных данных оператором;
    б) правовые основания и цели обработки персональных данных;
    в) цели и применяемые оператором способы обработки персональных данных;
    г) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
    д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
    е) сроки обработки персональных данных, в том числе сроки их хранения;
    ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
    з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
    и) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
    к) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
2. Все обращения субъектов ПДн обрабатываются в соответствии с утвержденным Регламентом реагирования Работников Оператора на обращения субъектов персональных данных.