УТВЕРЖДЕНО
приказом школы
от 09.06.2014 № 76

Политика в области обработки и обеспечения безопасности персональных данных в информационных системах

ерование и
о 16
73 листов

Тобольск

Оглавление

Введение

Настоящая политика информационной безопасности (далее - Политика) муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа № 13» (далее-Школа) представляет собой документ, в котором определены требования к пользователям информационных систем персональных данных, должностные обязанности и степень ответственности сотрудников, связанных с обработкой ПДн.

Также Политика описывает работы по обеспечению безопасности ПДн, состав системы защиты персональных данных и основывается на следующих нормативно-правовых и методических документах:

- Федеральный Закон от 27.07.2006 № 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».
- положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;
- положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное приказом ФСТЭС России от 05.02.2010 № 58;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утвержденные Постановлением Правительства РФ от 06.07.2008 № 512;
- нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн;
- концепция информационной безопасности информационных систем персональных данных Школы.

Политика служит основой для разработки системы защиты персональных данных, документов, регламентирующих обязанности пользователей информационных систем, порядков обработки персональных данных и иных нормативных и методических документов.

1. Термины и определения

Следующие термины и определения могут быть использованы в настоящем документе:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

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

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

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

Вспомогательные технические средства и системы- технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация -информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

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

Источник угрозы безопасности информации -субъект доступа, материальный объект или

физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

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

Межсетевой экран - локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

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

Оператор (персональных данных) - 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.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки -электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее

результаты ее функционирования.
Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Программная закладка -код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.
Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.
Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.
Средства вычислительной техники -совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Субъект доступа (субъект) -лицо или процесс, действия которого регламентируются правилами разграничения доступа.
Технические средства информационной системы персональных данных –средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.
Технический канал утечки информации -совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
Угрозы безопасности персональных данных -совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.
Утечка (защищаемой) информации по техническим каналам -неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.
Уязвимость -слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
Целостность информации -способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

Следующие обозначения и сокращения могут быть использованы в настоящем документе:
АВС - антивирусные средства
АРМ - автоматизированное рабочее место
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона

ЛВС - локальная вычислительная сеть
МЭ - межсетевой экран
НСД - несанкционированный доступ
ОС - операционная система
ТТДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПЭМИН - побочные электромагнитные излучения и наводки
САЗ - система анализа защищенности
СЗИ - средства защиты информации
СЗПДн -система (подсистема) защиты персональных данных
СОВ - система обнаружения вторжений
ТКУИ - технические каналы утечки информации
УБПДн - угрозы безопасности персональных данных

3. Общие положения

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в концепции информационной безопасности ИСПДн Школы.

Целью Политики является обеспечение безопасности объектов защиты ИСПДн от внешних и внутренних, умышленных и непреднамеренных угроз, а также - минимизация ущерба от возможной реализации угроз безопасности ПДн.

Требования Политики распространяются на всех сотрудников Школы (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

Все сотрудники, участвующие в обработке ПДн, а также лица, получающие временный доступ к ПДн на законном основании, знакомяться с Политикой под роспись. Соответствующая запись осуществляется в журнале ознакомления сотрудников с документами по обработке и защите ПДн.

На основании Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» Политика должна быть выложена на сайте Учреждения (при наличии сайта) в течение 10 дней с момента утверждения.

4. Категории пользователей ИСПДн

В концепции информационной безопасности ИСПДн определены основные категории пользователей ИСПДн. Эти категории должны быть адаптированы под каждую ИСПДн Школы. То есть под конкретную ИСПДн пользователи могут быть дополнительно разделены, также определён их уровень доступа и возможности.

Выделим следующие категории пользователей, участвующих в обработке ПДн в ИСПДн:

— Ответственный за ИСПДн;
— Администратор безопасности ИСПДн;
— Оператор ИСПДн;
— Администратор сети;
— Технический специалист по обслуживанию периферийного оборудования;
— Программист-разработчик ИСПДн.

• Ответственный за ИСПДн - работник, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа Оператору ИСПДн к элементам хранящим персональные данные. Ответственный за ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

• Администратор безопасности ИСПДн - работник, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент. Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Ответственного за ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки межсетевых экранов и систем обнаружения атак, в соответствии с которыми Оператор ИСПДн получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты ПДн;
- устанавливать доверительные отношения своей защищенной сети с сетями других учреждений.

• Оператор ИСПДн - работник, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор ИСПДн не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

• Администратор сети - работник, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности. Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

• Технический специалист по обслуживанию периферийного оборудования - работник, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности. Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

• Программист-разработчик информационной системы персональных данных - сотрудник организации-поставщика или сотрудник Школы, обеспечивающий сопровождение прикладного программного обеспечения. Лицо

этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

Пользователи ИСПДн назначаются и разделяются для каждой ИСПДн Школы. Данные о категориях пользователей, уровне их доступа к объектам ИСПДн и информированности отражены в положении о разграничении прав доступа сотрудников к ПДн.

5. Организация системы защиты ПДн

Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Школы, должны осуществляться в рамках системы защиты персональных, развертываемой в ИСПДн в процессе ее создания или модернизации.

СЗПДн должна представлять собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

СЗПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн. Для существующих ИСПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

В Политике отражены меры по обеспечению безопасности ПДн, которые могут быть включены в СЗПДн.

СЗПДн строится на основании следующих документов:

- актов обследования ИСПДн;
- перечня ПДн, подлежащих защите;
- перечня ИСПДн;
- порядка определения уровня защищенности ПДН в ИСПДн;
- модели угроз безопасности ПДн в ИСПДн;
- положении о разграничении прав доступа сотрудников к ПДн;

В результате делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в плане мероприятий по обеспечению безопасности ПДн.

Для каждой ИСПДн из перечня ИСПДн составляется список программного обеспечения участвующего в обработке ПДн.

В зависимости от требуемого уровня защищенности ПДн в ИСПДн и совокупности актуальных угроз безопасности система защиты ПДн может включать в себя следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Кроме того, должны быть включены меры защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС) и прикладным программным обеспечением, осуществляющим:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- обнаружение вторжений в объекты ИСПДн.

Перечень используемых технических средств также отражается в плане мероприятий по

обеспечению безопасности ПДн. Перечень используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть представлены в плане мероприятий и утверждены директором Школы или Администратором безопасности ИСПДн.

6. Состав системы защиты ПДн

Система защиты ПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от требуемого уровня защищенности ИСПДн, утвержденного в порядке определения уровня защищенности ПДн в ИСПДн.

- Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:
  - идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
  - идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
  - идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
  - регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
  - регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
  - регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

- Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при случайной или намеренной модификации. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.
- Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ операторов ИСПДн. Средства антивирусной защиты предназначены для реализации следующих функций:
  - резидентный антивирусный мониторинг;
  - антивирусное сканирование;
  - скрипт-блокирование;
  - централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
  - автоматизированное обновление антивирусных баз;
  - ограничение прав пользователя на остановку исполняемых задач и изменения

настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

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

- Подсистема межсетевого экранирования предназначена для реализации следующих функций:
  - фильтрации открытого и зашифрованного (закрытого) IP-трафика;
  - фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
  - идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
  - регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
  - контроля целостности своей программной и информационной части;
  - фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
  - фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
  - регистрации и учета запрашиваемых сервисов прикладного уровня;
  - блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
  - контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования классом не ниже 4.

- Подсистема анализа защищенности предназначена для выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.
- Подсистема обнаружения вторжений предназначена для выявления сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.
- Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн при ее передачи по каналам связи сетей общего пользования и (или) международного обмена. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

7. Проведение работ по созданию системы защиты ПДн

Проведение работ по созданию (модернизации) СЗПДн Школы предполагает реализацию следующих стадий:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

На предпроектной стадии определяется требуемый уровень защищённости ИСПДн, формируется модель угроз безопасности ПДн в ИСПДн, разрабатывается техническое задание на СЗПДн.

Определение требуемого уровня защищённости ПДн, обрабатываемых в ИСПДн, осуществляется в соответствии порядком определения уровня защищенности ПДн в ИСПДн;

Модель угроз безопасности ПДн в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России, а так же соответствующих ведомственных методических рекомендациях;

Перечень актуальных угроз формируется для каждой ИСПДн с учетом особенностей обработки ПДн;

Формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания СЗПДн.

Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн, а именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания СЗПДн;

Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПДн и средства защиты информации.

На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение уровня защищённости ПДн, обрабатываемых в ИСПДн;
- произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.).

8. Проведение работ по обеспечению безопасности ПДн

Под работами по обеспечению безопасности ПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мер, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн.

Проведение работ по обеспечению безопасности ПДн осуществляется в соответствии с концепцией информационной безопасности ИСПДн.

Работы по приведению деятельности Школы в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн Школы.

Проведение работ возлагается на специально создаваемую для этих целей комиссию и/или ответственных работников. В случаях, когда Школа на основании договора поручает обработку ПДн другому лицу/сторонней организации, необходимо выполнить одно из следующих условий:

- в тексте договора в требованиях к контрагенту прописывается обязанность обеспечения контрагентом безопасности и конфиденциальности ПДн;
- в случае невозможности или нецелесообразности изменения текста договора оформляется дополнительное соглашение к договору или соглашение о конфиденциальности, в котором прописывается обязанность обеспечения

контрагентом конфиденциальности ПДн и безопасности ПДн при их обработке.

Далее представим перечень мер по обеспечению безопасности ПДн по каждому из направлений.

- при обработке ПДн без использования средств автоматизации:
  - должен быть определён перечень лиц, осуществляющих неавтоматизированную обработку ПДн;
  - должно проводиться информирование работников об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
  - должен вестись учет и защита носителей ПДн;
  - должно проводиться разграничение доступа к носителям ПДн;
  - должно производиться уничтожение сведений, содержащих ПДн;
  - обработка должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, имеющих к ним доступ;
  - фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации;
  - фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не должна допускаться.
  - при необходимости использования или распространения определенных ПДн должно осуществляться копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и использоваться копия ПДн: например, копирование части страницы, содержащей ПДн, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;
  - при необходимости уничтожения или блокирования части ПДн должен уничтожаться или блокироваться материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию: например, копирование только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги;
  - если при работе с ПДн необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители должны запираться в отведенных для этого шкафах или сейфах.
- при обработке ПДн в ИСПДн
  - должен вестись учет действий, совершаемых с ПДн в ИСПДн работниками Школы;
  - доступ к ПДн должен определяться положением о разграничении прав доступа сотрудников к ПДн;
  - должны быть проинформированы лица, участвующие в обработке ПДн, о факте обработки ими ПДн (реализуется путем ознакомления лиц, обрабатывающих ПДн, с положением о разграничении прав доступа сотрудников к ПДн), о категориях обрабатываемых ПДн (реализуется путем ознакомления с утвержденным перечнем ПДн, подлежащих защите), о правилах осуществления обработки ПДн (реализуется путем проведения инструктажа сотрудниками, участвующими в обработке ПДн);
  - должен осуществляться мониторинг фактов несанкционированного доступа к ПДн и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором безопасности ИСПДн;
  - должна существовать возможность и средства для восстановления ПДн при их модификации или уничтожении вследствие несанкционированного доступа к ним;
  - должен быть определен перечень помещений, используемых для обработки ПДн. При

этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- Операторы ИСПДн должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя Операторы ИСПДн должны немедленно сообщить об этом Администратору безопасности ИСПДн;
- в случае достижения цели обработки должно прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральным законом.

• в целях своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн раз в год должен проводиться анализ изменений процессов защиты ПДн в:

- перечне лиц (подразделений), участвующих в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечне обрабатываемых ПДн;
- целях обработки ПДн;
- способах обработки ПДн (автоматизированная, неавтоматизированная);
- перечне сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача ПДн;
- перечне программно-технических средств, используемых для обработки ПДн;
- конфигурации и топологии ИСПДн в целом и ее отдельных компонентах, физических, функциональных и технологических связях как внутри этих систем, так и с другими системами различного уровня и назначения;
- способах физического подключения и логического взаимодействия компонентов ИСПДн;
- способах подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- режимах обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- составе используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;
- перечне организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн;
- физических меры защиты ПДн, организации пропускного режима.

Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

Задачи по приведению ИСПДн в соответствие с требования законодательства РФ в области защиты ПДн возлагаются на Администратора безопасности ИСПДн.

9. Требования к сотрудникам по обеспечению безопасности ПДн

- все сотрудники, являющиеся Пользователями ИСПДн, должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.
- при вступлении в должность нового сотрудника непосредственный Администратор безопасности ИСПДн должен организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.
- сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.
- сотрудники, использующие технические средства аутентификации, должны

обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

- сотрудники должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
- сотрудники должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все Операторы ИСПДн должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
- сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
- сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе в ИСПДн, третьим лицам.
- при работе с ПДн в ИСПДн сотрудники обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
- при завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
- сотрудники должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.
- сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, Ответственному за ИСПДн или Администратору безопасности ИСПДн;
- при возникновении условий, влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности ПДн и пр.) сотрудникам необходимо незамедлительно проинформировать об этом Администратору безопасности ИСПДн.

Более подробно представленные требования представлены в должностных обязанностях пользователей ИСПДн.

10.Должностные обязанности Пользователей ИСПДн

Должностные обязанности Пользователей ИСПДн описаны в следующих документах:

- инструкция администратора безопасности ИСПДн;
- инструкция ответственного за ИСПДн;
- инструкция Оператора ИСПДн;
- инструкция по антивирусной и парольной защите;
- порядок работы с носителями ПДн, конфиденциальной информацией и сетью интернет;
- положение о разграничении прав доступа к ПДн;
- положение об обработке ПДн

11.Ответственность Пользователей ИСПДн

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Ответственный за ИСПДн и Администратор безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учётных записей или системных учётных записей, если не доказан факт несанкционированного использования учётных записей.

При нарушениях Операторами ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.