Российская Федерация
Департамент образования Администрации г. Екатеринбурга
Муниципальное автономное общеобразовательное учреждение
средняя общеобразовательная школа № 19 (МАОУ СОШ № 19)
ул. П. Шаманова, 18 т. 366-86-68

УТВЕРЖДАЮ
Директор МАОУ СОШ № 19
_____С.А.Белова
«___»_____2018 г.
Приказ от «01»_06_____2018 г. № 330

ПРОГРАММА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАОУ СОШ № 19

Составил: Буров Андрей Владимирович
Заместитель директора

Екатеринбург, 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящая программа политики информационной безопасности Муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 19 (далее – программа), представляет собой документ, в котором определены и изложены требования к пользователям информационных систем персональных данных, должностные обязанности и степень ответственности сотрудников МАОУ СОШ № 19, связанных с обработкой ПДн, а также предусматривает принятия необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

Программа описывает работы по обеспечению безопасности ПДн, состав системы защиты персональных данных МАОУ СОШ № 19 и основываются на следующих нормативно-правовых и методических документах:

- Конституции Российской Федерации (с учетом поправок, внесенных Законами Российской Федерации, о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ);
- Федерального закона № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»;
- Закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Конвенции о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);
- Федерального закона Российской Федерации от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи»;
- Федерального закона от 25.07.2002 N 115-ФЗ (ред. от 03.07.2016) «О правовом положении иностранных граждан в Российской Федерации» (с изм. и доп., вступ. в силу с 31.07.2016);
- Федерального закона от 01.06.2005 N 53-ФЗ (ред. от 05.05.2014) «О государственном языке Российской Федерации»;
- «Правил подключения общеобразовательных учреждений к единой системе Контент-фильтрации доступа к сети интернет», реализованной Министерством образования и науки РФ, (утвержденные Минобрнауки РФ от 11.05.2011 г. № АФ-12/07 вн).

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.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения, которые могут быть использованы в настоящем документе:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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.

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

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).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Обозначения и сокращения, которые 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

ПДн – персональные данные

ПО – программное обеспечение

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности Муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 19 (далее – МАОУ СОШ № 19) города Екатеринбурга определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются сотрудники образовательной организации при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности МАОУ СОШ № 19 является защита информации образовательной организации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

1.3. Политика информационной безопасности разработана в соответствии с:

- Конституцией Российской Федерации (с учетом поправок, внесенных Законами Российской Федерации, о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ);
- Федеральным законом № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»;
- Законом Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- Федеральным законом Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Конвенцией о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);
- Федеральным законом Российской Федерации от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи»;
- Федеральным законом от 25.07.2002 N 115-ФЗ (ред. от 03.07.2016) «О правовом положении иностранных граждан в Российской Федерации» (с изм. и доп., вступ. в силу с 31.07.2016);
- Федеральным законом от 01.06.2005 N 53-ФЗ (ред. от 05.05.2014) «О государственном языке Российской Федерации»;
- «Правилами подключения общеобразовательных учреждений к единой системе Контент-фильтрации доступа к сети интернет», реализованной Министерством образования и науки РФ, (утвержденные Минобрнауки РФ от 11.05.2011 г. № АФ-12/07 вн).
- иными нормативными правовыми актами в сфере защиты информации.

1.4. Выполнение требований Политики информационной безопасности является обязательными для всех участников образовательного процесса.

1.5. Требования Политики информационной безопасности является обязательными, и распространяются на всех сотрудников МАОУ СОШ № 19

(штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

1.6. Всем сотрудникам МАОУ СОШ № 19, участвующим в обработке ПДн, а также лицам, получающим временный доступ к ПДн на законном основании, необходимо ознакомиться с настоящей Программой под роспись. Соответствующая запись осуществляется в **журнале ознакомления сотрудников МАОУ СОШ № 19 с документами по обработке и защите ПДн.**

1.7. Ответственность за соблюдение информационной безопасности несет каждый сотрудник образовательной организации.

2. ЦЕЛЬ И ЗАДАЧИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬИ

2.1. Основными целями политики информационной безопасности являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам образовательной организации;
- защита целостности информации с целью поддержания возможности образовательной организации по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами образовательной организации;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами политики информационной безопасности являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;

- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности образовательной организации;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности образовательной организации;
- организация антивирусной защиты информационных ресурсов образовательной организации – защита информации образовательной организации от несанкционированного доступа и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору образовательной организации.

3. КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Политика информационной безопасности МАОУ СОШ № 19 направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников образовательной организации, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

Наибольшими возможностями для нанесения ущерба обладает собственный персонал образовательной организации.

Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Стратегия обеспечения информационной безопасности МАОУ СОШ № 19 заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников образовательной организации.

4. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Основными принципами обеспечения информационной безопасности:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов образовательной организации;
- своевременное обнаружение проблем, потенциально способных повлиять на информационной безопасности образовательной организации, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками образовательной организации за обеспечение информационной безопасности образовательной организации исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. ОБЪЕКТЫ ЗАЩИТЫ

5.1. Объектами защиты с точки зрения информационной безопасности являются:

- информационный процесс профессиональной деятельности;
- информационные активы образовательной организации.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности образовательной организации;
- персональные данные – любая информация, относящаяся к определенному 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;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В отношении всех собственных информационных активов МАОУ СОШ № 19, активов, находящихся под контролем образовательной организации, а также активов, используемых для получения доступа к инфраструктуре образовательной организации, должна быть определена ответственность соответствующего сотрудника образовательной организации.

6.2. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами образовательной организации должна доводиться до сведения директора образовательной организации.

6.3. Все работы в пределах образовательной организации должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

6.4. Внос в здание и помещения образовательной организации личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы образовательной организации производится только при согласовании с заместителем директора по информатизации.

6.5. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну образовательной организации и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.6. В течении каждой учебной четверти должны периодически пересматриваться права доступа сотрудников и других пользователей к соответствующим информационным ресурсам.

6.7. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6.8. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе коллегам, членам своей семьи и близким.

6.9. В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не более 10 минут.

6.10. Каждый сотрудник обязан немедленно уведомить заместителя директора по информатизации (или при его отсутствии – администрацию МАОУ СОШ № 19) обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам МАОУ СОШ № 19 должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам образовательной организации должен быть четко определен, контролируем и защищен.

6.11. Сотрудникам, использующим в работе портативные компьютеры образовательной организации, может быть предоставлен удаленный доступ к сетевым ресурсам образовательной организации в соответствии с правами в корпоративной информационной системе.

6.12. Сотрудникам, работающим за пределами образовательной организации с использованием компьютера, не принадлежащего образовательной организации, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ и наоборот.

6.13. Сотрудники, имеющие право удаленного доступа к информационным ресурсам МАОУ СОШ № 19, должны соблюдать

требование, исключающее одновременное подключение их компьютера к сети образовательной организации и к каким-либо другим сетям, не принадлежащим образовательной организации.

6.14. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети образовательной организации, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.15. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности. Кроме того, доступ к сети Интернет допускается только с компьютеров с установленным антивирусным программным обеспечением, в котором имеется встроенный Firewall, имеющее последние обновления и включенным «Интрнет-Цензором»

6.16. Рекомендованные правила при работе с сетью Интернет:

- сотрудникам образовательной организации разрешается использовать сеть Интернет только в служебных целях и целях образовательного и воспитательного процесса;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- сотрудники образовательной организации не должны использовать сеть Интернет для хранения корпоративных данных;

- работа сотрудников образовательной организации с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации образовательной организации в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем образовательной организации;
- сотрудники образовательной организации я перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть образовательной организации для всех лиц, не являющихся сотрудниками образовательной организации, включая членов семьи сотрудников образовательной организации.

6.17. Заместитель директора (а также и администрация МАОУ СОШ № 19) имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.18. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация образовательной организации.

6.19. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит заместитель директора по информатизации или инженером обслуживающим компьютерную технику и периферию образовательной организации.

6.20. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, приводы для CD/DVD-дисков), коммуникационное

оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются «компьютерное оборудование».

6.21. Компьютерное оборудование, предоставленное образовательной организации, является ее собственностью и предназначено для использования исключительно в производственных целях.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

В случае утери, порчи, заражения вирусами, сотрудники несут персональную ответственность в соответствии с действующим законодательством РФ.

6.22. Все компьютеры должны защищаться паролем при загрузке системы. Для установки и настройки режимов защиты пользователь должен обратиться к заместителю директора по информатизации.

6.23. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Кроме того, должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6.24. При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации и защиты от вирусов.

Порты передачи данных, в том числе USB и CD/DVD приводы в стационарных компьютерах и ноутбуках сотрудников МАОУ СОШ № 19

блокируются, за исключением тех случаев, когда сотрудником получено разрешение от заместителя директора по информатизации.

6.25. Все программное обеспечение, установленное на предоставленном МАОУ СОШ № 19 компьютерном оборудовании, является собственностью образовательной организации и должно использоваться исключительно в производственных целях и целях образовательного и воспитательного процесса. Самостоятельная установка и настройка программного обеспечения сотрудниками МАОУ СОШ № 19 не допускается, **использование нелицензионного программного обеспечения – ЗАПРЕЩЕНО!**

6.26. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности и целям образовательного и воспитательного процесса. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено директору образовательной организации, кроме того, сотрудник может понести административную и уголовную ответственность в соответствии с действующим законодательством РФ.

6.27. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков.

6.28. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной заместителем директора по информатизации.

Сотрудники образовательной организации не имеют права:

- блокировать антивирусное программное обеспечение;

- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.29. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию образовательной организации по электронной почте без использования систем шифрования. Строго конфиденциальная информация образовательной организации, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.30. Использование сотрудниками МАОУ СОШ № 19 публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации ЛВС при условии применения механизмов шифрования.

Сотрудники образовательной организации для обмена документами должны использовать только свой официальный адрес электронной почты (указанный в анкете).

6.31. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать заместителя директора

по информатизации (а при его отсутствии – администрацию МАОУ СОШ № 19). Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.32. Не допускается при использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.33. Все пользователи должны быть осведомлены о своей обязанности сообщать, об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.34. В случае кражи переносного компьютера следует незамедлительно сообщить заместителю директора по информатизации и/или администрации МАОУ СОШ № 19.

6.35. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать заместителя директора по информатизации и/или инженера обслуживающим компьютерную технику и периферию образовательной организации;
- не пользоваться и не выключать зараженный компьютер;
- не подключать этот компьютер к сети образовательной организации до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование заметстителем директора по информатизации и/или инженером по ИТ.

Сотрудникам образовательной организации запрещается:

- нарушать информационную безопасность и работу сети образовательной организации;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников образовательной организации посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.36. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит непосредственно на пользователях, работающих на данных ПК.

6.37. Сотрудникам необходимо регулярно делать резервные копии всех основных служебных данных.

6.38. Только заместитель директора и/или инженер, обслуживающим компьютерную технику и периферию образовательной организации на основании заявок администрации, руководителей ШМО может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6.39. Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.40. Все заявки на проведение технического обслуживания компьютеров должны направляться заместителю директора по информатизации и/или инженеру, обслуживающим компьютерную технику и периферию образовательной организации, посредством записи в журнале заявок.

6.41. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с заместителем директора по информатизации.

7. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

7.1. Управление ИБ образовательной организации включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности.

8. РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Реализация Политики информационной безопасности МАОУ СОШ № 19 осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в образовательной организации.

9. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Внесение изменений и дополнений в Политику информационной безопасности МАОУ СОШ № 19 производится не реже одного раза в год с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации и изменениями в нормативно-правовой и законодательной базе.

10. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности МАОУ СОШ № 19 возлагается на сотрудника, назначенного приказом образовательной организации.

10.2. Директор МАОУ СОШ № 19 на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.

Приложение 1. КАТЕГОРИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДн

Выделим следующие категории пользователей, участвующих в обработке ПДн в ИСПДн в МАОУ СОШ № 19:

- Ответственный за ИСПДн;
- Администратор безопасности ИСПДн;
- Оператор ИСПДн;
- Инженер ИСПДн;
- Программист-разработчик информационной системы персональных данных;

Ответственный за ИСПДн

Сотрудник МАОУ СОШ № 19, 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.

Администратор 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

Сотрудник МАОУ СОШ № 19, 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

Сотрудник МАОУ СОШ № 19, 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

Инженер ИСПДн

Сотрудник МАОУ СОШ № 19, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Инженер ИСПДн не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Инженер ИСПДн:

- 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.
- 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 МАОУ СОШ № 19, 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 МАОУ СОШ № 19. Данные о категориях пользователей, уровне их доступа к объектам ИСПДн и информированности должны отражены в приказе по МАОУ СОШ № 19.

Приложение 2. ОРГАНИЗАЦИЯ И СОСТАВ СИСТЕМЫ ЗАЩИТЫ ПДн

Организация системы защиты ПДн

Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн МАОУ СОШ № 19, 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 МАОУ СОШ № 19. Для существующих ИСПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

В Политике информационной безопасности должны быть отражены меры по обеспечению безопасности ПДн, которые могут быть включены в СЗПДн МАОУ СОШ № 19. СЗПДн строится на основании следующих документов:

- актов обследования ИСПДн МАОУ СОШ № 19;
- перечня ПДн МАОУ СОШ № 19 подлежащих защите;
- перечня ИСПДн МАОУ СОШ № 19;
- порядка определения уровня защищенности ПДН в ИСПДн;
- модели угроз безопасности ПДн в ИСПДн;
- положении о разграничении прав доступа сотрудников к ПДн МАОУ СОШ № 19.

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 МАОУ СОШ № 19 или Администратором безопасности ИСПДн.

Состав системы защиты ПДн

Система защиты ПДн МАОУ СОШ № 19 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 МАОУ СОШ № 19, 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 МАОУ СОШ № 19. 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. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн МАОУ СОШ № 19 при ее передаче по каналам связи сетей общего пользования. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

Приложение 3. ПРОВЕДНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ И ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

Проведение работ по созданию системы защиты ПДн

Проведение работ по созданию (модернизации) СЗПДн МАОУ СОШ № 19 предполагает реализацию следующих стадий:

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

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

- Определение требуемого уровня защищенности 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 также соответствующих ведомственных методических рекомендациях;
- Перечень актуальных угроз формируется для каждой ИСПДн МАОУ СОШ № 19 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 защищенности 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.);
- изменения в нормативно-правовой и законодательной базе касаемо работы с ПДн.

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 в МАОУ СОШ № 19 осуществляется в соответствии с концепцией информационной безопасности ИСПДн.

Работы по приведению деятельности МАОУ СОШ № 19 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 МАОУ СОШ № 19.

Проведение работ возлагается на специально создаваемую для этих целей комиссию и/или ответственных работников. В случаях, когда МАОУ СОШ № 19 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 МАОУ СОШ № 19 по каждому из направлений.

При обработке ПДн без использования средств автоматизации:

- должен быть определен перечень лиц, осуществляющих неавтоматизированную обработку ПДн в МАОУ СОШ № 19;
- должно проводиться информирование работников МАОУ СОШ № 19 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, при таковой необходимости, 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 сотруднику МАОУ СОШ № 19 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 МАОУ СОШ № 19;
- 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 в МАОУ СОШ № 19), 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 или администрации МАОУ СОШ № 19;
- в случае достижения цели обработки ПДн МАОУ СОШ № 19 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 общего пользования 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.