СОГЛАСОВАНО

Председатель профсоюзного комитета

МОУ «Общеобразовательный лицей № 17»

протокол № 7 от 20 октября 2011 года

_____/Барашнина Г.В/

УТВЕРЖДАЮ

Директор МОУ

«Общеобразовательный лицей № 17»

приказ №436 от 21 октября 2011 года

_____/Сахарова И.С./

П О Л О Ж Е Н И Е
по организации защиты персональных данных в МОУ «Общеобразовательный лицей № 17»

1. Общие положения

1.1. Настоящее Положение по организации защиты персональных данных в МОУ «Общеобразовательный лицей № 17» (далее – Положение) разработано в целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. В соответствии с действующим законодательством персональные данные являются конфиденциальной информацией.

1.3. Настоящее Положение определяет перечень работ и порядок проведения организационных мероприятий и технических мер (далее – мероприятий) по защите персональных данных работников МОУ «Общеобразовательный лицей № 17» (далее – Учреждение) и граждан от несанкционированного доступа, неправомерного использования или утраты.

К мероприятиям по защите персональных данных относятся организационные и технические мероприятия, проводимые в соответствии с требованиями нормативных документов федеральных органов, уполномоченных в области обеспечения безопасности: Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности России (ФСБ).

Мероприятия по защите персональных данных в Учреждении могут проводиться на договорной основе сторонними организациями при наличии у исполнителя действующих лицензий ФСТЭК и ФСБ России.

1.4. Общее руководство деятельностью Учреждения по работе с персональными данными осуществляет директор.

1.5. Организационную структуру системы защиты персональных данных Учреждения образуют:

- техническая комиссия при Учреждении, созданная приказом директора Учреждения – в части координации работ по защите персональных данных и принятия коллегиальных решений по вопросам обеспечения безопасности информации;
- специалисты Учреждения, ответственные за обеспечение безопасности персональных данных и проведение мероприятий по их защите – в части реализаций мер технической защиты информации в Учреждении.

1.6. Финансирование мероприятий по технической защите персональных данных предусматривается в смете Учреждения.

1.7. Требования настоящего Положения являются обязательными для исполнения всеми работниками Учреждения, организующими обработку персональных данных (ПДн) и участвующих в ее обработке.

2. Организационные мероприятия по защите персональных данных

2.1. Директор Учреждения утверждает своим приказом списки работников, доступ которых к персональным данным необходим для выполнения своих служебных (функциональных) обязанностей.

Изменения и дополнения, вносимые в список лиц, осуществляющих обработку персональных данных, также утверждаются директором.

2.2. Выполнение работ с персональными данными включается в функциональные обязанности работника. В должностную инструкцию работника включается также его обязанность по защите персональных данных.

2.3. Директор Учреждения при необходимости и в зависимости от объемов работ назначает своим приказом работников, ответственных за обеспечение безопасности персональных данных и проведение мероприятий по их защите в информационных системах персональных данных, как правило, из числа специалистов, обеспечивающих информационное сопровождение и техническое обеспечение ПЭВМ Учреждения.

2.4. Все работники, участвующие в обработке персональных данных, должны быть ознакомлены под роспись с нормативными документами Учреждения, определяющими требования по защите информации.

2.5. Учреждение как организация, наделенная правами юридического лица, в случае обработки персональных данных граждан направляет, в установленных федеральным законом случаях, уведомление об обработке персональных данных в территориальное подразделение Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций России – Управление Россвязькомнадзора по Архангельской области и Ненецкому автономному округу для внесения в реестр операторов персональных данных.

2.6. Специалисты, ответственные за информационное обеспечение представляют директору Учреждения перечни информационных баз персональных данных.

Перечень информационных баз должен содержать следующие сведения:

- цель обработки персональных данных и основание для сбора информации, с указанием законодательных и нормативных документов, определяющих необходимость выполнения работ;
- перечень обрабатываемых персональных данных;
- перечень действий с персональными данными (обработка, использование, распространение и другие), общее описание используемых в структурном подразделении способов обработки персональных данных.

2.7. Работники Учреждения, ответственные за обеспечение безопасности информации, с целью минимизации затрат на защиту, рассматривают возможность обезличивания информационных баз, содержащих персональные данные, и определяют минимально необходимый перечень сведений, включаемых в базы данных.

2.8. Разрабатываемые и созданные в Учреждении информационные базы и банки данных регистрируются при необходимости в установленном порядке в Реестре информационных ресурсов Архангельской области.

3. Порядок обращения с документами, содержащими персональные данные

3.1. Порядок ведения личных дел работников, а также получение, хранение, комбинирование, передача и другое использование персональных данных, содержащихся в них, определены Порядком ведения личных дел работников Учреждения.

3.2. Порядок обращения с документами, содержащими персональные данные, с другими материальными (машинными) носителями конфиденциальной информации, а также обязанности и ответственность должностных лиц определены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

3.3. При обработке персональных данных должны соблюдаться следующие условия:

3.3.1. Учреждение при обработке персональных данных разрабатывает при необходимости инструкции, определяющие порядок работы, которые включают:

1) регламент взаимодействия с субъектами персональных данных;

2) регламент взаимодействия с уполномоченными органами;

3) регламент взаимодействия при передаче персональных данных сторонним организациям или третьим лицам.

3.3.2. Персональные данные при их обработке, должны обособляться от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

3.3.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, наименование структурного подразделения, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

2) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных.

3.3.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для регистрации обращений граждан или в иных аналогичных целях, должны соблюдаться следующие условия:

1) необходимость ведения такого журнала (реестра, книги) должна быть утверждена директором Учреждения, в котором отражаются сведения о цели обработки персональных данных, способы фиксации и состав информации, запрашиваемой у граждан, сроки обработки персональных данных;

2) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается.

3.3.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.3.6. В случае отсутствия типовых форм документов, в которые включаются персональные данные, исполнители работ обязаны получить от гражданина согласие на обработку его персональных данных в письменной форме согласно приложению № 2.

4. Порядок работ по обследованию информационной системы персональных данных

4.1. Специалистом информационного обеспечения проводится обследование информационных систем персональных данных (ИСПДн) Учреждения в части анализа информационных ресурсов персональных данных. Результаты работ отражаются в акте обследования, содержащем следующие сведения:

- перечень всех ИСПДн, существующих в составе локальной сети Учреждения;
- состав и структура каждой ИСПДн и технических особенностей их построения (состав и структура программного обеспечения, топология);
- перечень персональных данных, подлежащих защите, и местонахождение информационных систем персональных данных;
- категория персональных данных, включающая определение объемов информации с персональными данными – количество записей (документов), таблиц;
- режим обработки персональных данных в локальной сети и в отдельных компонентах.

4.2. Специалистом информационного обеспечения, или назначенным администратором безопасности проводится анализ уязвимых звеньев, возможных угроз безопасности персональных данных в соответствии с ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»:

- определение границ контролируемой зоны;
- оценка возможности физического доступа к ИСПДн;
- выявление возможных каналов утечки информации, в т.ч. технических;
- анализ возможностей программно-математического воздействия на ИСПДн;
- анализ возможностей электромагнитного воздействия на ИСПДн.

В здании Учреждения границей контролируемой зоны, как правило, являются несущие конструктивные строительные элементы помещения (стены).

5. Классификация информационной системы персональных данных

5.1. Классификация информационной системы персональных данных (ИСПДн) проводится с соответствии с пунктом 6 Постановления Правительства РФ от 17.11.2007 № 781 в целях разработки обоснованных мер по достижению требуемого уровня защиты информации.

Классификация информационной системы персональных данных проводится в порядке, определенном приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

5.2. Для проведения классификации информационной системы специалистом информационного обеспечения подготавливаются следующие документы:

1) акт обследования информационной системы персональных данных, подлежащей классификации;

2) технические паспорта или формуляры каждой информационной системы персональных данных в соответствии с РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;

3) перечень реквизитов информационной системы, содержащей персональные данные.

5.3. В зависимости от применяемой технологической схемы обработки персональных данных путем организации удаленного доступа, при котором вся информация обрабатывается и хранится на сервере, все ПЭВМ, участвующие в обработке ПДн,

классифицируются как типовые информационные системы, а сервера классифицируются как специальные ИСПДн.

В случае выявления в локальной вычислительной сети ПЭВМ, обрабатывающих различные категории и объемы персональных данных, необходимо выделить их в разные подсистемы обработки персональных данных.

Наиболее высокий класс ПЭВМ в составе локальной вычислительной сети распространяется на всю сеть или ее сегмент (подсистему) обработки персональных данных.

5.4. В исключительных случаях обработки и хранения персональных данных на отдельной ПЭВМ, такая ИСПДн классифицируется как специальная. В отличие от типовых ИСПДн, для которых существует перечень заданных требований, требования к специальным ИСПДн формируются исходя из модели угроз безопасности.

5.5. Класс защищенности специальной информационной системы персональных данных определяется следующим порядком:

1) на основании категории обрабатываемых в информационной системе персональных данных и их объема определяется класс типовой информационной системы (типовые К4÷К1);

2) на основании частной модели угроз ИСПДн определяются дополнительные угрозы безопасности персональных данных.

Допускаются следующие варианты определения класса защищенности ИСПДн: К4, К3, специальная К3, специальная К2, где индекс специальной ИСПДн указывает на наиболее близкий типовой класс защищенности.

5.6. Специалистом информационного обеспечения, или назначенным администратором безопасности на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации», утвержденного решением Председателя Гостехкомиссии России от 30.03.1992, дополнительно определяется класс защищенности информационной системы персональных данных как системы, содержащей конфиденциальную информацию.

5.7. Специалистом информационного обеспечения, или назначенным администратором безопасности готовится проект акта классификации информационной системы персональных данных. Проект акта классификации, а также документы, созданные при подготовке информационных систем персональных данных к проведению оценки соответствия требованиям безопасности, рассматриваются на заседании технической комиссии. Акт классификации утверждается директором Учреждения.

Допускается определение одним актом класса защищенности ИСПДн, выполняющих единую задачу по обработке персональных данных и имеющих одинаковый состав технических средств и программного обеспечения.

5.8. Пересмотр класса информационной системы персональных данных проводится в случаях:

- изменения состава персональных данных, обрабатываемых на ПЭВМ, или значительного изменения (свыше 1000) количества субъектов персональных данных;
- изменения состава или структуры ИСПДн или технологии обработки персональных данных;
- окончания срока действия декларации соответствия или аттестата соответствия требованиям безопасности информации, выданного на ИСПДн;
- выявления в ходе проверки уполномоченным контролирующим органом несоответствия класса ИСПДн условиям эксплуатации, обработки информации и объемам персональных данных.

6. Организационно-технические мероприятия по защите персональных данных

6.1. Специалистом информационного обеспечения или назначенным администратором безопасности в целях обоснования требований по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, проводится:

- разработка частной модели угроз безопасности персональных данных;
- оценка актуальных угроз безопасности персональных данных;
- уточнение класса ИСПДн (классификация рассматривается в разделе 5).

Частная модель угроз безопасности определяет актуальность угроз безопасности персональных данных и рекомендуемый перечень мер защиты информации. Конкретные меры защиты персональных данных определяются на основании перечня из условий эксплуатации ИСПДн и степени возможного ущерба.

Частная модель угроз безопасности персональных данных должна разрабатываться для каждой ИСПДн.

6.2. В случае необходимости обеспечения безопасности персональных данных с использованием криптосредств (шифрования) дополнительно проводится:

- доработка частной модели угроз персональных данных с учетом использования криптосредств;
- определение требуемого уровня криптографической защиты ПДн;
- определение требуемого уровня специальной защиты от утечки по каналам побочных излучений и наводок при защите ПДн с использованием криптосредств.

6.3. Модель угроз безопасности разрабатываются специалистом информационного обеспечения или назначенным администратором безопасности на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России от 15.02.2008, и «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных ФСБ России от 21.02.2008 № 149/54–144.

Разрабатываемые документы должны учитывать методические рекомендации как ФСТЭК, так и ФСБ России, а при оценке угроз для ИСПДн из однотипных угроз выбирается более опасная.

6.4. В целях проектирования системы защиты персональных данных специалистом информационного обеспечения или назначенным администратором безопасности на основании класса защищенности ИСПДн проводится анализ имеющихся в распоряжении мер и предлагаемых отечественным рынком средств защиты персональных данных для разработки частного технического задания на систему защиты или подготовки протокола экспертной оценки возможности применения мер и средств защиты:

- от физического доступа;
- от несанкционированного доступа;
- от программно-математического воздействия;
- от утечки по техническим каналам;
- от электромагнитных воздействий.

6.5. В случае применения в ИСПДн криптосредств для защиты персональных данных дополнительно учитываются «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных ФСБ России от 21.02.2008 № 149/6/6–622.

6.6. Проведение работ по организации обеспечения безопасности ПДн при их обработке в ИСПДн включает:

- разработку требований к системе защиты персональных данных (СЗПДн), а также формулирование задач по защите ПДн (разработка перечня мероприятий по защите персональных данных в соответствии с выбранным классом);
- выбор способов, мер и средств защиты ПДн в соответствии с мероприятиями по защите;
- разработку при необходимости технического задания (ТЗ) на СЗПДн;
- разработку отсутствующих документов, регламентирующих вопросы организации обеспечения безопасности персональных данных и эксплуатации СЗПДн информационной системы.

6.7. Основные обязательные требования к организации системы защиты информации в зависимости от класса типовой ИСПДн:

Для ИСПДн 4 класса:

- перечень мероприятий по защите персональных данных определяется Учреждением (в зависимости от возможного ущерба).

Для ИСПДн 3 класса:

- декларирование соответствия или аттестация по требованиям безопасности информации.

Для ИСПДн 2 класса:

- обязательная аттестация по требованиям безопасности информации.

Для ИСПДн 1 класса:

- обязательная аттестация по требованиям безопасности информации;
- должны быть реализованы мероприятия по защите персональных данных от побочных излучений и наводок.

6.8. Специалистом информационного обеспечения или назначенным администратором безопасности на основе ГОСТ Р 51898-2002, ГОСТ Р ИСО/МЭК ТО 13335-2007 (все части) организуется процесс анализа риска как части программы обеспечения информационной безопасности для оценки состояния безопасности Учреждения, а также безопасности конкретных систем и информационных баз.

Результаты процесса оценки риска, а также предложения по снижению рисков безопасности Учреждения до приемлемого уровня представляются технической комиссии для выработки рекомендаций директору Учреждения. Эти рекомендации определяют выбор соответствующих защитных мер, которые являются результатом оценки и определения величины возможных потерь, которые могут произойти в случае, если идентифицированные уязвимости системы будут использованы одной или более угрозами.

К активам Учреждения, которые подвергаются оценке риска, относятся: аппаратура и оборудование, прикладные программы, базы данных Учреждения, системы связи и компьютерные операционные системы.

6.9. Учреждение организует обучение специалистов в области защиты персональных данных, а специалист информационного обеспечения осуществляет первичный инструктаж пользователей.

6.10. Повышение квалификации специалистов Учреждения по технической защите конфиденциальной информации, а также совершенствование знаний руководителей Учреждения в области технической защиты информации ограниченного доступа организуются на базе учебных заведений, осуществляющих подготовку, переподготовку и повышение квалификации специалистов в области защиты информации.

6.11. Технические мероприятия по защите персональных данных определяются нормативными документами и включают:

1) внедрение системы защиты персональных данных;
2) выполнение требований по инженерной защите помещений;
3) выполнение требований по пожарной безопасности и охране;
4) выполнение требований по электропитанию и заземлению;
5) выполнение санитарных и экологических требований;
6) ввод в опытную эксплуатацию системы защиты в информационной системе;
7) проведение специальных исследований по оценке защищенности информационной системы персональных данных 1 класса от утечки по каналам побочных излучений и наводок;
8) доработку системы защиты по результатам опытной эксплуатации.

7. Лицензирование работ по защите персональных данных

7.1. В соответствии с нормативными документами ФСТЭК России в области персональных данных в Учреждении проводится работа по получению лицензии Федеральной службы по техническому и экспортному контролю России на право проведения работ по технической защите конфиденциальной информации или передача функций защиты персональных данных третьему (уполномоченному) лицу (аутсорсинг) – организации, имеющей предоставленную в установленном порядке лицензию.

7.2. Работа по лицензированию деятельности проводится в соответствии с Федеральным законом РФ от 08.08.2001 № 128–ФЗ. Порядок получения лицензии и требования, предъявляемые к лицензиату, установлены Постановлением Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

7.3. Получение лицензии Федеральной службы безопасности России, в соответствии с Постановлением Правительства РФ от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», не требуется в случае применения шифровальных (криптографических) средств, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей, не относящихся к критически важным объектам [1].

8. Аттестация информационной системы персональных данных

8.1. В соответствии с нормативными документами ФСТЭК России в области персональных данных информационные системы персональных данных, классифицированные по классу К1, К2, подлежат обязательной аттестации по требованиям безопасности персональных данных.

8.2. В случае установления для информационных систем персональных данных класса защищенности К3 организует аттестацию или декларирование соответствия требованиям безопасности информации.

---

[1] «критически важные объекты» - объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени. (Распоряжение Правительства РФ от 27.08.2005 № 1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов»)

8.3. Оценка соответствия требованиям по обеспечению безопасности информационных систем персональных данных, которым установлен класс защищенности К4, определяется Учреждением самостоятельно, с учетом руководящих документов ФСТЭК и ФСБ России.

8.4. Декларирование соответствия требованиям безопасности информации включает самостоятельное проведение Учреждением всех организационных и технических мероприятий по испытаниям информационных систем персональных данных в соответствии с техническим регламентом, утвержденным Президентом или Правительством Российской Федерации.

8.5. В зависимости от специфики обработки персональных данных, организационной структуры Учреждения и других особенностей разрабатываются организационно-распорядительные документы в области защиты персональных данных.

8.6. Работы по аттестации информационных систем персональных данных проводятся в Учреждении сторонними организациями на договорной основе при аккредитации ФСТЭК исполнителя работ в качестве органа по аттестации по требованиям безопасности конфиденциальной информации.

9. Контроль выполнения требований безопасности персональных данных

9.1. Контроль выполнения требований безопасности персональных данных (далее - контроль) осуществляется в целях оценки организации технической защиты персональных данных, своевременного выявления и предотвращения утечки персональных данных по техническим каналам, несанкционированного доступа к ним, оценки защиты их от технических разведок.

Контроль заключается в проверке выполнения требований федеральных законов, нормативно-методических и руководящих документов по технической защите персональных данных Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации, а также в оценке достаточности принимаемых мер по технической защите персональных данных.

9.2. Основными задачами контроля являются:

- оценка деятельности специалистов Учреждения в области технической защиты персональных данных в пределах их компетенции;
- выявление технических каналов утечки информации ограниченного доступа на объектах информатизации, каналов несанкционированного доступа к персональным данным и специальных воздействий на них, анализ и инструментальная оценка возможностей технических разведок по получению персональных данных;
- оценка эффективности проводимых мер по технической защите персональных данных;
- выявление и анализ нарушений установленных федеральным законодательством норм и требований, нормативно-методических и руководящих документов по технической защите персональных данных ФСТЭК и ФСБ России и принятие оперативных мер по пресечению выявленных нарушений;
- разработка рекомендаций по устранению выявленных недостатков в организации и состоянии работ по технической защите персональных данных;
- проверка устранения недостатков, выявленных в результате контроля.

9.3. Контроль в Учреждении (порядок функционирования средств технической защиты информации, соблюдение установленных режимов работы объектов информатизации, выполнение установленных мер по технической защите персональных данных, в том числе от несанкционированного доступа) осуществляется специалистом информационного обеспечения или назначенным администратором безопасности в соответствии с планом проверок, ежегодно утверждаемым директором Учреждения.

Контроль также может проводиться на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

9.4. Внеплановые проверки проводятся при поступлении в Учреждение обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

- о возникновении угрозы причинения вреда жизни, здоровью граждан;
- о причинении вреда жизни, здоровью граждан;
- о нарушении прав и законных интересов граждан действиями (бездействием) при обработке их персональных данных;
- о нарушении требований Федерального закона № 152-ФЗ «О персональных данных» и иных нормативных правовых актов в области персональных данных.

9.5. Материалы по выявленным недостаткам и нарушениям, а также мероприятия по их устранению и проекты соответствующих приказов подготавливаются специалистом информационного обеспечения или назначенным администратором безопасности и представляются в установленном порядке директору Учреждения.

9.6. По итогам года специалист информационного обеспечения или назначенный администратор безопасности составляет отчет по результатам проведенных мероприятий по защите персональных данных, состоянию системы защиты персональных данных в Учреждении, включающий предложения по повышению эффективности защиты информации. Отчет рассматривается на заседании технической комиссии и представляется директору Учреждения для рассмотрения и утверждения.