МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 1»

П Р И К А З

23.06. 2017 г. 480 -О

Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе и в информационных системах в 2017-2018 учебном году

Во исполнение федеральных законов от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Порядок организации работы по обеспечению безопасности персональных данных (далее-ПДн) при их обработке, в том числе и в информационных системах согласно приложению 1 к настоящему приказу.

1.2. Перечень лиц, имеющих в 2017-2018 учебном году доступ к персональным данным при выполнения трудовых обязанностей, в том числе с использованием информационных систем согласно приложению 2 к настоящему приказу.

1.3. Перечень лиц, ведущих обработку персональных данных без использования средств автоматизации либо имеющих к ним доступ согласно приложению 3 к настоящему приказу.

1.4. Перечень информационных систем персональных данных согласно приложению 4 к настоящему приказу.

1.5. Перечень персональных данных, обрабатываемых в муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа№1» Перечень обрабатываемых персональных данных согласно приложению 5 к настоящему приказу.

2. Назначить лиц, ответственных в муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа №1» за:

- организацию обработки персональных данных Храпунову Т.Г.,

заместителя директора по учебной работе МАОУ СОШ №1;

- информатизацию МАОУ СОШ №1 Галкину Л.А., заместителя директора по административно-хозяйственной части);

- реализацию мероприятий по защите информации и обеспечение безопасности персональных данных при их обработке, в том числе и в информационных системах Игумнова Э.В., лаборанта.

3. Назначить администратором безопасности информации Бардачеву Т.Н., учителя физики и математики.

4. Утвердить типовые функции и задачи:

4.1. Работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа №1» согласно приложению 6 к настоящему приказу.

4.2. Специалиста, ответственного за реализацию мероприятий по защите информации в муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа №1» согласно приложению 7 к настоящему приказу.

4.3. Администратора безопасности информации в муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа №1» согласно приложению 8 к настоящему приказу.

5. Ответственному за информатизацию МОАУ СОШ №1 при формировании бюджета школы учитывать затраты на обеспечение безопасности функционирования информационных систем персональных данных (далее – ИСПДн), в части приобретения сертифицированных технических средств защиты информации и планирования выполнения мероприятий по обязательной аттестации ИСПДн по требованиям безопасности информации.

6. Контроль за исполнением приказа оставляю за собой.

Директор МАОУ СОШ №1 **В.Г. Дихтенко**

Приложение 1
к приказу МАОУ СОШ №1
от «23» 06 2017 № 480-0

Порядок организации работы по обеспечению безопасности персональных данных при их обработке, в том числе и в информационных системах

1. Общие положения

1.1. Настоящий Порядок организации работы по обеспечению безопасности персональных данных при их обработке, в том числе и в информационных системах (далее – Порядок) разработан с целью организации и проведения работ по вопросам обеспечения безопасности информации в информационных системах и защиты ПДн в соответствии с требованиями нормативных правовых актов Российской Федерации в области информационной безопасности.

1.2. Порядок разработан с учетом требований следующих нормативных правовых актов Российской Федерации и методических документов, действующих в области обеспечения безопасности информации:

- федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства Российской Федерации № 1119);
- постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее – Постановление Правительства Российской Федерации № 211);
- приказ ФСБ России от 10.07.2014 № 378 «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК России № 21);

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ ФСТЭК России № 17);

- приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;

- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 02 2014;

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

1.3. Муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа №1» является оператором при обработке ПДн.

Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

1.4. Должностные лица, осуществляющие обработку ПДн несут гражданско-правовую, уголовную, административную, дисциплинарную и материальную ответственность за нарушение правил обращения с ПДн, предусмотренную следующими статьями:

а) Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ:

- статьей 5.39 «Отказ в предоставлении информации»;

- статьей 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (ПДн)»;

- статьей 13.12 «Нарушение правил защиты информации»;

- статьей 13.13 «Незаконная деятельность в области защиты информации»;

- статьей 13.14 «Разглашение информации с ограниченным доступом».

б) Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ:

- статьей 137 «Нарушение неприкосновенности частной жизни»;

- статьей 140 «Отказ в предоставлении гражданину информации»;

- статьей 272 «Неправомерный доступ к компьютерной информации»;

- статьей 274 «Нарушение правил эксплуатации средств хранения,

обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

в) Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ:

- статьей 81 «Расторжение трудового договора по инициативе работодателя»;

- статьей 90 «Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника».

1.5. Действие Порядка не распространяется на отношения, возникающие при обработке информации, отнесенной в установленном порядке к сведениям, составляющим государственную тайну.

1.6. В целях обеспечения безопасности ПДн при их обработке в ИС, в том числе и МИС, а также для защиты ПДн назначаются ответственные лица за организацию обработки ПДн и обеспечение безопасности.

1.7. Решение о назначении ответственных лиц оформляется соответствующим приказом директора МАОУ СОШ №1.

1.8. Установить сроки реализации мероприятий по обеспечению безопасности ПДн при их обработке в МИС.

1.9. Ответственный за организацию обработки ПДн, получает указания непосредственно от директора МАОУ СОШ №1, и подотчетный ему.

1.10. На ответственного за организацию обработки ПДн возлагается:

- осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

- доведение до сведения работников оператора положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

- организация приема и обработки обращений и запросов субъектов ПДн или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

1.11. Директор МАОУ СОШ №1 обеспечивает периодическое обучение на специализированных курсах повышения квалификации по вопросам защиты информации ограниченного доступа лиц, участвующих в обработке персональных данных.

1.12. Лица, ответственные за организацию обработки ПДн, должны обладать следующей актуальной информацией в отношении каждой ИС, в которой обрабатываются ПДн:

- цель обработки ПДн;

- категории ПДн;

- категории субъектов ПДн, информация о которых обрабатываются в ИС;

- правовое основание обработки ПДн;

- перечень действий с ПДн, общее описание используемых способов обработки ПДн;

- описание мер, обеспечения безопасности ПДн, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих

средств;

- дата начала обработки ПДн;

- срок или условие прекращения обработки ПДн;

- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки.

1.13. Ответственный за организацию обработки ПДн:

- обеспечивает разработку и поддержание в актуальном состоянии локальных актов МАОУ СОШ №1, регламентирующих организацию обработки ПДн в школе;

- осуществляет контроль за полнотой и эффективностью принятых мер обеспечения безопасности ПДн в школе, а также периодически проверяет условия обработки ПДн в МАОУСОШ №1.

- знакомит лиц, непосредственно осуществляющих обработку ПДн, с положениями действующего законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн;

- организует использование СЗИ, предназначенных для обеспечения безопасности ПДн при их обработке в ИСПДн, в обязательном порядке сертифицированных ФСТЭК России и ФСБ России (для криптографических средств защиты информации). Признаком сертифицированного СЗИ является наличие специального защитного знака, наносимого непосредственно на технические средства защиты, а также на магнитные или оптические носители с дистрибутивами программных средств защиты. Контроль маркирования СЗИ специальными защитными знаками осуществляют испытательные лаборатории, производившие сертификационные испытания данных средств защиты. В комплект поставки СЗИ должны входить формуляр, правила пользования этими средствами (инструкции по установке и настройке, инструкции администратору и пользователю).

1.14. СЗИ, предназначенные для обеспечения безопасности ПДн при их обработке в информационных системах, эксплуатационная и техническая документация к ним подлежат учету в журналах поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним, в которых отражается:

- индексы и наименования СЗИ;

- серийные (заводские) номера;

- номера специальных защитных знаков;

- номера и сроки действия сертификатов на СЗИ;

- место установки СЗИ;

- наименование и номера эксплуатационной и технической документации к средства защиты.

Журнал в установленном порядке регистрируется в делопроизводстве.

Перед вводом в эксплуатацию СЗИ ответственным за организацию обработки ПДн проводится оценка готовности данных средств к использованию с составлением заключений о возможности их эксплуатации, утверждаемых руководителем ОМУ.

1.15. С целью обеспечения возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД в МАОУ СОШ №1 организовано резервирование обрабатываемых ПДн. Периодичность и порядок проведения резервирования и восстановления ПДн определяется локальным актом школы.

При этом, необходимо учитывать объем обновляемых ПДн, а также возможный ущерб от нарушения функционирования конкретной информационной системы.

1.16. Все магнитные, оптические и другие машинные носители ПДн подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет. Машинные носители информации, в том числе с резервными копиями ПДн, регистрируются в журнале учета магнитные, оптические и другие машинные носителей информации.

Журнал в установленном порядке регистрируется в делопроизводстве.

1.17. Уничтожение информации с бумажных и магнитных носителей информации осуществляется средствами гарантированного уничтожения информации.

1.18. Обработка ПДн в МАОУ СОШ №1 может вестись и без использования средств автоматизации.

1.19. Условия хранения ПДн должны обеспечивать сохранность персональных данных и исключать НСД к ним доступ.

2. Мероприятия по обеспечению безопасности ПДн при их обработке в том числе и в случае их автоматизированной обработки

2.1. Защита ПДн при их обработке в МИС ПДн обеспечивается путем выполнения требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

2.2. Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

- установку и настройку средств защиты информации в информационной системе в соответствии с эксплуатационной документацией на них;
- разработку документов, определяющих правила и процедуры для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;
- управление системой защиты информации информационной системы;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее – инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты информации информационной системы;

- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

- защиту информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;

- внедрение организационных мер защиты информации.

2.3. Оценка эффективности реализованных в рамках системы защиты ПДн мер проводится с привлечением организаций-лицензиатов не реже одного раза в 3 года. Дополнительная проверка эффективности системы защиты МИС ПДн осуществляется в случае изменения условий и технологии обработки ПДн в МАОУ СОШ №1.

Организация-лицензиат, проводившая аттестационные испытания, несет ответственность за полноту и качество выполненных работ, а также за сохранность полученных в ходе испытаний сведений ограниченного доступа.

2.4. Аттестация информационной системы включает в себя проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы требованиям безопасности информации.

В общем виде аттестация информационной системы по требованиям безопасности информации включает в себя следующие этапы:

- анализ исходных данных по аттестуемой информационной системе;

- предварительное ознакомление с аттестуемой информационной системой;

- проведение экспертного обследования информационной системы и анализ разработанной документации по обеспечению безопасности ПДн на соответствие требованиям нормативных и методических документов;

- проведение комплексных аттестационных испытаний информационной системы в реальных условиях эксплуатации с использованием специальной аппаратуры контроля и программных средств контроля защищенности от несанкционированного доступа;

- анализ результатов комплексных аттестационных испытаний, оформление и утверждение заключения по результатам аттестации.

2.5. МАОУ СОШ №1 несет ответственность за выполнение установленных условий функционирования МИС ПДн, технологии обработки ПДн и требований по обеспечению их безопасности.

Обеспечение защиты информации в ходе эксплуатации информационной системы осуществляется в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации.

2.6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации включает в себя:

- архивирование информации, содержащейся в информационной системе;

- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Архивирование информации, содержащейся в информационной системе, осуществляется при необходимости дальнейшего использования информации в

деятельности оператора.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.