МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 6»

ПРИКАЗ

10.07.2017 № 369

Об утверждении локальных актов по защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 г. 152 ФЗ «О Персональных данных» и Постановлением правительства Российской Федерации от 17.11.2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», с целью организации работ по соблюдению требований законодательства в сфере защиты персональных данных, приказываю:

1. Утвердить Положение о порядке обработки и обеспечения безопасности персональных данных (конфиденциальной информации) в автоматизированной системе «АРМ-К СОШ № 6» МБОУ «СОШ № 6» (Приложение № 1).
2. Утвердить Политику информационной безопасности МБОУ «СОШ № 6» (Приложение № 2).
3. Утвердить Политику по работе с инцидентами информационной безопасности МБОУ «СОШ № 6» (Приложение № 3).
4. Утвердить «Положение о разрешительной системе доступа в МБОУ «СОШ № 6». Матрица доступа к защищаемым ресурсам в автоматизированной системе «АРМ-К СОШ №6» Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» (Приложение № 4).
5. Утвердить Инструкцию пользователя автоматизированной системы «АРМ-К СОШ № 6» МБОУ «СОШ № 6» (Приложение № 5).
6. Утвердить Инструкцию по эксплуатации средств антивирусной защиты информационных средств, производящих обработку персональных данных (конфиденциальной информации) в МБОУ «СОШ № 6» (Приложение № 6).
7. Утвердить Инструкцию по уничтожению персональных данных (конфиденциальной информации) в МБОУ «СОШ № 6» (Приложение № 7).
8. Утвердить Инструкцию по работе с электронной подписью в МБОУ «СОШ № 6» (Приложение № 8).
9. Утвердить Инструкцию по защите от несанкционированного доступа к персональным данным (конфиденциальной информации) в МБОУ «СОШ № 6» (Приложение № 9).
10. Утвердить Инструкцию по защите персональных данных (конфиденциальной информации) в МБОУ «СОШ № 6» (Приложение № 10).

11. Утвердить форму листа согласия субъекта на обработку его персональных данных и данных его ребёнка/воспитанника, обучающегося в МБОУ СОШ № 6 (Приложение № 11).

12. Утвердить форму листа согласия на обработку персональных данных работника МБОУ СОШ № 6 (Приложение № 12).

13. Чирковой Е.В., ответственной за осуществление мероприятий по обработке персональных данных, ознакомить с локальными актами по защите персональных данных работников МБОУ «СОШ № 6»

14. Контроль за исполнением приказа возложить на Чиркову Е.В., заместителя директора по УВР.

Директор Т.Н.Барматина

Приложение № 1
к приказу от 10.07.2017 № 369

Положение о порядке обработки и обеспечения безопасности персональных данных (конфиденциальной информации) в автоматизированной системе «АРМ-К СОШ № 6» МБОУ «СОШ № 6»

1.Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных в Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» (далее - Учреждение).

1.2. В целях настоящего Положения используются следующие термины и понятия:

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;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1. Основные условия проведения обработки персональных данных

2.1. Обработка персональных данных осуществляется:

после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;

после принятия необходимых мер по защите персональных данных.

2.2. Приказом руководителя Учреждения назначается сотрудник, ответственный за защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные.

2.4. **Запрещается**:

обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

осуществлять ввод персональных данных под диктовку.

3. Порядок определения защищаемой информации

3.1. В Учреждении определяется и утверждается Перечень персональных данных и перечень информационных систем персональных данных, в которых осуществляется обработка персональных данных.

3.2. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных.

4. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

4.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации

осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» и иных нормативно правовых актов Российской Федерации.

4.2. Учреждением определяется уровень защищённости персональных данных согласно Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в зависимости от категории обрабатываемых данных, их количества и актуальных угроз.

4.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4.4. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт защищённости персональных данных в ИСПДн, инструкции пользователя по эксплуатации средств антивирусной защиты, и других нормативных и методических документов;
- настроенных от несанкционированного доступа средств защиты информации, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

5.

6. Порядок обработки персональных данных без использования средств автоматизации

6.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

6.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

6.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

6.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

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

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

6.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность

несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

6.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

6.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

6.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6.10. 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).

7. Ответственность должностных лиц

Сотрудники Учреждения и рабочий персонал, допущенные к обработке персональных данных, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к приказу от
10.07.2017 № 369

ПОЛИТИКА
информационной безопасности МБОУ «СОШ № 6»

1. Назначение и правовая основа политики информационной безопасности

1.1. Настоящая Политика информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» (далее – Учреждение) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.

1.2. Настоящая Политика является документом, доступным любому сотруднику Учреждения и пользователю его ресурсов, и представляет собой официально принятую руководством Учреждения систему взглядов на проблему обеспечения информационной безопасности.

1.3. Руководство Учреждения осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства, а также ожиданий преподавательского и рабочего состава Учреждения, обучающихся и их родителей и других заинтересованных сторон. Обеспечение информационной безопасности – необходимое условие для успешного осуществления образовательной деятельности Учреждения. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны преподавательского и рабочего состава Учреждения, обучающихся и их родителей.

1.4. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения безопасности защищаемой информации, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим средствам разведки и технической защиты информации, и основывается, в том числе, на:

- Доктрине информационной безопасности Российской Федерации (утвержденной Президентом Российской Федерации 09.09.2000 года № Пр-1895);
- Федеральном законе от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральном законе от 27.07.2006 года № 152-ФЗ «О

персональных данных».

• Федеральном законе от 06.04.2011 года № 63-ФЗ «Об электронной подписи».

1.5. Необходимые требования обеспечения информационной безопасности Учреждения должны неукоснительно соблюдаться сотрудниками и рабочим персоналом Учреждения и другими сторонами как это определяется положениями внутренних нормативных документов Учреждения, а также требованиями договоров и соглашений, стороной которых является Учреждение.

1.6. Настоящая Политика распространяется на процессы Учреждения и обязательна для применения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов.

2. Термины и определения

В настоящей Политике использованы термины с соответствующими определениями законодательства Российской Федерации и норм права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

2.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

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

2.3. **Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

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

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

2.6. **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.

2.7. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

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

2.9. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

2.11. **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.

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

2.13. **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

2.15. **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.16. **Режим обработки персональных данных** - организационно-технические мероприятия по защите персональных данных, позволяющие Оператору персональных данных при существующих или возможных обстоятельствах обеспечить целостность, доступность и конфиденциальность персональных данных, избежать неоправданных расходов, и реализующие меры по охране персональных данных, включающие в себя:

- определение перечня персональных данных в соответствии с целями и задачами обработки, требованиями Федерального закона от 27.07.2006 года №152 «О персональных данных»;
- ограничение доступа к персональным данным путем установления порядка обращения с ними и контроля за соблюдением такого

порядка;

- определение класса информационной системы, в которой осуществляется обработка персональных данных;
- учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию персональных данных работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.17. **Рисковое событие информационной безопасности** - это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Учреждения и произошедшее по причине ошибочности или сбоя процессов Учреждения, действий людей и систем, а также по причине внешних событий.

2.18. **Угроза информационной безопасности** - операционный риск, влияющий на нарушение одного (или нескольких) свойств информации - целостности, конфиденциальности, доступности.

2.19. **Уязвимость** – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

3. Цели и задачи, принципы обеспечения информационной безопасности

3.1 Целями деятельности по обеспечению информационной безопасности Учреждения являются:

- снижение угроз информационной безопасности до приемлемого для Учреждения уровня;
- защита персональных данных, обрабатываемых в информационной системе Учреждения; защита информационной системы от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- минимизация уровня рисков.

3.2 Основные задачи деятельности по обеспечению информационной безопасности Учреждения:

- отнесение информации к категории несекретной, ограниченного распространения, коммерческой и другим видам тайн, иной конфиденциальной информации, информации персонального характера подлежащей защите от неправомерного использования;
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Учреждения, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования Учреждения с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и

нанесения ущерба;

- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Учреждения, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного предотвращения и локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц.

3.3 Построение системы обеспечения безопасности информации Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- **законности** – соблюдение законодательства по защите информации, защите персональных данных и законных интересов всех участников информационного обмена;
- **системности** – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь категорирование обрабатываемой информации, информационной системы, оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Учреждения;
- **эффективности** – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к приемлемому уровню, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;
- **целесообразности** – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;
- **непрерывности** – принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;
- **взаимодействии и координации** – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи структурных подразделений Учреждения, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться подготовленными сотрудниками Учреждения;
- **совершенствовании** – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических

средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

- **приоритетности** – категорирование (ранжирование) информации и всех информационных ресурсов Учреждения по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;
- **информированности и персональной ответственности** – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационных сервисов индивидуально идентифицирующих и аутентифицирующих пользователей и инициируемые ими процессы;
- **обязательность контроля** – контроль за деятельностью пользователей, а также мониторинг работы информационной системы должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

4. Объекты информационной безопасности

4.1 Основными объектами защиты системы информационной безопасности в Учреждении являются:

- персональные данные, информационные ресурсы обрабатывающие персональные данные, сведения ограниченного распространения, независимо от формы и вида их представления;
- информационные ресурсы, содержащие персональные данные физических лиц;
- сотрудники Учреждения, являющиеся пользователями информационных ресурсов (систем) Учреждения;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационной системы Учреждения, с помощью которых производится обработка защищаемой информации;
- помещения, предназначенные для обработки персональных данных, сведений конфиденциального (персонального) характера;
- помещения, в которых расположены средства обработки защищаемой информации;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

4.2 Подлежащая защите информация может находиться:

- на бумажных носителях;

- в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
- передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
- в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
- записываться и воспроизводиться с помощью программных и технических средств (диктофоны, видеомагнитофоны и др.).

4.3 Среда информационного обмена обеспечивается, в том числе, общедоступными информационными ресурсами.

5. Угрозы информационной безопасности

5.1 Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

- несанкционированное распространение (передача) персональных данных;
- утрата сведений, составляющих конфиденциальную информацию, персональные данные Учреждения и иную защищаемую информацию, а также искажение такой информации;
- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д);
- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;
- отсутствие планирования и контроля;
- низкая степень надежности программного обеспечения;
- недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

5.2 В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Учреждения и его нормальное функционирование:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности Учреждения и потери, связанные с невозможностью выполнения им своих обязательств;
- моральные потери (ущерб репутации Учреждения).

6. Меры обеспечения информационной безопасности

6.1 Требования об обеспечении информационной безопасности Учреждения и обработке персональных данных обязательны к соблюдению всеми работниками Учреждения и пользователями информационных систем.

6.2 Руководство Учреждения приветствует и поощряет в установленном порядке деятельность работников Учреждения и пользователей информационных систем по обеспечению информационной безопасности.

6.3 Неисполнение или некачественное исполнение сотрудниками Учреждения и пользователей информационных систем обязанностей по обеспечению информационной безопасности и обработке персональных данных может повлечь применение к виновным административных мер воздействия, степень которых определяется установленным в Учреждении порядком либо требованиями действующего законодательства.

6.4 Система обеспечения безопасности информационных ресурсов должна соответствовать экономической целесообразности.

6.5 Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, криптографических, программных средств и мер по защите информации в процессе документооборота, при работе работников с персональными данными, конфиденциальными документами и сведениями, при обработке информации в информационных системах различного уровня и назначения, при передаче по каналам связи, при ведении деловых переговоров.

6.6 Управление рисками информационной безопасности в Учреждении включает в себя:

- анализ влияния на информационную безопасность Учреждения применяемых в деятельности Учреждения технологий, а также внешних по отношению к Учреждению событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз, выявление, анализ и оценка значимых для Учреждения угроз информационной безопасности;
- выявление возможных негативных последствий для Учреждения, наступающих в результате проявления рисков информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Учреждения;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и выявление рисков, неприемлемых для Учреждения;
- оценку влияния защитных мер на цели основной деятельности Учреждения;
- оценку затрат на реализацию защитных мер.

6.7 Организационные меры обеспечения информационной

безопасности включают в себя:

- организацию контроля доступа в здания и помещения Учреждения, предназначенные для обработки сведений конфиденциального и персонального характера;
- разработку и осуществление разрешительной системы допуска работников к работам с документами и персональными данными;
- заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности, обработки персональных данных и сохранность конфиденциальной информации (персональных данных);
- установление единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);
- координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;
- проведение периодического обучения и повышения квалификации работников Учреждения в области информационной безопасности;
- минимизацию данных конфиденциального (персонального) характера, доступных работникам;
- обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;
- практическую проверку функционирования мер защиты обработки персональных данных и конфиденциальной информации.

6.8 Технические меры обеспечения информационной безопасности включают в себя:

- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Учреждения и информации, обрабатываемой в них;
- применение программных, программно-аппаратных средств криптографической защиты информации;
- обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;
- обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- применение средств обнаружения вторжений;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- предотвращения несанкционированного изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;
- проверку машинных и ручных протоколов выполнения работ со стороны пользователей;
- применение мер и технических средств, снижающих вероятность

несанкционированного получения информации в устной форме (пассивная защита);

6.9 Управление инцидентами информационной безопасности в Учреждении включает в себя:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Учреждения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности.

7. Структура управления политикой информационной безопасности

7.1 В целях выполнения задач по обеспечению информационной безопасности Учреждения, в Учреждении определены следующие роли:

- Руководитель Учреждения.
- Ответственный за обработку персональных данных.
- Администратор сети.
- Классные руководители.
- Преподаватели.
- Работники Учреждения.
- Охранники

7.2 При необходимости могут быть определены и другие роли по информационной безопасности.

7.3 Общее руководство обеспечением информационной безопасности Учреждения осуществляет руководитель Учреждения.

7.4 Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Учреждения лежит на **ответственном за обработку персональных данных.**

7.5 Ответственность преподавательского состава и работников Учреждения за невыполнение настоящей Политики определяется законодательством Российской Федерации, а также положениями внутренних нормативных документов (локальных актов) Учреждения.

7.6 Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Учреждения осуществляются и координируются **ответственным за обработку персональных данных.**

7.7 Задачи ответственного за обработку персональных данных и преподавательского состава Учреждения по обеспечению информационной безопасности определяются законодательством Российской Федерации и локальными актами **Учреждения.**

7.8 **Руководитель Учреждения** может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые ответственным за обработку персональных данных**,** и может, при необходимости привлекать для работы в них ответственных сотрудников других подразделений Учреждения на основе совмещения работы в группе со своими основными должностными обязанностями.

7.9 Финансирование работ по реализации положений настоящей Политики осуществляется в рамках бюджета Учреждения.

8. Контроль за соблюдением положений Политики

8.1 Общий контроль состояния информационной безопасности Учреждения осуществляется **Руководителем Учреждения.**

8.2 Контроль соблюдения настоящей Политики осуществляет **ответственный за обработку персональных данных** на основе проведения внутреннего аудита информационной безопасности**.**

8.3 Контроль осуществляется путем проведения мониторинга и управлением инцидентов информационной безопасности Учреждения, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

9. Заключительные положения

9.1 Требования настоящей Политики могут развиваться другим внутренними нормативными документами Учреждения, которые дополняют и уточняют ее.

9.2 В случае изменения действующего законодательства и иных нормативных актов, а также Устава Учреждения настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Учреждения. В этом случае ответственный за обработку персональных данных обязан незамедлительно инициировать внесение соответствующих изменений.

9.3 Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 12 месяцев;
- внеплановое внесение изменений в настоящую Политику может

производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Приложение № 3
к приказу от 10.07.2017
№ 369

ПОЛИТИКА
по работе с инцидентами информационной безопасности МБОУ «СОШ № 6»

1.Общие положения

1.1. Настоящая Политика развивает положения «Политики информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» (далее – Учреждение).

1.2. Целью настоящей Политики является установление общих руководящих принципов наблюдения состояния информационной безопасности (далее - ИБ) и использования результатов для осуществления менеджмента инцидентами ИБ.

1.3. Настоящая Политика распространяется на все технологические процессы Учреждения и обязательна для применения всеми работниками Учреждения.

1.4. Мероприятия по обеспечению ИБ Учреждения, выполняемые с целью реализации требований настоящей Политики, утверждаются внутренними нормативными документами в соответствии с установленным в Учреждении порядком.

1. Список терминов и определений

2.1. **Активы Учреждения** – все, что имеет ценность для Учреждения и находится в его распоряжении.

2.2. **Работники Учреждения** - преподавательский состав, административный и вспомогательный персонал образовательного учреждения.

К активам Учреждения относятся:

- преподавательский и рабочий персонал, финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации - платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;
- Технологические процессы;
- Продукты и услуги, предоставляемые обучающимся и их родителям;

2.3. **Технологический процесс** – технологический процесс, содержащий операции по изменению и (или) определению состояния информации, используемой при функционировании автоматизированных

систем Учреждения или необходимой для реализации услуг.

2.4. **Комиссия для расследования инцидентов информационной безопасности** (далее - Комиссия) – действующая на постоянной (временной) основе группа работников Учреждения, которая выполняет процедуры менеджмента инцидентами ИБ в течение их жизненного цикла.

Комиссия способствует оперативному реагированию на инциденты ИБ, в том числе за счет независимости применяемых процедур и средств вычислительной техники от компонентов информационной инфраструктуры Учреждения.

2.5. **Информационно-технологический актив** (далее - ИТ-актив) – актив Учреждения, к которому относятся:

- информационные активы;
- программные средства;
- аппаратные и программно-аппаратные средства.

2.6. **Информационный актив** – информация с позволяющими ее идентифицировать реквизитами, имеющая ценность для Учреждения, находящаяся в его распоряжении, представленная в виде документов на бумажном носителе, а также в виде электронных копий, пригодных для обработки.

2.7. **Инцидент ИБ** – рисковое событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Реализация угрозы ИБ – это нарушение свойств ИБ (конфиденциальности, целостности или доступности) информационных активов Учреждения.

Нарушение может вызываться источниками угроз ИБ, либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

2.8. **Менеджмент инцидентов ИБ** – деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них в интересах минимизации и/или ликвидации негативных последствий для Учреждения (включая нарушение непрерывности технологических процессов) при нарушениях ИБ.

2.9. **Рисковое событие** – реализовавшееся событие, обусловленное операционным риском, повлекшее или способное повлечь за собой операционные потери Учреждения и произошедшее по причине ошибочности или сбоя процессов, действий людей и систем, а также по причине внешних событий.

2.10. **Событие ИБ** – изменение состояния объекта или области мониторинга ИБ, подлежащее регистрации средствами мониторинга ИБ.

2. Перечень сокращений

АС – автоматизированная система.

БД – база данных.

ИТ – информационные технологии.

ИТ-актив – информационно-технологический актив.

ИБ – информационная безопасность.

3. Общие положения по организации мониторинга ИБ и менеджмента инцидентов ИБ

3.1. Организация мониторинга ИБ

3.1.1. Мониторинг ИБ в Учреждении осуществляется с целью своевременного выявления фактов, оказывающих негативное воздействие на ИТ-активы Учреждения. Указанная цель достигается путем решения следующих задач:

- своевременное выявление угроз ИБ, как внешних, так и внутренних, способных нанести ущерб Учреждению, а также условий и факторов их реализации;
- выявление уязвимостей в сфере ИБ;
- выявление злоумышленных или несанкционированных (выполненных с нарушением установленных правил и прав) действий работников Учреждения и обучающихся (внутренних нарушителей);
- контроль выполнения требований внутренних нормативных и организационно-распорядительных документов Учреждения по обеспечению ИБ.

3.1.2. Перечень ИТ-активов Учреждения, являющихся объектами мониторинга ИБ, и целесообразность изменения состава этого перечня определяются на основании:

- требований законодательства Российской Федерации и внутренних нормативных документов Учреждения;
- результатов оценки важности ИТ-активов Учреждения;
- результатов оценки рисков ИБ Учреждения;
- необходимости контроля состояния защитных мер ИБ;
- технических возможностей потенциальных объектов мониторинга.

Состав перечня ИТ-активов, являющихся объектами мониторинга ИБ, и параметры мониторинга ИБ устанавливаются ответственным и согласовываются с руководителем Учреждения.

3.1.3. Планирование и реализация мероприятий по осуществлению мониторинга ИБ и реагированию на инциденты ИБ выполняется ответственным.

3.1.4. Во внутренних нормативных документах Учреждения должны быть определены условия и временные периоды хранения информации, собранной в процессе мониторинга ИБ.

3.1.5. Доступ к информации мониторинга ИБ должен быть ограничен. Список лиц, допущенных к информации мониторинга ИБ, должен быть определен ответственным.

3.2. Организация менеджмента инцидентов ИБ

4.2.1. Менеджмент инцидентов ИБ должен основываться на результатах мониторинга ИБ.

4.2.2. Основными целями менеджмента инцидентов ИБ являются:

- своевременное обнаружение инцидентов ИБ;
- адекватное и оперативное реагирование на них в интересах предотвращения реализации угроз ИБ;
- минимизация операционных рисков ИБ;
- минимизация и/или ликвидация негативных последствий для Учреждения (включая нарушение непрерывности технологических процессов) при нарушениях ИБ.

4.2.3. Менеджмент инцидентов ИБ должен поддерживаться в Учреждении совокупностью нормативно-правовых, организационных и технических мер.

4.2.4. Для исключения и/или минимизации негативных последствий инцидентов ИБ на технологические процессы должна поддерживаться согласованность процедур менеджмента инцидентов ИБ с процедурами менеджмента рисков ИБ, процедурами управления операционными рисками, а также с процедурами по обеспечению непрерывности технологических процессов.

4.2.5. Работники Учреждения должны быть проинструктированы на основании материалов, подготавливаемых Ответственным за обработку персональных данных, о возможных инцидентах ИБ и относительно порядка действий в условиях их реализации.

4.2.6. Деятельность в рамках менеджмента инцидентов ИБ должна осуществляться как оперативный, непрерывный и автоматизированный процесс.

4.2.7. Сбор информации в процессе управления инцидентом ИБ, расследование причин возникновения инцидентов ИБ и выявление нарушителей ИБ, а также применение дисциплинарных и административных мер должны осуществляться с соблюдением законодательства Российской Федерации и договорных обязательств Учреждения.

4. Реализация положений настоящей Частной политики

5.1. Критерии идентификации и оценки инцидентов ИБ

5.1.1. Причинами инцидентов ИБ в Учреждении могут являться действия, техногенных, антропогенных, природных факторов. По отношению к Учреждению эти факторы могут быть как внешними, так и внутренними, а их действие носить как случайный, так и умышленный характер.

5.1.2. Для целей идентификации и классификации инцидентов ИБ, а также выбора способов и методов последующего управления ими должны применяться следующие критерии:

- локализация воздействия, которая характеризует локальный или распределенный характер воздействия;
- масштаб (число ИТ-активов, на которые негативно повлиял или может повлиять инцидент ИБ);
- вовлеченные ИТ-активы (например, резервные копии данных, коммуникационное оборудование, программные средства электронной почты);
- связанные с инцидентом области ИБ (например, защита от вредоносных программ, управлением доступом);
- продолжительность, определяющая длительность и/или определенную последовательность нежелательных действий/событий во времени;
- вовлеченные в инцидент ИБ работники Учреждения, посторонние лица и их роль в инциденте (например, лицо, обнаружившее инцидент; предполагаемые нарушитель, владелец ИТ-актива);
- источник воздействия – природное явление, техногенный фактор или человеческий фактор;
- нарушаемые в результате инцидента свойства безопасности ИТ-активов, а также технологические процессы, непрерывность которых нарушена;
- степень опасности: оцениваются потенциальные негативные последствия для Учреждения, рассчитываемые исходя из степени потенциального или явного воздействия последствий инцидента на технологические процессы;
- категория потерь – прямые финансовые и/или материальные потери Учреждения, ущерб здоровью персонала, ущерб репутации Учреждения, снижение доверия к Учреждению со стороны заинтересованных лиц, нарушение законодательства РФ и договорных обязательств и т.д.;
- приоритет – степень срочности требуемого отклика на инцидент ИБ;
- объем имеющейся информации об инциденте.

Приведенный перечень критериев может быть при необходимости уточнен в рамках процесса планирования и подготовки менеджмента инцидентов ИБ.

5.2. **Роли и ответственность**

5.2.1. Для обеспечения процессов и процедур мониторинга и менеджмента инцидентов ИБ и минимизации воздействия инцидента на основную деятельность в Учреждении создается Комиссия.

5.2.2. Допускается совмещение одним работником Учреждения исполнения роли члена Комиссии с исполнением других ролей ИБ. Не допускается исполнение роли члена Комиссии лицом, в отношении которого проводится расследование.

5.2.3. Работники Учреждения могут быть включены в состав

Комиссии как обязательные эксперты на постоянной основе или как привлекаемые эксперты по мере необходимости. Постоянными членами Комиссии являются руководитель группы (работник ответственного подразделения), несущий ответственность за организацию и координацию всех работ, а также работники ответственного подразделения, непосредственно выполняющие различные процедуры по обеспечению ИБ.

5.2.4. В функции обязательных экспертов Комиссии входит:

- участие в следующих процессах:
  - согласования с ответственным за обработку персональных данных деятельности по управлению инцидентами ИБ;
  - выбора критериев классификации инцидентов ИБ;
  - разработки операционных процедур менеджмента инцидентов ИБ;
  - проверки и тестирования процессов и процедур менеджмента инцидентов ИБ;
- сбор и регистрация информации о событиях, связанных с обеспечением ИБ, полученной из различных источников, включая:
  - информацию мониторинга ИБ;
  - результаты анализа информации мониторинга ИБ;
  - информацию об инцидентах ИБ, получаемую от работников Учреждения обучающихся и их родителей;
- контроль процесса мониторинга ИБ в целях его планирования и дальнейшего совершенствования, а именно:
  - выявление и регистрация инцидентов ИБ;
  - анализ инцидентов ИБ, определение и регистрация их характеристик (масштаб, воздействие, вовлеченные лица и др.), идентификация инцидентов ИБ на основе критериев классификации, оценка инцидентов ИБ, планирование дальнейших действий по управлению конкретным инцидентом ИБ на основе предварительного плана для соответствующего класса инцидентов ИБ;
  - регистрация инцидента ИБ в качестве рискового события операционного риска в соответствии с порядком, определенным в соответствующих внутренних нормативных документах Учреждения;
- оповещение об инцидентах ИБ лиц, заинтересованных в обеспечении ИБ, организация, координирование и регистрация действий по управлению инцидентами ИБ, а также участие в данных действиях в рамках своей компетенции;
- организация расследования инцидента ИБ и (или) участие в расследовании инцидента ИБ (выявление причин, вызвавших инцидент, анализ и оценка эффективности и адекватности мер, предпринимаемых исполнителями соответствующих ролей в рамках своей компетенции), в частности, сбор, регистрация и анализ дополнительных сведений об инциденте ИБ;
- участие в процессах пересмотра и улучшения менеджмента инцидентов ИБ, включая:
  - подготовку информационных материалов для проведения оценки

эффективности менеджмента инцидентов ИБ;

- участие в проведении оценки эффективности менеджмента инцидентов ИБ;
- формирование предложений по повышению качества менеджмента инцидентов ИБ;
- реализацию принятых решений по улучшению менеджмента инцидентов ИБ в пределах своей компетенции;
- администрирование и использование инструментальных средств автоматизации менеджмента инцидентов ИБ.

5.2.5. Главная задача Комиссии состоит в реализации процедур мониторинга и менеджмента инцидентов ИБ, кроме того на Комиссию может быть возложен и ряд других задач, таких как:

- разработка рекомендаций по ИБ;
- мониторинг уязвимости сетей, систем и приложений;
- обнаружение вторжений;
- повышение осведомленности персонала Учреждения в сфере ИБ;
- исследование тенденций развития ИБ в целях выявления новых угроз;
- менеджмент изменений и обновлений сетей, систем и приложений.

5.3. **Процедуры мониторинга ИБ, проводимые с использованием программно-технических средств**

5.3.1. Сбор и фильтрация информации мониторинга.

5.3.1.1. При проведении мониторинга ИБ с использованием программно-технических средств источниками информации мониторинга ИБ должны быть журналы регистрации событий (аудита) штатных систем, регистрации событий контролируемых объектов, входящих в состав прикладных и общесистемных продуктов и платформ, и/или специализированные средства сбора информации о событиях ИБ.

5.3.1.2. Регистрации событий ИБ обеспечивается путём:

- защиты от неавторизованного отключения средств регистрации событий ИБ;
- защиты от неавторизованного изменения списка регистрируемых событий ИБ;
- защиты от неавторизованного редактирования или удаления файлов с записями информации мониторинга (журналов регистрации событий ИБ);
- сохранения архива файлов с записями журналов регистрации событий ИБ.

5.3.2. Администрирование базы данных мониторинга должно включать следующие операции:

- архивирование БД мониторинга;
- резервное копирование БД мониторинга;
- восстановление архивных и резервных копий БД мониторинга.

5.3.3. Сохраненная в БД информация мониторинга в дальнейшем может использоваться как доказательства инцидентов ИБ при анализе этих инцидентов.

5.3.4. Анализ информации мониторинга

5.3.4.1. В ходе анализа множества собранных событий ИБ выявляется множество параметров, характеризующих действия/поведение/состояние объектов мониторинга. Анализ выявленных параметров выполняется по правилам (критериям мониторинга ИБ), применение которых обеспечивает решение следующих задач мониторинга:

- оперативное выявление событий ИБ, свидетельствующих об инцидентах ИБ, в целях их последующего использования в рамках менеджмента инцидентов ИБ;
- оперативное выявление фактов нарушения функционирования и/или нештатного функционирования средств обеспечения ИБ (защитных мер);
- наблюдение за действиями пользователей систем и средств, находящихся во владении и/или под управлением (в распоряжении) Учреждения, с целью контроля соблюдения ими норм и требований ИБ, установленных в Учреждении;
- наблюдение за состоянием ИТ- активов и поведением участников информационных технологических процессов (в т.ч. внешних по отношению к ней субъектов) с целью выявления их нетипичного состояния/поведения, представляющего опасность для информационных активов или для ее деятельности в целом;
- наблюдение за критичными для Учреждения ИТ-активами в интересах обеспечения непрерывности технологических процессов.

5.3.4.2. Применяемые программно-технические средства мониторинга должны обеспечивать возможность проведения анализа данных мониторинга в оперативном режиме, а также на основе информации из архивной БД мониторинга по запросам уполномоченных сотрудников Комиссии (за прошедший период).

5.3.5. Контроль и пересмотр процедур мониторинга ИБ.

5.3.5.1. Контроль и пересмотр процедур мониторинга ИБ, применяемых средств мониторинга должно производиться по результатам анализа и оценки эффективности функционирования средств мониторинга ИБ, их адекватности требованиям по своевременному выявлению и идентификации инцидентов ИБ, связанных с контролируемыми объектами.

5.3.5.2. Пересмотр должен выполняться периодически, в плановом порядке, не реже одного раза в год или во внеплановом порядке при необходимости.

5.3.6. Процедура улучшения.

5.3.6.1. В рамках этой процедуры должно проводиться изменение параметров и критериев мониторинга ИБ, совершенствование средств сбора и анализа информации мониторинга на основании результатов оценки эффективности мониторинга, изменения задач мониторинга, изменения

состава и свойств контролируемых ИТ- активов.

5.4. Процедуры мониторинга ИБ, проводимые на основе организационных мер

5.4.1. Отслеживание изменений нормативно-правовой базы в области ИБ. Требования по обеспечению ИБ в Учреждении определяются в частности:

- законодательством Российской Федерации;
- международными актами и межгосударственными соглашениями;
- законодательством государств, с резидентами которых Учреждение осуществляет взаимодействие;
- стандартами (межгосударственными и Российской Федерации);
- внутренними нормативными документами Учреждения.

5.4.2. Проверка соблюдения процедур ИБ работниками Учреждения.

Контроль соблюдения процедур ИБ организационными мерами проводится в целях выявления нарушений ИБ работниками Учреждения в форме проверок деятельности структурных подразделений и отдельных работников. Указанный контроль должен быть направлен на:

- наличие и достаточность документов, регламентирующих в Учреждении деятельность в области обеспечения ИБ;
- соблюдение процедур хранения, использования и уничтожения носителей конфиденциальной информации и документов, содержащих сведения ограниченного доступа;
- использование работниками Учреждения при выполнении своих должностных обязанностей документов, регламентирующих деятельность в области обеспечения ИБ;
- соблюдение работниками Учреждения и обучающимися правил по ИБ в случае необходимости выполнения своих обязанностей, обучения за пределами установленной продолжительности рабочего времени и состояния рабочего места (мест обучения);
- соблюдение работниками Учреждения процедур использования съемных машинных носителей информации;
- соблюдение договорных обязательств (соглашений) в части обеспечения ИБ.

5.4.3. Результаты мониторинга ИБ организационными мерами должны использоваться для принятия решений, направленных на формирование и реализацию корректирующих и превентивных действий по совершенствованию системы менеджмента инцидентов ИБ, в том числе для выработки предложений по повышению эффективности организационных мер проведения мониторинга.

5.5. Планирование и подготовка менеджмента инцидентов ИБ

В рамках процесса планирования и подготовки менеджмента инцидентов ИБ ответственным должно быть предусмотрено выполнение следующих процедур:

- разработка и документирование организационных мер и

программно-технических средств управления инцидентами ИБ. Формы, процедуры и инструменты поддержки для обнаружения, оповещения, оценки и реагирования на инциденты ИБ должны быть изложены в соответствующих внутренних нормативных документах Учреждения;

- распределение ролей и назначение ответственных исполнителей по выполнению процедур менеджмента инцидентов ИБ;
- обеспечение осведомленности исполнителей ролей ИБ по вопросам выполнения процедур менеджмента инцидентов ИБ;
- обеспечение исполнителей ролей менеджмента инцидентов ИБ необходимыми ресурсами для выполнения процедур менеджмента инцидентов ИБ;
- выработка (уточнение) критериев, используемых для идентификации и оценки инцидента ИБ;
- определение/уточнение перечня новых инцидентов, подлежащих выявлению. Выбор может основываться на результатах оценки рисков ИБ Учреждения;
- разработка планов по управлению различными инцидентами ИБ с участием всех заинтересованных самостоятельных структурных подразделений Учреждения и их согласование (при необходимости) с планами обеспечения непрерывности технологических процессов и процедурами управления операционными рисками Учреждения;
- проверка и тестирование процессов и процедур менеджмента инцидентов ИБ;
- составление форм сообщений и отчетов об инцидентах ИБ;
- оповещение персонала Учреждения и других организаций, чьи информационные ресурсы находятся во владении (распоряжении) Учреждения, о том, что они находятся в зоне действия процедур управления инцидентами ИБ.

5.6. Реализация (использование) менеджмента инцидентов ИБ

5.6.1. Обнаружение и фиксирование инцидентов ИБ

5.6.1.1. Своевременное обнаружение и фиксирование всех инцидентов ИБ должно основываться на сборе и анализе необходимой для этого информации, а также на выявлении тенденций, указывающих на негативное развитие ситуации, связанной с идентифицированным инцидентом ИБ.

5.6.1.2. Инициирование процедур менеджмента инцидентов ИБ должно выполняться:

- в оперативном режиме по данным систем/средств мониторинга;
- после получения сообщения об инциденте ИБ.
- по запросам заинтересованных лиц (руководства, администраторов ИБ и др.) данных об инцидентах ИБ за любой прошедший период.

5.6.1.3. Источниками информации об инцидентах ИБ являются:

- системы/средства мониторинга ИБ;
- программные (технические) средства обнаружения вторжений;

- антивирусное программное обеспечение;
- средства регистрации событий операционных систем, услуг и приложений;
- средства регистрации событий активного сетевого оборудования;
- устройства сигнализации;
- работники Учреждения (пользователи систем/средств, администраторы ИБ, администраторы систем);
- работники других организаций, имеющие доступ к информационным активам, находящимся под управлением (в распоряжении) Учреждения.

5.6.1.4. Для обнаружения инцидентов ИБ должны реализовываться механизмы мониторинга ИБ Учреждения.

5.6.1.5. Для обнаружения и фиксирования инцидентов ИБ должны применяться специализированные инструментальные средства, обеспечивающие возможность фиксирования работниками Учреждения, а также, при необходимости, работниками других организаций, информация об инцидентах ИБ при помощи специализированных форм регистрации.

5.6.1.6. Вся информация об инцидентах ИБ, полученная от различных источников, должна быть сохранена в отдельной базе данных. Эта информация может быть в дальнейшем использована для анализа и проведения расследования инцидента ИБ.

5.6.2. Анализ и оценка инцидентов ИБ

5.6.2.1. Анализ и оценка (по степени опасности) идентифицированных инцидентов ИБ проводится с целью выявления среди них инцидентов, представляющих непосредственную угрозу ИБ Учреждения.

5.6.2.2. Для анализа и оценки инцидентов ИБ используется информация из хранилища данных об инцидентах ИБ, позволяющая определить источник и детальные характеристики инцидента ИБ.

5.6.2.3. В ходе анализа и оценки инцидентов ИБ определяется их приоритетность и действия по управлению в соответствии с установленными критериями для предотвращения и/или минимизации возможных негативных последствий (ущерба) для Учреждения.

5.6.2.4. Менеджмент инцидентов ИБ должен выполняться в соответствии со следующими установленными приоритетами:

- приоритет № 1 – обеспечение здоровья и безопасности работников Учреждения, обучающихся и их родителей;
- приоритет № 2 – обеспечение непрерывности технологических процессов;
- приоритет № 3 – обеспечение требуемых свойств безопасности ИТ- активов;
- приоритет № 4 – минимизация финансовых и материальных потерь (в т. ч., связанных с нарушением договорных обязательств);
- приоритет № 5 – соблюдение законодательства РФ и требований регулирующих органов;
- приоритет № 6 – поддержание деловой репутации Учреждения.

5.6.3. Сообщение (оповещение) об инциденте ИБ

5.6.3.1. Работники Учреждения должны быть проинструктированы о процедурах оповещения об инцидентах ИБ различных типов.

5.6.3.2. Сообщение об инциденте ИБ должно содержать следующие основные параметры:

- информацию о факте обнаружения инцидента ИБ;
- краткое описание инцидента ИБ с указанием вовлеченных в инцидент ИТ- активов;
- действия, предпринятые членами Комиссии в отношении этого инцидента ИБ;
- контактную информацию для заинтересованных сторон (например, владельцев ИТ-актива, системных администраторов ИБ);
- комментарии членов Комиссии;
- перечень мер, которые должны быть предприняты для нейтрализации инцидента ИБ.

5.6.4. Сбор и регистрация информации об инциденте ИБ и о действиях по управлению этим инцидентом.

5.6.4.1. Сбор и регистрация информации об инциденте ИБ и действиях по управлению этим инцидентом проводится для поддержания процедур последующего анализа и расследования (при необходимости) и выработки мер по совершенствованию деятельности по обеспечению ИБ.

5.6.4.2. Сообщение об инциденте ИБ и другая дополнительная информация, включающая доказательства (свидетельства) инцидента ИБ, собранная автоматизированными и организационными способами, должны быть оформлены и сохранены. При этом должна сохраняться информация, относящаяся к инциденту ИБ, необходимая для его дальнейшего анализа, формирования отчета об инциденте ИБ и потенциального использования в качестве свидетельства в дисциплинарных процессах.

5.6.4.3. Вся информация об инцидентах ИБ и действиях по управлению ими должна быть сохранена в базе данных инцидентов ИБ. По ходу выполнения анализа и процедур реагирования на инцидент ИБ, данные об инциденте ИБ в базе данных должны обновляться. Указанные действия должен осуществлять ответственный за обработку персональных данных (администратор информационных ресурсов Учреждения).

5.6.4.4. На инциденты ИБ распространяются требования действующего в Учреждении порядка регистрации рисковых событий.

5.6.4.5. Управление информацией об инцидентах ИБ и действиях по управлению ими включает:

- определение места, условий и времени оперативного и архивного хранения данных;
- документирование инструкций и описаний инструментов и правил выполнения резервирования, дублирования, архивирования и порядок доступа к архивным и резервным копиям;
- обеспечение конфиденциальности, целостности и доступности данных;

- обеспечение доступа к данным только авторизованным лицам.

5.6.5. Действия ответственного за обработку персональных данных по управлению инцидентом ИБ.

5.6.5.1. Сдерживание/предотвращение:

- после обнаружения и оценки инцидента ИБ необходимо предпринять все необходимые и доступные меры по сдерживанию/пресечению распространения негативного воздействия на ИТ-активы Учреждения;
- для обеспечения своевременной и эффективной реакции на выявленный инцидент ИБ должны быть разработаны соответствующие действия и защитные меры по сдерживанию/пресечению инцидента ИБ. Действия по сдерживанию должны зависеть от типа инцидента ИБ и должны выполняться в соответствии с установленным регламентом и планом по управлению каждым из основных типов инцидентов. Процедуры сдерживания инцидента ИБ должны учитывать потенциальный ущерб ИТ - активам от инцидента; время и ресурсы, необходимые для сдерживания; эффективность сдерживания (частичное или полное сдерживание инцидента).

5.6.5.2. Расследование инцидента ИБ:

- процедура расследования предназначена для выявления, в том числе с применением организационных процедур, причин (условий и факторов), вызвавших инцидент ИБ, и/или негативную тенденцию развития связанной с этим инцидентом ИБ ситуации, а также анализа и оценки адекватности и эффективности действий, предпринятых в Учреждении, по управлению инцидентом ИБ;
- процедура расследования инцидента ИБ может включать идентификацию нарушителя ИБ по данным, собранным при обнаружении инцидента ИБ, а также при необходимости эскалацию инцидента ИБ. Уровень эскалации инцидента ИБ выбирает руководитель Комиссии на основании возможных операционных потерь Учреждения.

5.6.5.3. Восстановление (устранение последствий):

- процедуры восстановления ИТ-активов, которым был нанесен ущерб, служат для минимизации или ликвидации (по возможности) негативных последствий от инцидентов ИБ и зависят от типа инцидента ИБ. Процедуры определяются на этапе планирования для каждого типа инцидентов ИБ и реализуются с учетом доступных ресурсов и потребностей (частичное или полное восстановление);
- деятельность по восстановлению после инцидентов ИБ должна быть согласована с планами обеспечения непрерывности технологических процессов и может быть делегирована для выполнения соответствующим системным администраторам ИБ и/или администраторам систем.

5.6.5.4. Закрытие (разрешение) инцидента ИБ:

- после выполнения всех необходимых действий по анализу, оценке и реагированию инцидент ИБ должен быть закрыт (разрешен);
- решение о закрытии (разрешении) инцидента ИБ может быть

принято не только при выполнении процедур реагирования на инцидент, но и ранее – при анализе инцидента, и позже – при оценке инцидента. Решение о закрытии (разрешении) инцидента ИБ должен принимать руководитель Комиссии.

5.7. Пересмотр процессов менеджмента инцидентов ИБ

5.7.1. Процедуры пересмотра и улучшения процессов менеджмента инцидентов ИБ должны выполняться как на регулярной основе (периодически), так и по результатам применения их для любого существенного инцидента ИБ (при необходимости).

5.7.2. Оценка процедур и процессов менеджмента инцидента ИБ включает:

- просмотр документов и отчетов по инциденту ИБ и оценку их полноты;
- рассмотрение эффективности мониторинга ИБ для регистрации инцидента ИБ;
- оценку ущерба от инцидента ИБ;
- определение достаточности принятых мер и ресурсов по управлению инцидентом ИБ;
- оценку адекватности планов и процедур реагирования на инциденты ИБ;
- прогноз мер, которые могли бы предотвратить инцидент ИБ.

5.7.3. Завершающий отчет по инциденту ИБ должен включать информацию, которая может быть использована в будущем при выполнении процедур менеджмента инцидентов ИБ. Также отчет может служить основой для оценки ущерба от инцидента ИБ для дальнейшего дисциплинарного процесса.

В отчете об инциденте ИБ должны быть отражены:

- дата, время и место инцидента ИБ;
- сведения о работнике, выявившем инцидент ИБ, информацию об инциденте ИБ, описание предпринятых действий и мер при обнаружении инцидента (включая использованные инструментальные средства) с обоснованием;
- место хранения свидетельства (информации, показаний) инцидента ИБ, способа архивирования, способа защиты и доступа к нему.

5.7.4. Отчет об инциденте ИБ должен сохраняться в базе данных инцидентов ИБ.

5.7.5. Результаты анализа и оценки инцидентов ИБ после их всестороннего исследования могут быть использованы для принятия решений, направленных на выбор и реализацию мер по совершенствованию менеджмента инцидентов ИБ, оценке рисков ИБ, по подготовке предложений по улучшению ИБ, обновлению и/или реализации новых защитных мер ИБ.

5.7.6. Предложения по улучшению менеджмента инцидентов ИБ могут касаться:

- изменения или подготовки новых требований к защитным мерам ИБ (программно-техническим и организационным);
- пересмотра политик, стандартов, процедур и регламентирующих документов ИБ;
- изменений в политике менеджмента инцидентов ИБ, а также в процессах, процедурах управления инцидентами ИБ и в отчетных формах;
- подготовки новых организационно-распорядительных документов (мероприятий).
- изменения конфигурации аппаратных и программных средств ИТ-блока и системы менеджмента ИБ;
- разработки новых организационных мер обеспечения ИБ;
- перераспределения финансовых затрат на обеспечение ИБ.

5.8. Улучшение менеджмента инцидентов ИБ

Улучшение менеджмента безопасности должно заключаться в следующем:

- введении новых или изменении действующих защитных мер ИБ, доработке внутренних нормативных документов ИБ, изменении конфигурации аппаратного и программного обеспечения;
- введении в действие усовершенствованных процедур менеджмента инцидентов ИБ и документов, новых отчетных форм и их тестировании до ввода в эксплуатацию.

5. Контроль за соблюдением требований настоящей политики

Контроль за соблюдением настоящей политики осуществляет ответственный за обработку персональных данных на основе проведения мониторинга и оценки состояния ИБ, а также в рамках иных контрольных мероприятий.

6. Ответственность за несоблюдение требований настоящей политики

Ответственность за несоблюдение требований настоящей политики, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством РФ, внутренними нормативными документами Учреждения, а также должностными инструкциями работников Учреждения.

7. Заключительные положения

8.1. Настоящая Политика вступает в силу с даты ее утверждения.

8.2. Ответственность за поддержание настоящей Политики в актуальном состоянии, создание, внедрение, координацию процессов системы менеджмента инцидентов ИБ и внесение изменений в процессы системы менеджмента инцидентов ИБ возлагается на руководителя

Учреждения.

8.3. В случае изменения законодательства РФ, изменения или введения в действие стандартов, нормативных методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным документам. При необходимости ответственное подразделение незамедлительно инициирует внесение соответствующих изменений в настоящую Политику в установленном в Учреждении порядке.

8.4. Внесение изменений в настоящую Политику должно осуществляться на периодической и внеплановой основе:

- периодическое внесение изменений не реже одного раза в 24 месяца;
- внеплановое внесение изменений может проводиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.

Приложение № 4
к приказу от 10.07.2017 № 369

ПОЛОЖЕНИЕ
о разрешительной системе доступа. Матрица доступа к защищаемым ресурсам в автоматизированной системе «АРМ-К СОШ №6» Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6»

№ п/п	Учётный (заводской) номер АРМ	Адрес, № помещения	ФИО пользователя (группы) ресурсом	Наименование защищаемых информационных ресурсов	Тип доступа
1.	1622C051600169	628307, РФ, ХМАО-Югра, Тюменская обл., г. Нефтеюганск, 8 микрорайон, здание 28 Кабинет приемной	Трутнева Елена Геннадьевна	C:\avers\db1.gdb	чтение запись выполнение удаление
				DVD-RW	чтение запись выполнение
				Программные средства	чтение выполнение
				Операционная система, средства защиты информации	чтение выполнение
2.	1201891	628307, РФ, ХМАО-Югра, Тюменская обл., г. Нефтеюганск, 8 микрорайон, здание 28	Ханкишиева Бановша Фейрузовна	C:\	чтение запись выполнение удаление
				DVD-RW	чтение
				Программные средства	чтение запись выполнение

		Кабинет 220 лаборантская			удаление
				Операционная система, средства защиты информации	чтение запись выполнение удаление
3.	D3012	628307, РФ, ХМАО-Югра, Тюменская обл., г. Нефтеюганск, 8 микрорайон, здание 25 Кабинет заместителя директора	Александрова Ирина Алексеевна	C:\	чтение запись выполнение удаление
				DVD-RW	чтение
				Программные средства	чтение выполнение

Приложение 5
к приказу от 10.07.2017 № 369

ИНСТРУКЦИЯ
пользователя автоматизированной системы «АРМ-К СОШ №6» муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6»

1. Общие положения

Настоящая Инструкция разработана для обеспечения защиты персональных данных (конфиденциальной информации), обрабатываемых в автоматизированной системе «АРМ-К СОШ №6» Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6».

Персональные данные относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации являются:

- несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с конфиденциальной информацией (в том числе со служебными документами ограниченного распространения, персональными данными и т.д.) строится на следующих принципах:

принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник;

принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах;

2. Обязанности сотрудников, имеющих доступ к персональным данным (конфиденциальной информации).

Сотрудники, получившие доступ к персональным данным (конфиденциальной информации), обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки конфиденциальной информации немедленно информировать руководителя Учреждения.

Персональные данные (конфиденциальная информация) не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает сотрудника от взятых им обязательств по неразглашению сведений ограниченного распространения.

Сотрудники Учреждения при работе с персональными данными (конфиденциальной информацией) обязаны:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами автоматизированных рабочих мест;

выполнять требования Ответственного за обработку персональных данных (защиту информации), касающиеся защиты информации;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

хранить в тайне логин и пароль своей учётной записи, а также информацию о системе защиты, установленной на автоматизированном рабочем месте;

использовать для работы, только учтенные съемные носители информации;

контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления Ответственному за защиту персональных данных;

Немедленно ставить в известность руководителя Учреждения:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах автоматизированных рабочих мест или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищенному автоматизированному рабочему месту;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств автоматизированного рабочего места.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию персонального компьютера, выхода из строя или неустойчивого функционирования периферийных устройств (принтера, сканера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования

установленных в автоматизированном рабочем месте средств защиты, немедленно ставить в известность Ответственного за обработку персональных данных (защиту информации).

Ставить в известность Ответственного за обработку персональных данных (защиту информации) при:

- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации автоматизированного рабочего места;
- необходимости вскрытия системных блоков персональных компьютеров, входящих в состав автоматизированного рабочего места;
- резервном копировании информации;
- и т.д.

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос аппаратных средств автоматизированного рабочего места, на котором проводилась обработка персональных данных, за пределы Учреждения с целью их ремонта, замены и т.п. без согласования с руководителем Учреждения и ответственным за обработку персональных данных (защиту информации) **запрещен**. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за обработку персональных данных (защиту информации). В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

Автоматизированные рабочие места, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана монитора, не имеющими отношения к обрабатываемой информации сотрудниками.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно конфиденциальную информацию;
- использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с конфиденциальной информацией на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя Учреждения;
- накапливать ненужные для работы персональные данные;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища;
- использовать компоненты программного и аппаратного обеспечения автоматизированных рабочих мест в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств автоматизированных рабочих мест или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить персональные данные на неучтенных носителях информации (USB-накопителях, CD, DVD дисках, гибких магнитных дисках и т.п.);

- оставлять автоматизированное рабочее место без блокировки входа в учётную запись (экрана монитора);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению инцидента информационной безопасности. Об обнаружении такого рода ошибок необходимо – ставить в известность ответственного за обработку персональных данных (защиту информации).

3. Ответственность

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты конфиденциальной информации (персональных данных).

За разглашение конфиденциальной информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной, административной или уголовной ответственности, предусмотренной законодательством Российской Федерацией.

Приложение № 6
к приказу от 10.07.2017
№ 369

ИНСТРУКЦИЯ
по эксплуатации средств антивирусной защиты информационных средств, производящих обработку персональных данных (конфиденциальной информации) в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 6»

1. Общие положения

Компьютерный вирус является вредоносным программным средством и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на машинных носителях информации. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать информацию, при этом также могут пострадать аппаратные средства.

Основными путями «вирусного заражения» являются неквалифицированное обращение пользователей с автоматизированным рабочим местом при использовании ими «зараженных» машинных носителей информации и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы собственной безопасности Учреждения.

2. Порядок, обеспечивающий безопасную работу на автоматизированном рабочем месте и с носителями информации:

2.1. Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.

2.2. За эксплуатацию автоматизированной системы (далее - АС) отвечает ответственный за обработку персональных данных (защиту информации) и непосредственно сотрудник, работающий на нём.

2.3. На автоматизированных рабочих местах должно использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности.

2.4. На работающем автоматизированном рабочем месте, в обязательном порядке должно быть установлено антивирусное средство защиты. Ответственность за это несет конкретный, работающий на нём сотрудник, а также Ответственный за обработку персональных данных (защиту информации). Средства антивирусной защиты информации устанавливаются при вводе в эксплуатацию автоматизированного рабочего места или при их плановой замене.

2.5. Эксплуатируемые средства антивирусной защиты информации, устанавливаемые на автоматизированное рабочее место, входящее в состав государственной (муниципальной) информационной системы должны иметь сертификат соответствия ФСТЭК России.

2.6. Периодически, не реже 1 раза в неделю, Пользователем должна быть проведена антивирусная проверка на своём автоматизированном рабочем месте на возможное наличие компьютерного вируса.

2.7. Пользователь обязан проводить антивирусный проверку любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях информации.

2.8. Порядок и правила эксплуатации средств антивирусной защиты (САВЗ) информации определяется в руководстве пользователя на средство антивирусной защиты информации поставляемой вместе с САВЗ.

2.9. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- сообщить об обнаружении вируса Ответственному за обработку персональных данных (защиту информации);
- в дальнейшем действовать по указанию Ответственного за обработку персональных данных (защиту информации).

3. **Ответственность**

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Пользователя, обрабатывающего персональные данные.

Пользователь и Ответственный за обработку персональных данных (защиту информации) несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Приложение № 7
к приказу от 10.07.2017 № 369

Инструкция по уничтожению персональных данных (конфиденциальной информации) в МБОУ «СОШ № 6»

1.Основные положения

1.1. Настоящая Инструкция определяет порядок уничтожения конфиденциальной информации (персональных данных) (далее – персональных данных) и носителей, содержащих персональные данные в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 6» (далее – Учреждение).

1.2. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

1.3. Целью настоящей Инструкции является соблюдение конфиденциальности персональных данных в Учреждении.

1.4. Уничтожению подлежат персональные данные, обрабатываемые автоматизированными средствами обработки информации и обрабатываемые на бумажных носителях.

1.5. Порядок уничтожения персональных данных и носителей, содержащих персональные данные, определяет этапы организации уничтожения, порядок назначения ответственных за уничтожение, порядок оформления распорядительных и отчётных документов по уничтожению персональных данных и носителей, содержащих персональные данные.

2. Условия уничтожения персональных данных (конфиденциальной информации)

2.1. Персональные данные (конфиденциальная информация) уничтожаются в следующих случаях:

при достижении целей обработки информации;

в случае решения субъекта персональных данных;

в случае недостоверности персональных данных (конфиденциальной информации);

в случае вывода из пользования носителей, содержащих персональные данные.

2.2. Решение на уничтожение персональных данных (конфиденциальной информации) и носителей персональных данных принимает руководитель Учреждения.

3. Назначение комиссии

3.1. Приказом руководителя Учреждения создаётся постоянно действующая комиссия для уничтожения документов, содержащих персональные данные (конфиденциальную информацию).

3.2. В состав комиссии должны входить не менее двух сотрудников (работников) Учреждения, имеющих доступ к персональным данным (конфиденциальной информации) и состоять из председателя и членов комиссии.

3.3. Состав комиссии утверждает руководитель Учреждения. Заместитель руководителя Учреждения (ответственный) подаёт предложения, руководитель Учреждения утверждает состав членов комиссии.

3.4. Как правило, комиссия для уничтожения документов, содержащих персональные данные, назначается на год или на больший срок по решению руководителя Учреждения.

4. Процедура уничтожения персональных данных (конфиденциальной информации) и носителей, содержащих персональные данные (конфиденциальную информацию).

4.1. Уничтожение персональных данных и носителей, содержащих персональные данные, осуществляется в присутствии членов комиссии в помещении, допущенном для обработки персональных данных.

4.2. Каждый документ и носитель, содержащие персональные данные (конфиденциальную информацию) рассматриваются отдельно на предмет значимости и необходимости его уничтожения.

4.3. Для уничтожения электронных документов, содержащих персональные данные (конфиденциальную информацию) обрабатываемые в АС применяется программное обеспечение прошедшее в установленном порядке сертификацию ФСТЭК России. В информационных системах персональных данных (иных информационных системах) допускается использование программы типа «FileShredder» или программного средства безвозвратного удаления электронных документов с возможностью применения алгоритмов многоразового перезаписывания информации на носителе персональных данных.

4.4. Уничтожение физических носителей, содержащих персональные данные (конфиденциальную информацию), осуществляется методом нанесения нескольких механических воздействий специальным инструментом, например, металлическим бруском, насаженным под прямым углом на рукоятку или другим аналогичным инструментом. Применение указанного метода для носителя должно продолжаться до тех пор, пока

визуально не будет установлено разрушение носителя информации. Для жёсткого магнитного диска – это пластины с магнитным покрытием.

4.5. Допускается уничтожение носителей информации: с использованием химических, термо-химических реактивов, в специально отведенном для этого месте; путем сожжения (термической обработки).

5.Порядок оформления отчётных документов.

5.1.По окончании процедуры уничтожения, составляется Акт об уничтожении персональных данных (конфиденциальной информации).

5.2.Акт об уничтожении персональных данных (конфиденциальной информации) подписывается членами комиссии по уничтожению персональных данных (конфиденциальной информации).

Приложение № 8
к приказу от 10.07.2017 № 369

ИНСТРУКЦИЯ
по работе с электронной подписью в МБОУ «СОШ № 6»

1. Общие положения

Инструкция разработана для сотрудников Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», «Инструкцией 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», утвержденной приказом ФАПСИ РФ от 13 июня 2001 г. № 152, Приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и иными нормативными правовыми актами Российской Федерации.

1. Пользователи средствами электронной подписи обязаны:

обеспечить сохранность, функционирование и безопасность средств электронной подписи (далее – средства ЭП);

обеспечить сохранность личных печатей, ключей от помещений и хранилищ;

обеспечить конфиденциальность ключей электронных подписей;

выполнять указания ответственного пользователя;

не разглашать информацию об средствах ЭП, ключевых документах к ним;

не допускать снятие копий с ключевых документов;

не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

не допускать записи на ключевой носитель посторонней информации;

не допускать установки ключевых документов в другие ПЭВМ;

под расписку в журнале поэкземплярного учета получать экземпляры средств электронной подписи (далее - пользователей), эксплуатационной и технической документации к ним, ключевых документов;

на время отсутствия пользователей средствами ЭП, оборудование, функционирующее со средствами ЭП, должно быть выключено, отключено от линии связи и убрано (при технической возможности) в опечатываемые хранилища;

по окончании рабочего дня закрыть и сдать под охрану: помещения в которых осуществляется работа со средствами ЭП; сейфы (металлические шкафы, хранилища) предназначенные для хранения средств ЭП. Находящиеся в пользовании ключи от сейфов (металлических шкафов, хранилищ) сдать под расписку в соответствующем журнале пользователю, ответственному за обработку информации содержащей персональные данные (далее – ответственный пользователь);

сдать и списать со своего лицевого счёта средства ЭП, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств ЭП;

немедленно сообщить ответственному пользователю о возможном несанкционированном проникновении в помещения, сейфы (металлические шкафы, хранилища) посторонних лиц;

немедленно сообщить ответственному пользователю о попытках посторонних лиц получить сведения об используемых ЭП или ключевых документах к ним;

немедленно уведомить ответственного пользователя о фактах утраты или недостачи средств ЭП, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2. Ответственный пользователь обязан:

обеспечить функционирование и безопасность средств ЭП;

осуществлять текущий контроль за организацией и обеспечением функционирования средств ЭП;

осуществлять поэкземплярный учет используемых средств ЭП, эксплуатационной и технической документации к ним, носителей персональных данных;

осуществлять учет лиц, допущенных к работе со средствами ЭП;

осуществлять контроль за соблюдением условий использования средств ЭП;

осуществлять разбирательство и составление заключений по фактам нарушения условий хранения и использования средств ЭП;

осуществлять допуск пользователей к работе со средствами ЭП по решению руководителя Учреждения;

вести на каждого пользователя лицевой счет и регистрировать числящиеся за ними средства ЭП, эксплуатационную и техническую документацию к ним;

выдавать пользователям средства ЭП, эксплуатационную и техническую документацию к ним и ключевые документы под расписку в соответствующем журнале поэкземплярного учета;

по окончании рабочего дня закрыть и опечатать помещения, сейфы (металлические шкафы, хранилища).

3. Учёт средств электронной подписи.

Средства ЭП, эксплуатационная и техническая документация подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

Средства ЭП, эксплуатационная и техническая документация числящиеся за пользователями подлежат регистрации на их лицевых счетах.

Средства ЭП, эксплуатационная и техническая документация выдаются пользователям под расписку в соответствующем журнале поэкземплярного учета.

4. Хранение средств электронной подписи.

Хранение средств ЭП, эксплуатационной и технической документации должно осуществляется в сейфах или хранилищах, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания замочных скважин.

Хранение действующих и резервных средств ЭП, эксплуатационной и технической документации должно осуществляется раздельно.

5. Передача средств электронной подписи.

Передача по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования средств ЭП осуществляется только с использованием средств ЭП.

Передача средств ЭП, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями и (или) ответственным пользователем под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями должна быть санкционирована ответственным пользователем.

6. Уничтожение средств электронной подписи.

Уничтожение средств ЭП (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) средств ЭП (исходной ключевой информации) без повреждения ключевого носителя.

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

Средства ЭП уничтожают по решению руководителя, владеющего средствами ЭП, с уведомлением организации, ответственной за ведение поэкземплярного учета средств ЭП.

Электронные записи ключевой информации выведенные из действия уничтожаются пользователями этих средств самостоятельно под расписку в техническом (аппаратном) журнале.

7. Компрометация и потеря средств электронной подписи.

При наличии оснований полагать, что конфиденциальность ключа нарушена (скомпрометирована), использование ключа электронной подписи – запрещено.

В случае компрометации средств ЭП необходимо уведомить удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

О нарушениях, которые могут привести к компрометации средств ЭП, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи обязаны сообщать ответственному пользователю (руководителю организации).

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации средств ЭП, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях потери, недостачи или не предъявления ключевых носителей, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

8. Организация режима охраны в помещениях где проводится работа с электронной подписью.

Организация режима доступа в помещения должна исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними ведущихся там работ.

Помещения, как правило, должны быть оснащены охранной сигнализацией. Режим охраны помещений должен предусматривать периодический контроль за состоянием технических средств охраны.

Входные двери помещений должны быть прочными, с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Входные двери должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения, под расписку в журнале учета. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе ответственного пользователя.

Окна помещений должны быть защищены от просмотра извне. Окна помещений, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками (ставнями) и системой предотвращения просмотра извне.

Аппаратные средства, с которыми осуществляется штатное функционирование средств ЭП, а также аппаратные и аппаратно-программные

средства ЭП должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

Приложение № 9
к приказу от 10.07.2017 № 369

ИНСТРУКЦИЯ
по защите от несанкционированного доступа к персональным данным (конфиденциальной информации) в МБОУ «СОШ № 6»

I. Общие положения

1.1. Настоящая инструкция определяет права, обязанности и ответственность пользователей при работе в автоматизированной системе персональных данных (далее - АС) с целью защиты от несанкционированного доступа (далее - НСД) к персональным данным. Также инструкция определяет функции, задачи и порядок эксплуатации пользователями средств вычислительной техники (далее - СВТ), входящих в состав АС.

1.2. Пользователями АС являются сотрудники (работники) Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 6» (далее - Учреждение), допущенные к обработке персональных данных согласно утвержденному руководителем Учреждения Списку лиц.

1.3. Перед началом работ пользователь должен ознакомиться с содержанием следующих документов:

– Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– эксплуатационной документацией на установленные в АС средства защиты;

– нормативными актами Учреждения в области защиты персональных данных.

1.4. Оперативный контроль за действиями пользователей при работе в АС осуществляет ответственный за обработку персональных данных (Администратор автоматизированной системы, локальной сети и т.п.) Учреждения, который имеет право приостановить обработку информации в случае выявления нарушений.

II. Обеспечение защиты от несанкционированного доступа

2.1. Пользователю АС устанавливаются соответствующие его полномочиям атрибуты управления доступом к ресурсу (диску, каталогу, файлу, принтеру, коммуникационным портам и т.п.).

2.2. Начальными процедурами управления регистрацией пользователей в системе являются процедуры идентификации и аутентификации. Каждому пользователю АС ответственный за обработку персональных данных (Администратор информационной системы (локальной сети)) назначает персональный идентификатор и пароль.

2.3. Устройства отображения и вывода информации (дисплей, принтер) в процессе эксплуатации АС должны устанавливаться с учетом исключения несанкционированного доступа к выводимой информации лицами, не имеющими к ней соответствующего допуска. В случае невозможности выполнения указанных требований по размещению технических средств АС, должны приниматься дополнительные организационные и технические меры по исключению несанкционированного доступа к информации. Изменение места расположения основных технических средств АС без согласования с Ответственным (Администратором) запрещено.

2.4. При эксплуатации АС должно быть обеспечено непрерывное функционирование установленных средств защиты информации от несанкционированного доступа и антивирусного программного обеспечения.

2.5. В процессе работы с персональными данными (конфиденциальной информацией) должны использоваться исключительно штатные технические средства АС.

2.6. Внесение пользователем самостоятельных изменений в аппаратно-программную конфигурацию АС **категорически запрещено.**

III. Права и обязанности пользователя

3.1. Пользователь обязан:

- выполнять требования настоящей инструкции, а также требования организационно-технических и распорядительных документов в области защиты персональных данных;
- соблюдать правила работы со средствами защиты информации, установленными в АС, согласно утвержденной инструкции по эксплуатации этих средств;
- докладывать Ответственному (Руководителю, Администратору) о фактах нарушения требований инструкций по обеспечению защиты информации;
- знать штатные режимы работы программного обеспечения;
- использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- помнить личные пароли и идентификаторы;
- не допускать использования в АС неучтенных машинных носителей (флеш-дисков, CD, DVD, дискет);

- при поступлении необходимой для работы информации на неучтенных электронных носителях из сторонних организаций осуществлять регистрацию использования данных носителей в соответствующем журнале.

3.2. Пользователь имеет право:

- использовать штатные программно-аппаратные средства АС для решения профессиональных задач;
- обращаться к Ответственному (Администратору) с просьбой об оказании технической и методической помощи в работе по обеспечению безопасности информации;
- обращаться к Ответственному (Администратору) с требованием о прекращении обработки ПДн в случаях нарушения установленной технологии обработки информации или выхода из строя средств защиты.

3.3. Пользователю **запрещается:**

- разглашать сведения о применяемых средствах защиты персональных данных (конфиденциальной информации) и содержание документов лицам, не имеющим отношения к проводимым работам;
- использовать в АС неучтенные машинные носители информации или не предназначенные для хранения персональных данных (конфиденциальной информации) каталоги рабочих станций;
- использовать учтенные служебные машинные носители информации для хранения информации, не имеющей отношения к выполняемым работам;
- оставлять учтенные служебные машинные носители информации и документы бесконтрольно;
- разрабатывать и/или использовать программы, с помощью которых можно получить несанкционированный доступ к персональным данным (конфиденциальной информации), разработка и использование которых квалифицируется как попытка преднамеренного несанкционированного доступа к обрабатываемым данным;
- изменять или тиражировать установленное в АС программное обеспечение;
- фиксировать на любых носителях персональный пароль;
- передавать персональный идентификатор сторонним лицам;
- подключать к СВТ нештатные блоки и устройства;
- проводить обработку информации в АС при неработоспособных или отключенных средствах защиты информации.

IV. Порядок работы пользователя в АС

4.1. Перед началом обработки информации пользователь обязан убедиться в отсутствии в помещении посторонних лиц, а также в том, что средства защиты включены и работоспособны.

4.2. Осуществить вход в АС используя личные идентификатор и пароль.

4.3. После окончания работы в АС пользователь обязан произвести полное выключение СВТ.

4.4. В случае поступления из сторонних организаций необходимой для работы информации на неучтенных электронных носителях пользователю необходимо:

- зафиксировать использование поступившего электронного носителя информации в соответствующем журнале;
- перед использованием произвести проверку электронного носителя на наличие вредоносного программного обеспечения с помощью установленных средств антивирусного контроля;
- при выявлении наличия вредоносного программного обеспечения незамедлительно прекратить использование электронного носителя и доложить Ответственному (Администратору) о данном факте.

V. Ответственность пользователя

5.1. Пользователь отвечает за соблюдение правил эксплуатации АС, сохранность информации, документов и электронных носителей информации, с которыми он работает.

5.2. Пользователь несет **персональную ответственность** за:

- соблюдение установленных требований по безопасности информации при обработке, копировании (уничтожении) персональных данных;
- использование неучтенных электронных носителей информации;
- несоблюдение правил использования электронных носителей информации, поступающих из сторонних организаций;
- правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него;
- сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты персональных данных;
- выполнение указаний Ответственного (Администратора), касающихся работы в АС и защиты информации;
- обеспечение сохранности и неразглашение сведений о парольной защите АС;
- соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и/или состав технических средств обработки и защиты информации, состав используемого в АС программного обеспечения) в соответствии с организационно-технической документацией на АС;
- неисполнение или ненадлежащее исполнение обязанностей, предусмотренных настоящей инструкцией, в пределах, установленных законодательством Российской Федерации, а также за действия (бездействия), нарушающие права и законные интересы граждан и юридических лиц.

Приложение № 10
к приказу от 10.07.2017
№ 369

ИНСТРУКЦИЯ
по защите персональных данных (конфиденциальной информации) в МБОУ «СОШ № 6»

1. Общие положения

1.1. Целью настоящей инструкции является четкая регламентация эффективных мер защиты и надежного сохранения информации согласно Политики информационной безопасности (Политики обработки персональных данных) (далее - Политики) в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 6» (далее - Учреждение) и обрабатываемой в автоматизированной системе (далее - АС). Мероприятия защиты проводятся для обеспечения физической и логической целостности, а также для предупреждения несанкционированного получения, распространения и модификации информации. Меры защиты подразумевают обязательное наличие ответственного за защиту информации в АС лица, выработку и неукоснительное соблюдение организационных мер.

1.2. Термины и определения

Авторизованный субъект — субъект АС, пользовательские функции которого, а также права и обязанности по отношению к данного уровня ресурсам и информации определены его должностной инструкцией, либо другими административными актами.

АРМ — автоматизированное рабочее место, персональное, созданное на основе персональной электронной вычислительной машины.

Доступность ресурса — обеспечение беспрепятственного доступа к нему авторизованного субъекта АС.

Конфиденциальность ресурса – свойство ресурса быть доступным только авторизованному субъекту АС, и одновременно быть недоступным для неавторизованного субъекта или нарушителя.

Ресурс — компонент АИС (аппаратные средства, программное обеспечение, данные), в отношении которого необходимо обеспечивать безопасность, т. е. конфиденциальность, целостность и доступность.

Субъекты АС — пользователи, технический персонал,

обеспечивающий работу системы, администрация АС, администрация Учреждения и контролирующие службы.

Целостность ресурса — обеспечение его правильности и работоспособности в любой момент времени.

2. Допуск к использованию ресурсов

Допуск к работе с конфиденциальными документами (конфиденциальной информацией) имеют сотрудники Учреждения, в том числе и находящиеся на испытательном сроке, которые: ознакомлены под роспись с Политикой Учреждения, настоящей Инструкцией, другими организационно-распорядительными документами; подписали Соглашение о неразглашении персональных данных (конфиденциальной информации).

Запрещается допускать к работе с конфиденциальными документами (персональными данными) других лиц, кем бы они не являлись, без письменного разрешения руководителя Учреждения.

Под допуском подразумевается официальное присвоение сотруднику Учреждения конкретного статуса, дающего ему возможность использовать ресурсы АС и обмена данными на заданном четко категорированном уровне и в ограниченном должностными обязанностями (не превышающем его непосредственные задачи) объеме.

Обязанности по присвоению статуса возлагаются на ответственного за защиту персональных данных (Администратора автоматизированной системы, локальной сети, объекта информатизации и т.п.) или специально назначенного сотрудника. При этом он должен, руководствоваться принципами разумного ограничения возможностей и разграничения доступа к различным информационным массивам. Он несет ответственность за регистрацию и предоставление (изменение) полномочий.

Все пользователи подлежат учету по категориям установленного допуска и другим системным параметрам.

3. Доступ к использованию ресурсов. Регистрации пользователей

Доступ к использованию ресурсов имеют сотрудники, получившие допуск определенного уровня, соответствующий, как правило, занимаемой должности, с соблюдением всей процедуры оформления допуска, и| зарегистрированные у Администратора (Ответственного должностного лица).

3.1. Специальные вопросы доступа к использованию ресурсов:

3.1.1. Определение расширенного доступа, т. е. привилегий системного Администратора.

Привилегии Администратора, кроме тех сотрудников, которым должностными обязанностями предписано выполнять работы по эксплуатации и ремонту ресурсов, имеют право получать представители руководства Учреждения и другие должностные лица по согласованию со специально назначенным сотрудником и с разрешения руководителя Учреждения. Все лица, имеющие права Администратора, подлежат

отдельному учету.

3.1.2. Доступ к работе с авторским (лицензионным) программным обеспечением (далее - ПО).

При наличии в АС или ее компонентах авторских либо лицензионных программ они должны быть соответствующим образом, ясным для пользователя, помечены; там же должны быть указаны все ограничения, связанные с работой с данным ПО.

Однозначно (по умолчанию) запрещается их копирование.

4. Хранение носителей персональных данных (конфиденциальной информации) в АС

За организацию хранения и сохранность персональных данных (конфиденциальной информации) Учреждения отвечает его руководитель. Контроль за выполнением мероприятий осуществляет Ответственный за обработку персональных данных (далее – ПДн) (защиту информации). Общий процесс хранения регламентирован в локальных актах Учреждения.

Машинные носители персональных данных (конфиденциальной информации) хранятся в недоступном для посторонних лиц месте (сейф, металлический шкаф, файл-бокс), исключающем несанкционированный доступ и пользование ими.

Сейф (-ы) (несгораемый металлический шкаф) должен быть постоянно закрыт на ключ.

Один комплект ключей от сейфа(-ов) — у ответственного сотрудника Учреждения. Остальные комплекты должны храниться в сейфе ответственного за обработку персональных данных (защиту информации) (далее – Ответственного) в опечатанном (или иным способом обеспечивающим целостность) пенале. Порядок опечатывания и сдачи под охрану сейфов определяется локальными актами Учреждения.

5. Защита ресурсов АС

5.1. В целях обеспечения надежной охраны материальных ценностей вычислительных средств, сетей и данных конфиденциального характера, своевременного предупреждения и пресечения попыток несанкционированного доступа к ним устанавливается определенный режим деятельности, соблюдение которого обязательно для всех сотрудников, посетителей и клиентов. Порядок его регламентации устанавливается в локальных актах Учреждения.

При этом: запрещен несанкционированный внос-вынос машинных накопителей информации (дискет, CD-R, USB накопителей, переносных накопителей на твердых магнитных дисках и т.п.); запрещено кому бы то ни было, кроме специально уполномоченных сотрудников, перемещать компьютерную технику и комплектующие без соответствующих сопроводительных документов (служебных записок или накладных), согласованных с Ответственным.

5.2. Аппаратная защита ресурсов проводится исходя из потребностей

Учреждения в реальном сохранении своей информации ограниченного доступа по назначению руководства и может включать в себя:

- использование источников бесперебойного или автономного питания;
- поддержание единого времени;
- изъятие с АРМов необязательных дисководов, факсимильных и модемных плат и т.п.;
- проведение периодических «чисток» АРМов и общих системных директорий на файл- серверах и серверах АС.

5.3. Программная защита ресурсов также проводится исходя из потребностей Учреждения в реальном сохранении своей информации ограниченного доступа по назначению руководства и может включать в себя:

- установку входных паролей на клавиатуру АРМ;
- установку сетевых имен-регистраторов и паролей для доступа к работе в АС;
- обеспечение восстановления информации после несанкционированного доступа;
- обеспечение антивирусной защиты (в т. ч. от неизвестных вирусов) и восстановления информации, разрушенной вирусами;
- контроль целостности программных средств обработки информации;
- проведение периодической замены (возможно принудительной) всех паролей и регистрационных имен;
- использование расширенных систем аутентификации.

5.4. Техническая защита ресурсов включает в себя защиту АРМ, помещений и всех коммуникаций от устройств съема и передачи информации.

6. Копирование персональных (конфиденциальных) данных

Согласно Политики Учреждения копирование информации (персональных данных) запрещено, если это не оговорено дополнительно, т.е. запрещено копирование в любые другие, несанкционированные виртуальные области и на прочие носители. Порядок получения разрешения на копирование определен локальными актами Учреждения.

7. Архивирование персональных данных (конфиденциальной информации)

Архивирование текущей конфиденциальной информации (персональных данных) в АС проводится пользователями не реже чем один раз в неделю. Архивирование должно также предусматривать восстановление разрушенной архивной информации, даже при ее значительных потерях. С этой целью делаются ежедневные, еженедельные и т. д. архивные копии. Копии на твердых носителях архивируются и хранятся согласно Политики Учреждения.

8. Уничтожение данных, содержащих персональные данные (конфиденциальную информацию)

Процесс создания конфиденциальных документов и обработки данных в АС после получения печатных и прочих копий для дальнейшей работы должен при необходимости завершаться очисткой памяти и рабочих областей на машинных носителях. Для уничтожения персональных данных (конфиденциальной информации) назначается специальная комиссия. Уничтожения информации проводится согласно Инструкции с составлением Акта.

9. Передача персональных данных (конфиденциальной информации)

Порядок передачи персональных данных (конфиденциальной информации) на различных носителях регламентируется должностными инструкциями, а также Политикой.

Все факты получения информации должны быть надежно подтверждены.

На Ответственного также возлагаются обязанности по правильному управлению потоками данных с целью предотвращения записи персональных данных (конфиденциальной информации) на посторонние носители информации.

10. Доведение специальных правил обращения с персональными данными (конфиденциальной информацией) в АС до персонала

Доведение данной инструкции до персонала проводится Ответственным или руководителем Учреждения при ознакомлении сотрудника с Политикой. Повторное ознакомление и разъяснение данной Инструкции проводится специально назначенным ответственным лицом Учреждения при предоставлении доступа, за что сотрудник расписывается в графе «Ознакомлен» журнала ознакомления или в ином локальном документе Учреждения, например: «Журнале учета доведения нормативных документов».

Все изменения и дополнения настоящей Инструкции официально доводятся до всего персонала (сотрудников) Учреждения.

11. Защита персональных данных (конфиденциальной информации) пользователями ресурсов

Пользователь лично отвечает за понимание и соблюдение правил безопасности. Если ему не понятны функции по защите информации, он обязан спросить Ответственного. Запрещаются любые действия, направленные на:

- получение доступа к информации о пользователях;
- вскрытие и использование чужих регистрационных имен (логинов) и паролей;
- тестирование и разрушение служб сети;
- просмотр всех доступных для чтения файлов на сетевых устройствах, не принадлежащих пользователю;

- модификация файлов, которые не являются собственными, даже если они имеют право записи в них;

- вскрытие блоков и комплектующих, а также изменение физической конфигурации;

- использование одного и того же регистрационного имени и пароля;

- раскрывание и передача кому бы то ни было своего регистрационного имени и(или) пароля.

При выборе пароля Пользователь **обязан**:

- не использовать регистрационное имя в каком бы то ни было виде;

- не использовать имя, фамилию или отчество в каком бы то ни было виде, имена супруга или детей, а также другую информацию, которую легко получить (номер телефона, дату рождения и пр.);

- не использовать пароль из одних цифр или их одних букв, а также короче шести символов;

- использовать пароль с буквами из разных регистров, с небуквенными символами;

- использовать пароль, который легко запомнить, чтобы не возникало желания записать его, а также который можно легко набрать на клавиатуре, не глядя на нее.

Пользователю при работе с персональными данными (конфиденциальной информацией) **запрещено**, отлучаясь из помещения, оставлять свой АРМ без блокировки операционной системы (рабочего стола). Рабочие файлы и базы данных, содержащие конфиденциальную информацию, пользователь обязан хранить в установленных местах.

В целях выявления незаконного использования регистрационного имени Пользователь должен контролировать свое время входа и выхода в АС и проверять последние команды и, если параметры отличаются, обязан немедленно сообщить об этом Ответственному (Администратору).

Пользователь обязан немедленно сообщать о возникших проблемах и ошибках, которые не могут быть устранены путем перезагрузки компьютера после отключения от системных служб. Производить любые попытки восстановления работы компьютера при наличии соединения с системой **категорически запрещается**.

12. Ответственность за нарушение правил обращения персональных данных (конфиденциальной информации) в АС

За умышленное невыполнение или халатное исполнение правил обращения с персональными данными (конфиденциальной информацией), изложенных в данной Инструкции, если это повлекло за собой нанесение материального ущерба, виновное лицо наказывается в административном (дисциплинарном) порядке. Размер и кратность возмещения ущерба определяется в соответствие с законодательством РФ, после проведения внутреннего расследования.

По итогам проведения внутреннего расследования инцидентов информационной безопасности, руководителем Учреждения могут быть инициированы ходатайства в надзорные органы о возбуждении уголовного

или гражданского судебного делопроизводства.

13. Контроль

Контроль за выполнением требований Настоящей Инструкции сотрудниками и работниками Учреждения возлагается на Руководителя Учреждения и Ответственного.

Приложение № 11
к приказу от 10.07.2017
№ 369

В муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №6»,
628307, Российская Федерация,
Ханты-Мансийский автономный округ – Югра,
город Нефтеюганск, 8 микрорайон, здание 28.

СОГЛАСИЕ
на обработку персональных данных

Я,

_____

фамилия, имя, отчество (при наличии) родителя (законного представителя)

документ, удостоверяющий личность _____ _____ __
наименование документа, серия, номер
дата выдачи

_____

орган, выдавший документ

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие своей волей и в своем интересе на обработку моих персональных данных, а также персональных данных несовершеннолетнего

_____

фамилия, имя, отчество (при наличии)

которому являюсь

_____

(отцом, матерью, опекуном, попечителем)

муниципальному бюджетному общеобразовательному учреждению «Средняя общеобразовательная школа № 6» (далее – Оператор), расположенному по

адресу: 628307, Российская Федерация, Ханты-Мансийский автономный округ – Югра, город Нефтеюганск, 8 микрорайон, здание 28.

Цель обработки персональных данных:

- обеспечение соблюдения законов и иных нормативных правовых актов Российской Федерации;
- содействие в получении общего образования, дополнительного образования.

Перечень персональных данных, на обработку которых дано настоящее согласие:

- фамилия, имя, отчество родителя и/или законного представителя учащегося;
- данные документа, удостоверяющего личность родителя и/или законного представителя учащегося;
- данные документа, подтверждающего право родителя и/или законного представителя находиться на территории Российской Федерации (для иностранных граждан и лиц без гражданства в Российской Федерации);
- сведения об образовании родителя и/или законного представителя, месте работы, занимаемой должности;
- данные документа о родстве учащегося с родителем и/или законным представителем учащегося;
- сведения о контактных данных родителя и/или законного представителя учащегося;
- фамилия, имя, отчество учащегося;
- данные документа, удостоверяющего личность учащегося (свидетельство о рождении или паспорт);
- сведения о регистрации по месту жительства учащегося;
- сведения о составе семьи учащегося;
- сведения о национальной принадлежности учащегося;
- сведения, необходимые для предоставления учащемуся гарантий и компенсаций, установленных действующим законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);
- данные полиса медицинского страхования учащегося;
- сведения о состоянии здоровья учащегося (медицинская группа здоровья);
- данные ИНН, СНИЛС;
- сведения о контактных данных учащегося.

Перечень действий с персональными данными, на совершение которых дается согласие: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (в том числе передача уполномоченным органам), обезличивание, блокирование, уничтожение персональных данных.

Способы обработки персональных данных:

- на бумажных носителях;
- в информационных системах персональных данных с использованием и без использования средств автоматизации, а также смешанным способом;
- при участии и при непосредственном участии человека.

Срок, в течение которого действует согласие: до достижения цели обработки персональных данных или до момента утраты необходимости в их достижении.

Настоящее согласие может быть отозвано мной путем подачи Оператору письменного заявления об отзыве согласия.

«___» _____ 20___г.

_____(_____)

подпись

инициалы, фамилия

Приложение № 12
к приказу от 10.07.2017 № 369

Согласие на обработку персональных данных

№_____ «_____» _____20___ г.

Я,

_____

фамилия, имя, отчество

документ, удостоверяющий личность _____ _____ _____
наименование документа, серия, номер
дата выдачи

_____

орган, выдавший документ

_____

именуемый в дальнейшем «Субъект персональных данных» свободно, своей волей и в своем интересе разрешает _____,

в лице ответственного за обработку персональных данных далее «Оператор», обработку персональных данных, приведенных в пункте 2 настоящего согласия на следующих условиях:

1. «Субъект персональных данных» дает согласие «Оператору» на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, то есть совершение следующих действий: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», в следующих целях:

- в целях исполнения трудового договора;
- для обеспечения личной безопасности, защиты жизни и здоровья работника;
- в целях ведения финансово-хозяйственной деятельности организации;
- в целях соблюдения прав и законных интересов «Оператора» или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы «Субъекта персональных данных»;

- в целях осуществления научной, литературной или иной творческой деятельности.

2. Перечень персональных данных, передаваемых Оператору на обработку (ненужное вычеркнуть):

- дата и место рождения;
- сведения об образовании (образовательное учреждение, время обучения, присвоенная квалификация);
- сведения о местах работы (город, название организации, должность, сроки работы);
- сведения о семейном положении, детях (фамилия, имя, отчество, дата рождения);
- сведения о месте регистрации, проживании;
- контактная информация;
- сведения о наличии (отсутствии) судимости;
- паспортные данные;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей);
- сведения о постановке на налоговый учет (ИНН);
- сведения о регистрации в Пенсионном фонде (номер страхового свидетельства);
- сведения об открытых банковских счетах;
- отношение к воинской обязанности, сведения о воинском учете;
- выполняемая работа с начала трудовой деятельности;
- биографические сведения;
- владение иностранными языками и языками народов Российской Федерации;
- сведения о наличии (отсутствии) заболеваний, подтвержденные медицинским учреждением;
- результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования.

3. В соответствии с пунктом 4 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных.

4. Срок действия данного согласия устанавливается на период:
с_____ по ___

5. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

6. В случае отзыва согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

7. После прекращения трудовых отношений персональные данные хранятся в _____ в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации.

8. Персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных на Оператора законодательством Российской Федерации и трудовыми (иными) договорами функций, полномочий и обязанностей.

Данные об операторе персональных данных:
Наименование организации:
_____
Адрес оператора:
_____
Ответственный за обработку ПДн
_____

Субъект персональных данных:
Фамилия, имя, отчество:_____
Паспорт: серия _____ номер _____
Выдан:
_____
_____
Дата выдачи: «___»_____ 20___ г.
Адрес:
_____
_____
_____
_____

«___» _____ 20___ г. _____
_____
дата подпись Ф.И.О.