КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ «МЕГИОНСКАЯ ШКОЛА ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ»
(КОУ «МЕГИОНСКАЯ ШКОЛА ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ»)

УТВЕРЖДАЮ
Директор КОУ «Мегионская школа для обучающихся с ограниченными возможностями здоровья»
_____ Е.В. Масленников
«06» 02 2020 г. № 39-О

Положение
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных КОУ «Мегионская школа для обучающихся с ограниченными возможностями здоровья»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных работников и обучающихся образовательного учреждения и гарантии их конфиденциальности.

1.2. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

1.3.Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе криптографические средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

1.4.Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

1.5. 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 (далее - ИСПДн);

- 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.

2.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. В школе приказом директора 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. Учреждение создает в пределах своих полномочий, установленных в соответствии с федеральными законами, городские ИСПДн, в целях обеспечения реализации прав объектов персональных данных.

3.2. В школе на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента РФ от 06.031997 №188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - конфиденциальной информации) и перечень информационных систем персональных данных (приложение 1).

3.3. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых 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 постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2. Оператором осуществляется классификация информационных систем персональных данных в соответствии с приказом ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» в зависимости от категории обрабатываемых данных и их количества.

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 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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 классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, и других нормативных и методических документов;

– настроенных средств защиты от несанкционированного доступа, 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.Порядок обработки персональных данных без использования средств автоматизации

5.1. 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.

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

5.3. 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.

5.4. 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.

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

5.6. 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.

5.7. Электронные носители информации, содержащие персональные данные, учитываются в Журнале учёта электронных носителей персональных данных (приложение 2).

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

5.8. 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.

5.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и

опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.10. 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).

6.Основные группы угроз, на противостояние которым направлены цели и требования безопасности

6.1. Угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при её обработке и хранении.

6.2. Угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся.

6.3. Угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца (субъекта персональных данных).

6.4. Угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам.

6.5. Угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств.

6.6. Угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоев (отказов) программного и аппаратного обеспечения.

6.7. Угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения.

6.8. Угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

7.Функциональные требования безопасности

- требования к осуществлению аудита безопасности;
- требования к обеспечению подлинности субъектов обмена информацией;
- требования к криптографической поддержке;
- требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;
- требования к идентификации и аутентификации пользователей ИСПДн;
- требования к управлению безопасностью;
- требования к защите системы безопасности.

8. Основные функциональные возможности ИСПДн, связанные с обеспечением безопасности (защитой информации)

8.1. Защита данных пользователя ИСПДн должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к ИСПДн, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В ИСПДн доступ к информации должен быть разрешен только уполномоченным на это Пользователям. Модель защиты ИСПДн должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в ИСПДн, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться. Изменение их значений должно быть обеспечено только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

8.2. Аудит событий безопасности

ИСПДн должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ИСПДн или доступа к защищаемой информации. В частности, определяя политику аудита, уполномоченный администратор ИСПДн должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к ИСПДн. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору ИСПДн. Просмотр журналов регистрации событий аудита должен выполняется с использованием средств ИСПДн (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

8.3. Идентификация и аутентификация

ИСПДн должна требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к ИСПДн с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. ИСПДн должна поддерживать аутентификацию Пользователей вместе с их авторизацией. Предусматривается, что авторизация Пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам.

ИСПДн должна обеспечивать хранение паролей в преобразованном формате. ИСПДн должна предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

ИСПДн должна предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором ИСПДн или по истечении времени действия, заданного для счетчика блокировки.

8.4. Защита системы безопасности

ИСПДн должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций системы безопасности ИСПДн. Возможность осуществления

периодического тестирования среды функционирования ИСПДн (аппаратной части) и собственно самих функций системы безопасности ИСПДн должно обеспечивать поддержание уверенности администратора ИСПДн в целостности и корректности функционирования функций системы безопасности.

9. Основные функциональные возможности повышения надежности

ИСПДн должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

9.1. Резервное копирование данных

В ИСПДн должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

9.2. Восстановление системы

Функциональные возможности восстановления системы должны позволять возвращать ИСПДн в состояние, предшествующее сбою. При этом в ИСПДн не должно происходить потери (либо потери должны быть минимальны) и искажения данных.

9.3. Средства администрирования, управления и поддержки

В состав ИСПДн должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

10. Среда безопасности ИСПДн

10.1. Модели угроз, характерные для ИСПДн

10.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемое свойство безопасности – конфиденциальность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.

10.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).

Источники угрозы – внешний злоумышленник.

Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба образовательному учреждению.

10.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.

Источники угрозы – программное и аппаратное обеспечение.

Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучаемых.

Нарушаемое свойство безопасности – доступность, достоверность.

Возможные последствия реализации угрозы – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.

10.1.4. Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.

Источники угрозы – программное и аппаратное обеспечение, персонал образовательного учреждения.

Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.

Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД, связанные с возможностью нарушения согласованности.

Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.

Нарушаемые свойства безопасности активов – достоверность, целостность.

Возможные последствия реализации угрозы – рассогласование в персональных данных работников и обучаемых, хранимых в БД, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба образовательному учреждению.

10.1.5. Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в ИСПДн, без согласия субъекта персональных данных или окончания срока действия такого согласия.

Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

Способ (метод) реализации угрозы – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением ИСПДн.

Используемые уязвимости – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

Вид информации, потенциально подверженной угрозе – персональные данные обучающихся.

Нарушаемые свойства безопасности – конфиденциальность.

Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.

10.1.6. Внедрение в информационную систему образовательного учреждения вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.

Источники угрозы – внутренние пользователи и персонал образовательного учреждения, внешние системы.

Способ (метод) реализации угрозы – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

Вид информации, потенциально подверженной угрозе – программное обеспечение информационной системы образовательного учреждения.

Нарушаемое свойство безопасности активов – целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

10.1.7. Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему образовательного учреждения, осуществляемых из внешних систем.

Источники угрозы – внешние злоумышленники, внешние системы.

Способ (метод) реализации угрозы – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от несанкционированных внешних воздействий.

Вид информации, потенциально подверженной угрозе – программно-аппаратное обеспечение информационной системы образовательного учреждения.

Нарушаемые свойства безопасности активов – конфиденциальность, целостность.

Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы образовательного учреждения, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

10.2. Политика и цели безопасности для ИСПДн

ИСПДн должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося на обработку предоставленных им в образовательное учреждение своих персональных данных.

2. Должна быть обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).

3. Должна быть обеспечена возможность безопасного восстановления ИСПДН после сбоев и отказов программного обеспечения и оборудования.

4. Должна быть обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.

5. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора ИСПДН о любых событиях, относящихся к безопасности ИСПДН.

6. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы образовательного учреждения, доступных только уполномоченным администраторам.

7. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.

8. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.

10.3. Политика и цели безопасности для среды функционирования ИСПДН

Среда функционирования ИСПДН должна обеспечить следование приведенным ниже правилам безопасности:

10.3.1.Должна быть обеспечена инженерно-техническая укреплённость объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.

10.3.2.Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть оборудованы системой охранной сигнализации.

10.3.3.Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.

10.3.4.На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.

10.3.5.Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.

10.3.6.На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования образовательного учреждения.

10.3.7.Должны быть обеспечены установка, конфигурирование и управление программно-аппаратными средствами ИСПДн в соответствии с руководствами и согласно оценённым конфигурациям.

10.3.8.Персонал, ответственный за администрирование ИСПДн, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

10.3.9.Уполномоченные на работу с ИСПДн операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на ИСПДн, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

11. Проведение работ по обеспечению безопасности персональных данных

11.1.Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение 3). Внутренние проверки режима защиты ПДн КОУ «Мегионская школа для обучающихся с ограниченными возможностями здоровья» проводятся в соответствии с Планом внутренних проверок режима защиты персональных данных (Приложение 4).

11.2.Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн требованиям безопасности ПДн.

11.3.При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

12. Ответственность должностных лиц

12.1. Работники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.