

Муниципальное бюджетное общеобразовательная организация
«Снежская гимназия» Брянского района

Приказ № 47/2
от 19.01.2015 г.

Брянский район, п.Путёвка

**Об утверждении локальных актов
по защите персональных данных**

В целях исполнения Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных», на основании решения педагогического совета №12 от 16.01.2015 г.,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие следующие документы по защите информации:
 - 1.1. Политика информационной безопасности (Приложение 1);
 - 1.2. Положение о разграничении прав доступа к персональным данным (Приложение 2);
 - 1.3. Перечень персональных данных (Приложение 3);
 - 1.4. Порядок резервирования и восстановления работоспособности (Приложение 4);
 - 1.5. Инструкцию администратора безопасности информационной системы персональных данных (Приложение 5);
 - 1.6. Инструкцию пользователя информационной системы персональных данных (Приложение 6);
 - 1.7. Инструкцию по обеспечению безопасности рабочих мест обработки персональных данных (Приложение 7);
 - 1.8. Инструкцию по работе с обращениями субъектов персональных данных (Приложение 8);
 - 1.9. Инструкцию по работе со съемными носителями, содержащими персональные данные (Приложение 9);
 - 1.10. Инструкцию по обработке персональных данных без использования средств автоматизации (Приложение 10);
 - 1.11. Порядок уничтожения носителей персональных данных (Приложение 11);
 - 1.12. Инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 12);
 - 1.13. Положение о защите персональных данных обучающихся МБОУ «Снежская гимназия» Брянского района (Приложение 13);
2. Всем сотрудникам, имеющим доступ к персональным данным в соответствии с должностными обязанностями, ознакомить с документами под роспись.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор гимназии _____ А.А.Львович

«ПРИНЯТА»

на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»

Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ № ____ от _____

ПОЛИТИКА информационной безопасности ТЕРМИНЫ и ОПРЕДЕЛЕНИЯ

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - 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.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АВПО – антивирусной программное обеспечение

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее Политика) МБОУ «Снежская гимназия» Брянского района (далее Оператор) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями нормативных документов:

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановления Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012г. №1119;
- Приказа «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. ФСТЭК N 21.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Оператора.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации УБПДн.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Область действия

Требования настоящей Политики распространяются на всех сотрудников Оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (контрагентов).

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- перечня персональных данных;
- частной модели актуальных угроз и вероятного нарушителя;
- положения о разграничении прав доступа к персональным данным;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Оператора. На основании анализа актуальных угроз безопасности ПДн описанного в Частной модели актуальных угроз и вероятного нарушителя, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю за соблюдением безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение ответственных лиц за соблюдением мер безопасности;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;

- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы уничтожения персональных данных.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;
- обнаружения вторжений;
- контроля защищенности персональных данных;
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- защиты среды виртуализации;
- защиты от утечки по ТКУИ.

4. Требования к подсистемам СЗПДн

СЗПДн может включать в себя следующие подсистемы:

- Идентификации и аутентификации субъектов доступа и объектов доступа. Подсистема обеспечивает присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).
- Управления доступом субъектов доступа к объектам доступа. Подсистема обеспечивает управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.
- Ограничения программной среды. Подсистема обеспечивает установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.
- Регистрации событий безопасности. Подсистема обеспечивает сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
- Антивирусной защиты. Подсистема обеспечивает обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
- Обнаружения (предотвращения) вторжений. Подсистема обеспечивает обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.
- Контроля (анализа) защищенности персональных данных. Подсистема обеспечивает контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.
- Обеспечения целостности информационной системы и персональных данных. Подсистема обеспечивает обнаружение фактов несанкционированного нарушения

целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

- Обеспечения доступности персональных данных. Подсистема обеспечивает авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

- Защиты среды виртуализации. Подсистема исключает несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

- Защиты технических средств. Подсистема исключает несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивает защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

- Защиты информационной системы, ее средств, систем связи и передачи данных. Подсистема обеспечивает защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

- Выявления инцидентов и реагированию на них. Подсистема обеспечивает обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

- Управления конфигурацией информационной системы и системой защиты персональных данных. Подсистема обеспечивает управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

5. Пользователи ИСПДн

В ИСПДн Оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администраторы безопасности ИСПДн;
- пользователи ИСПДн;
- системные администраторы.

Данные о группах пользователей, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к персональным данным.

Администраторы безопасности ИСПДн:

Администратором безопасности является штатный сотрудник Оператора, ответственный за функционирование СЗПДн, назначается приказом Директора гимназии.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с другими защищенными сетями.

Пользователь ИСПДн

Пользователем ИСПДн является штатный сотрудник Оператора, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Системные администраторы:

Системным администратором может быть штатный сотрудник Оператора или лица сторонних организаций, осуществляющих свои функции на основании двухстороннего договора. Системный администратор не имеет полномочий для управления подсистемами обработки данных и безопасности.

Системный администратор обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Оператора, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и

процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Оператора, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. Ответственность сотрудников

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Администраторы безопасности ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Оператора – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

«ПРИНЯТО»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ № ____ от _____

ПОЛОЖЕНИЕ
о разграничении прав доступа к персональным данным

1. Общие положения

В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа к обрабатываемым персональным данным.

Перечень групп, участвующих в обработке персональных данных в ИСПДн :

Группа	Уровень доступа к ПДн	Разрешенные действия
Системные администраторы	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Администраторы безопасности ИСПДн	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

«ПРИНЯТ»

на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района

Протокол №__ от _____ г.

«УТВЕРЖДАЮ»

Директор МБОУ «Снежская гимназия»
Брянского района

_____ А.А.Львович

Приказ №__ от _____

ПЕРЕЧЕНЬ персональных данных

1. Персональные данные сотрудников

1.1. Перечень персональных данных (ПДн) сотрудников МБОУ «Снежская гимназия» Брянского района (далее Оператор):

- паспортные данные работника, ИНН;
- данные страхового свидетельства государственного пенсионного страхования;
- данные документов об образовании, квалификации или наличии специальных званий, статусных и ведомственных наград;
- анкетные данные, фото и видео (в том числе сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности, данные медицинской книжки);
- сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, содержащие сведения, необходимые для выполнения обязанностей в соответствии с действующим законодательством.

1.2. ПДн сотрудников обрабатываются Оператором на основании Трудового Кодекса Российской Федерации, ФЗ №152 «О персональных данных».

1.3. Согласие субъекта на обработку его ПДн не требуется в соответствии со статьей 6 ФЗ №152 «О персональных данных».

1.4. Средствами обработки ПДн являются: сбор, запись, систематизация, накопление, хранение, уточнение, обновление (изменение), использование, передачи (без передачи по сети Интернет).

1.5. ПДн сотрудников обрабатываются в отделах: кадровая служба, бухгалтерия и иные структурные подразделения.

1.6. Срок хранения ПДн сотрудников составляет 75 лет.

1.7. ПДн сотрудников представлены в электронном и бумажном виде.

1.8. Места хранения ПДн - локально на АРМ, в помещениях, предназначенных для хранения.

2. Персональные данные обучающихся

2.1 Перечень персональных данных (ПДн) обучающихся МБОУ «Снежская гимназия» Брянского района (далее Оператор):

- ФИО;
- пол;
- дата рождения;
- адрес, телефон, e-mail;
- паспортные данные;
- сведения об образовании;

- сведения о родителях (законных представителях обучающихся)
- наличие льгот (сирота, инвалидность и др.);
- сведения банка данных по различным категориям обучающихся (в том числе одарённым детям, детям из приоритетных категорий, участие в олимпиадах и конкурсах, турнирах соревнованиях, фестивалях и т.п.);
- спортивный разряд, разряд ГТО, и т.п.;
- информация из документов об образовании;
- выбранные специальности;
- данные по призыву на воинскую службу;
- данные для ГИА (ЕГЭ, ОГЭ и т.п.);
- данные страхового свидетельства государственного пенсионного страхования;
- анкетные данные, фото и видео;
- документы о состоянии здоровья;
- сведения, содержащиеся в приказах о зачислении, отчислении, переводе, поощрении и взыскании;
- сведения, необходимые для исполнения норм действующего законодательства.
- личные дела;

2.2 ПДн обучающихся обрабатываются Оператором на основании письменного согласия родителей обучающихся.

2.3 Средствами обработки ПДн являются: сбор, запись, систематизация, накопление, хранение, уточнение, обновление (изменение), использование, передачи.

2.4 ПДн обучающихся представлены в электронном и бумажном виде.

2.5 Места хранения ПДн - локально на АРМ, в помещениях, предназначенных для хранения.

«ПРИНЯТ»

на Педагогическом совете
МБОУ «Снежская гимназия»

Брянского района

Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»

Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович

Приказ № ____ от _____

ПОРЯДОК

резервирования и восстановления работоспособности

1. Назначение и область действия.

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (далее – Инструкция) определяет действия, связанные с функционированием ИСПДн МБОУ «Снежская гимназия» Брянского района (далее Оператор), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Оператора, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящим к потере защищаемой информации и контроль обеспечения мероприятий по предотвращению инцидентов безопасности, назначается Администратор безопасности ИСПДн.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.
- В результате преднамеренных действий пользователей и третьих лиц.
- В результате нарушения правил эксплуатации технических средств ИСПДн.
- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Оператора предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывной работы и восстановления ресурсов при возникновении инцидентов.

Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

– пожарные сигнализации и системы пожаротушения;

– системы резервного питания.

Все критичные помещения Оператора (помещения, в которых размещаются сервера ИСПДн) должны быть оборудованы средствами пожарной сигнализации.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, могут применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

– резервные линии электропитания в пределах комплекса зданий.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, могут использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск, flash-накопитель и т.п.).

Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

– для обрабатываемых персональных данных – не реже раза в месяц;

– для технологической информации – не реже раза в год;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы.

Носители должны храниться в негорючем шкафу.

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ № ____ от _____

ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных муниципального бюджетного образовательного учреждения «Снежская гимназия» Брянского района (далее – Гимназия).

1.2. Администратор безопасности информационных систем персональных данных (далее – ИСПДн) является сотрудником Гимназии и назначается приказом по Гимназии.

1.3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.4. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам Гимназии.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных (*Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.)*)

2.13. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

3.1. Знать перечень и условия обработки персональных данных в Гимназии.

3.2. Знать перечень установленных в кабинетах Гимназии технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

3.3. Определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт и периодический контроль над составом и полномочиями пользователей автоматизированных рабочих мест (далее АРМ).

3.5. Осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации.

3.6. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.7. Реагировать на попытки несанкционированного доступа к информации в установленном ст. 4 настоящей Инструкции.

3.8. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.

3.9. Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).

3.10. Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.

3.11. Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.

3.12. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.13. Предоставлять доступ к ИСПДн новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям «Инструкции по организации парольной защиты».

3.14. Производить мероприятия по внеплановой смене паролей в соответствии с «Инструкцией по организации парольной защиты».

3.15. Вносить плановые и внеплановые изменения в учётную запись пользователей ИСПДн, в том числе по требованию руководителя отдела и в случае увольнения сотрудника.

3.16. Осуществлять периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных.

3.17. Осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для восстановления утраченных сведений.

3.18. Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц.

3.19. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.20. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.21. Выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с ИСПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

4.2.1. прекратить несанкционированный доступ к ИСПДн;

4.2.2. доложить директору Гимназии о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

V. ПРАВА

Администратор безопасности ИСПДн имеет право:

5.1. Требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.

5.4. Производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля.

5.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил

работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Администратор безопасности ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в Гимназии, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Администратор безопасности ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

«ПРИНЯТА»

на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол №__ от _____ г.

«УТВЕРЖДАЮ»

Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №__ от _____

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник МБОУ «Снежская гимназия» Брянского района (далее Оператор), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется:

- Положением по защите персональных данных;
- Политикой информационной безопасности;
- Инструкциями по обеспечению безопасности персональных данных;
- настоящей инструкцией;
- нормативными документами ФСТЭК России.

1.5. Методическое руководство работой пользователя осуществляется администратором безопасности (АБ) ИСПДн.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ ИСПДн.

2.8. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.

- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Блокировка>

2.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий в пределах, возложенных на него функций.

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ № ____ от _____

ИНСТРУКЦИЯ **по обеспечению безопасности рабочих мест** **обработки персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет требования по защите рабочих мест ИСПДн, на которых ведется обработка и хранение персональных данных.

1.2. Настоящая инструкция составлена на основании требований нормативных документов ФСТЭК России.

1.3. В понятие защиты рабочих мест ИСПДн входит:

- физическая защита технических средств от несанкционированного доступа;
- парольная защита рабочих мест от несанкционированного доступа к персональным данным;
- антивирусная защита рабочих мест от несанкционированного доступа к персональным данным из сети Интернет.

2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В соответствии с требованиями нормативных документов ФСТЭК России методами и способами защиты информации от несанкционированного доступа являются:

- 2.1. реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- 2.2. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- 2.3. разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- 2.4. регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- 2.5. учет и хранение съемных носителей информации, и их обращение, исключающее хищение, подмену и уничтожение;
- 2.6. резервирование технических средств, дублирование массивов и носителей информации;
- 2.7. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- 2.8. использование защищенных каналов связи;
- 2.9. размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- 2.10. организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- 2.11. предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

3. ТРЕБОВАНИЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

3.1. С целью контроля учетных записей для доступа к информационным ресурсам персональных данных, все легализованные учетные записи ведутся в Журнале учета Логинов (Приложение 1).

3.2. Личные пароли доступа к элементам ИСПДн создаются пользователям самостоятельно.

3.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.4. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- Пароль должен состоять не менее чем из 6 символов.

- В пароле должны присутствовать символы трех категорий из числа следующих четырех:
 - прописные буквы английского алфавита от А до Z;
 - строчные буквы английского алфавита от а до z;
 - десятичные цифры (от 0 до 9);
 - символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).
- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- Запрещается выбирать пароли, которые уже использовались ранее.

3.5. Правила ввода пароля:

- Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами и или техническими средствами.

3.6. Правила хранения пароля:

- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.7. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

3.8 Необходимо своевременно сообщать администратору безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. ТРЕБОВАНИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

4.1. На каждом рабочем месте и серверах ИСПДн должно быть установлено антивирусное программное обеспечение (АВПО).

4.2. Антивирусные базы всегда должны быть в актуальном состоянии.

4.3. Запрещается работа на элементах ИСПДн с выключенным или неработоспособным АВПО.

4.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности (АБ) ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

4.5. Проверка на наличие вирусов должна проводиться регулярно. Проверке подлежат:

- все файлы на жестких дисках серверов и рабочих мест;
- съемные носители, содержащие персональные данные;
- получаемые из сторонних организации файлы;
- передаваемые в сторонние организации файлы.

4.6. Результаты проверок должны фиксироваться в Журнале антивирусных проверок.

4.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях АБ. АБ совместно с пользователем должен выполнить внеочередной антивирусный контроль.

5. ТРЕБОВАНИЯ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

5.1. Работа в сети Интернет на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2. При работе в сети Интернет запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран).
- Передавать по сети защищаемую информацию без использования средств шифрования.

- Загружать нелицензионное программное обеспечение.
- Посещать сайты сомнительной репутации (сайты содержащие нелегально распространяемое ПО и т.п.).

6. ТРЕБОВАНИЯ ПО РАБОТЕ СО СРЕДСТВАМИ ЗАЩИТЫ

6.1. На рабочих местах и серверах ИСПДн, исходя из Частной модели актуальных угроз, должны быть установлены специальные средства защиты. К ним относятся:

- средства защиты от несанкционированного доступа;
- межсетевые экраны;
- антивирусные средства защиты.

6.2. Все средства защиты могут быть установлены только организацией, имеющей лицензию на техническую защиту конфиденциальной информации.

6.3. Все средства защиты, установленные в ИСПДн, а также эксплуатационная документация на них, подлежат учету в Журнале учета средств защиты.

6.4. Настройка средств защиты проводится в соответствии с эксплуатационной документацией и требованиями нормативных документов ФСТЭК России.

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол № ____ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ № ____ от _____

ИНСТРУКЦИЯ

по работе с обращениями субъектов персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

В соответствии с требованиями Федерального Закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ, каждый субъект имеет право знать, как проходит обработка его персональных данных.

2. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Право субъекта персональных данных на доступ к своим персональным данным:

- 2.1. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
- 2.2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.
- 2.3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации. Форма запроса субъекта прилагается.
- 2.4. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:
 - подтверждение факта обработки персональных данных оператором;
 - правовые основания и цели обработки персональных данных;
 - цели и применяемые оператором способы обработки персональных данных;
 - наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
 - обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
 - сроки обработки персональных данных, в том числе сроки их хранения;
 - порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
 - информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
 - иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

2.5. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2.6. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обязанности оператора при сборе персональных данных:

3.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, указанную в разделе 2 настоящего документа.

3.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных пунктом 3.4. настоящего документа, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилию, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом права субъекта персональных данных;
- источник получения персональных данных.

3.4. Оператор освобождается от обязанности предоставить субъекту персональные данные, предусмотренные частью 3.3 настоящего документа, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в

- связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
 - оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
 - предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

3.5. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

3.6. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.7. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на законодательную базу, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3.8. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.9. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса. Форма уведомления приведена в Приложении.

3.10. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.11. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.12. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган. Форма уведомления приведена в приложении.

3.13. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

3.14. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

3.15. Оператор обязан вести учет обращений субъектов. Форма Журнала приведена в Приложении.

Форма запроса субъекта на доступ к его персональным данным

Директору МБОУ «Снежская гимназия» Брянского района

Александрю Анатольевичу Львовичу

от _____

ФИО субъекта

вид документа

номер документа

дата выдачи и кем выдан документ

запрос.

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные; указать цели, способы и сроки ее обработки; предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ); сведения о том, какие юридические последствия для меня может повлечь её обработка. В случае отсутствия такой информации, прошу Вас уведомить меня об этом.

_____ / _____ /

«__» _____ 20__ г.

Форма заявления субъекта на уточнение его персональных данных

Директору МБОУ «Снежская гимназия»
Брянского района

Александрю Анатольевичу Львовичу

от _____

ФИО субъекта

вид документа

номер документа

дата выдачи и кем выдан документ

заявление.

Прошу уточнить, обрабатываемые Вами, мои персональные данные в соответствии со сведениями: _____;

_____;

(указать уточненные персональные данные заявителя)

в связи с тем, что _____

(указать причину уточнения персональных данных)

_____ / _____ /

подпись/расшифровка

«__» _____ 201__ г.

Форма заявления субъекта на блокирование его персональных данных

Директору МБОУ «Снежская гимназия»
Брянского района
Александру Анатольевичу Львовичу

от _____

ФИО субъекта

вид документа

номер документа

дата выдачи и кем выдан документ

Заявление.

Прошу заблокировать, обрабатываемые Вами, мои персональные данные:

(указать блокируемые персональные данные)

На срок: _____;

(указать срок блокирования)

в связи с тем, что _____

(указать причину блокирования персональных данных)

_____/_____/

подпись/расшифровка

«__» _____ 20__ г.

Форма заявления субъекта на уничтожение его персональных данных

Директору МБОУ «Снежская гимназия»
Брянского района
Александру Анатольевичу Львовичу

от _____

ФИО субъекта

вид документа

номер документа

дата выдачи и кем выдан документ

заявление.

Прошу уничтожить, обрабатываемые Вами, мои персональные данные:

(указать уничтожаемые персональные данные)

в связи с тем, что _____

(указать причину уничтожения персональных данных)

_____/_____/

подпись/расшифровка

«__» _____ 201__ г.

Форма уведомления органа по защите прав субъектов

Руководителю Управления Роскомнадзора
по Брянской области

МБОУ «Снежская гимназия»
Брянского района

Уведомление.

Сообщаю Вам о том, что персональные данные субъекта _____ (ФИО)
обрабатываются в _____ (название организации) с
целью _____, на
основании _____, и
составляют: _____ (перечень ПДн).

_____ Львович Александр Анатольевич
подпись/ руководителя организации

«___» _____ 20__ г.

Форма уведомления субъекта об устранении неправомерных действий с его
персональными данными

Субъекту персональных данных

_____ ФИО

от МБОУ «Снежская гимназия» Брянского района

уведомление.

Сообщаю Вам, что допущенные нарушения при обработке персональных данных, а именно
_____ устранены.

(указать допущенные нарушения)

_____ Львович Александр Анатольевич
подпись/ руководителя организации

«___» _____ 20__ г.

Форма Журнала учета обращений субъектов ПДн

№	ФИО субъекта	Дата обращения	Цель обращения	Результат	Дата ответа	Исх. № ответа
1.						
2.						
3.						
4.						
5.						

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района

Протокол №___ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №___ от _____

ИНСТРУКЦИЯ

по работе со съемными носителями, содержащими персональные данные

- 1.1. Съемными накопителями являются:
 - USB-накопители (флеш-диски);
 - съемные накопители на жестких магнитных дисках (НЖМД);
 - дискеты;
 - диски;
 - и т.д.
- 1.2. Съемные накопители применяются для хранения электронных баз данных персональных данных в сейфах или других местах хранения, передачи персональных данных в вышестоящие организации, в филиалы оператора или в сторонние организации. Так же съемные накопители могут служить для переноса персональных данных на автономное рабочее место ИСПДн.
- 1.3. Перед использованием съемный носитель должен быть проверен антивирусными средствами на наличие вирусов.
- 1.4. Хранение съемных накопителей должно осуществляться в местах не доступных для посторонних лиц, также для должностных лиц оператора, не имеющих полномочий на обработку персональных данных для выполнения должностных обязанностей.
- 1.5. Учет съемных накопителей должен вестись в Журнале учета (форма журнала прилагается).
- 1.6. Уничтожение съемных носителей персональных данных должно проводиться комиссионно с оформлением Акта уничтожения (форма акта прилагается).

Форма Журнала учета съемных носителей

№	Уч.№ носителя	Назначение носителя	Дата начала использования носителя	Дата уничтожения носителя	№ и дата Акта уничтожения носителя	Подпись АБ

Форма Акта уничтожения съемного носителя
АКТ № _____
уничтожения съемных носителей персональных данных

« ____ » _____ 201_ г.

_____ населенный пункт

Настоящий акт составлен в том, что комиссией в составе:

Члены комиссии:

_____ ФИО

_____ должность

_____ ФИО

_____ должность

_____ ФИО

_____ должность

проведено уничтожение съемных носителей:

№	Уч. № носителя	Форма носителя	Способ уничтожения
1.			
2.			
3.			
4.			

Члены комиссии:

_____ ФИО

_____ должность

_____ ФИО

_____ должность

_____ ФИО

_____ должность

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол №___ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №___ от _____

ИНСТРУКЦИЯ

по обработке персональных данных без использования средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция разработана в соответствии с Постановлением Правительства «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008г. № 687.

1.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), 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.

1.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

– 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;

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

2.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой

без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

2.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный 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:

- 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;

- 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.

2.6. 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).

2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. При хранении материальных носителей, содержащих персональные данные должна обеспечиваться их сохранность. Несанкционированный доступ к ним должен быть исключен.

3.2. Сотрудники, производящие обработку персональных данных, должны быть осведомлены о методах обработки и защиты персональных данных.

3.3. Материальные носители персональных данных (документы) должны храниться в сейфе или в закрываемом на ключ шкафу (ящике).

3.4. Доступ в помещения, в которых осуществляется обработка персональных данных без использования средств автоматизации, должен быть ограничен.

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района

Протокол №___ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №___ от _____ г.

Порядок уничтожения носителей персональных данных

Носителями персональных данных являются:

- бумажные носители (документы);
- машинные носители:
 - накопители на жестких магнитных дисках (НЖМД), установленные в системных блоках автоматизированных рабочих мест обработки персональных данных;
 - съемные носители (дискеты, CD-DVD диски, USB-носители, съемные НЖМД).

1. Носители уничтожаются в случаях:

- истек срок хранения носителя;
 - носитель пришел в негодность.
2. Для уничтожения носителей приказом руководителя назначается комиссия.
3. Бумажные носители персональных данных, CD-DVD диски и дискеты уничтожаются путем сожжения или измельчения shredderом (уничтожителем бумаги).
4. НЖМД и USB-носители уничтожаются при помощи специальных устройств или физического повреждения, исключающего возможность восстановления носителя.
5. В том случае, если необходимо уничтожить персональные данные на машинном носителе и сохранить носитель для последующего использования необходимо произвести 3 цикла полного форматирования носителя.
6. После уничтожения носителей комиссия составляет Акт об уничтожении и делает отметку в Журнале учета носителей. Форма акта приведена в Приложении.

АКТ

об уничтожении носителей, содержащих персональные данные субъектов

Брянский район, п. Путёвка

«__» _____ 20__ г.

Настоящий Акт составлен в том, что комиссией, в составе:

Председатель:

(ФИО) - _____ (должность)

Члены комиссии:

(ФИО) - _____ (должность)

(ФИО) - _____ (должность)

(ФИО) - _____ (должность)

произведено уничтожение носителей, содержащих персональные данные субъектов.

Уничтожение произведено путем _____.

Опись носителей:

№	Наименование	Перечень персональных данных	Учетный номер	Примечания

Председатель

(ФИО) _____ (подпись) «__» _____ 20__ г.
(дата)

Члены комиссии:

(ФИО) _____ (подпись) «__» _____ 20__ г.
(дата)

(ФИО) _____ (подпись) «__» _____ 20__ г.
(дата)

(ФИО) _____ (подпись) «__» _____ 20__ г.
(дата)

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района

Протокол №__ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №__ от _____ г.

ИНСТРУКЦИЯ

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных МБОУ «Снежская гимназия» Брянского района (далее Оператора) разработана с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящая Инструкция определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.3. Настоящая Инструкция утверждается Директору гимназии.

2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

2.1.1. соответствие полномочий пользователя матрице доступа;

2.1.2. соблюдение пользователями информационных систем персональных данных парольной политики;

2.1.3. соблюдение пользователями информационных систем персональных данных антивирусной политики;

2.1.4. соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;

2.1.5. соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

2.1.6. соблюдение порядка резервирования баз данных и хранения резервных копий;

2.1.7. соблюдение порядка работы со средствами защиты информации;

2.1.8. знание пользователями информационных систем персональных данных о своих действиях во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

2.2.1. хранение бумажных носителей с персональными данными;

2.2.2. доступ к бумажным носителям с персональными данными;

2.2.3. доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

3. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее Ответственный) либо комиссией, назначаемой директором гимназии.

- 3.3. Внутренние проверки проводятся в соответствии с Планом внутренних проверок, составленным Ответственным либо Председателем комиссии и утвержденным директором гимназии.
- 3.4. План внутренних проверок составляется в декабре текущего года на следующий год.
- 3.5. Очередность и объем проверок определяется Ответственным либо Председателем комиссии.
- 3.6. По результатам каждой проверки составляется Протокол проведения внутренней проверки.
- 3.7. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
- 3.8. Протоколы хранятся у Ответственного либо Председателя комиссии. Срок хранения протокола – 1 год.
- 3.9. О результатах проверки и мерах, необходимых для устранения нарушений докладывает директору гимназии Ответственный либо Председатель комиссии.

План внутренних проверок условий обработки персональных данных

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя матрице доступа	Положение о разграничении прав доступа к персональным данным Инструкция пользователя информационной системы персональных данных Политика информационной безопасности		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Инструкция пользователя информационной системы персональных данных Инструкция по обеспечению безопасности рабочих мест обработки персональных данных		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики	Инструкция пользователя информационной системы персональных данных Инструкция по обеспечению безопасности рабочих мест обработки персональных данных		
4.	Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных	Инструкция по работе со съемными носителями, содержащими персональные данные		
5.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Инструкция пользователя информационной системы персональных данных Инструкция по обеспечению безопасности рабочих мест обработки персональных данных		
6.	Соблюдение порядка работы со средствами защиты информации	Инструкция пользователя информационной системы персональных данных Инструкция по обеспечению безопасности рабочих мест обработки персональных данных		
7.	Хранение бумажных носителей с персональными данными	Инструкция по обработке персональных данных без использования средств автоматизации		
8.	Доступ к бумажным носителям с персональными данными			
9.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Инструкция по обработке персональных данных без использования средств автоматизации Перечень помещений, предназначенных для обработки персональных данных		

**Протокол
проведения внутренней проверки условий обработки персональных данных**

Настоящий Протокол составлен в том, что _____.20__ ответственным за организацию обработки персональных данных/комиссией по внутреннему контролю проведена проверка

тема проверки

Проверка осуществлялась в соответствии с требованиями _____

название документа

В ходе проверки проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____.

Должность Ответственного

_____ И.О. Фамилия

Члены комиссии:

Должность

_____ И.О. Фамилия

Должность

_____ И.О. Фамилия

Должность

_____ И.О. Фамилия

Должность руководителя проверяемого подразделения

_____ И.О. Фамилия

«ПРИНЯТА»
на Педагогическом совете
МБОУ «Снежская гимназия»
Брянского района
Протокол №___ от _____ г.

«УТВЕРЖДАЮ»
Директор МБОУ «Снежская гимназия»
Брянского района

А.А.Львович
Приказ №___ от _____

ПОЛОЖЕНИЕ
о защите персональных данных обучающихся
МБОУ «Снежская гимназия» Брянского района

1. Общие положения

- 1.1. Целью данного Положения является защита персональных данных обучающихся от несанкционированного доступа, неправомерного их использования или утраты.
- 1.2. Положение о защите персональных данных обучающихся образовательного учреждения (далее – Положение) разработано с целью защиты информации, относящейся к личности и личной жизни обучающихся МБОУ «Снежская гимназия» Брянского района (далее – образовательная организация) в соответствии со статьей 24 Конституции Российской Федерации, Трудовым кодексом Российской Федерации и Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- 1.3. Персональные данные относятся к категории конфиденциальной информации.
- 1.4. Настоящее Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным обучающихся и их родителей (законных представителей).

2. Понятие и состав персональных данных

- 2.1. Персональные данные обучающегося МБОУ «Снежская гимназия» Брянского района - информация, необходимая администрации гимназии для обеспечения образовательного процесса конкретного ученика. Под информацией о обучающихся понимаются сведения о фактах, событиях и обстоятельствах жизни обучающегося, позволяющие идентифицировать его личность.
- 2.2. В состав персональных данных обучающегося входят:
- ФИО;
 - пол;
 - дата рождения;
 - адрес, телефон, e-mail;
 - паспортные данные;
 - сведения об образовании;
 - сведения о родителях (законных представителях обучающихся)
 - наличие льгот (сирота, инвалидность и др.);
 - сведения банка данных по различным категориям обучающихся (в том числе одарённым детям, детям из приоритетных категорий, участие в олимпиадах и конкурсах, турнирах соревнованиях, фестивалях и т.п.);
 - спортивный разряд, разряд ГТО, и т.п.;
 - информация из документов об образовании;
 - выбранные специальности;
 - данные по призыву на воинскую службу;
 - данные для ГИА (ЕГЭ, ОГЭ и т.п.);
 - данные страхового свидетельства государственного пенсионного страхования;
 - анкетные данные, фото и видео;
 - документы о состоянии здоровья;

- сведения, содержащиеся в приказах о зачислении, отчислении, переводе, поощрении и взыскании;
- сведения, необходимые для исполнения норм действующего законодательства.
- личные дела;

2.3. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных.

3.1. Под обработкой персональных данных обучающегося понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных обучающегося.

3.2. В целях обеспечения прав и свобод человека и гражданина работники гимназии при обработке персональных данных обучающихся обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных обучающегося может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности обучающегося.

3.2.2. При определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, законом об образовании и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их родителями обучающегося, или законными представителями, так и путем получения их из иных источников при условии предоставления оператору подтверждения наличия следующих оснований:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления 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;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего

Федерального закона, при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно – розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Также, если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

3.2.4. Персональные данные следует получать только от родителей или законных представителей. Если персональные данные обучающегося, возможно, получить только у третьей стороны, то родители или законные представители должны быть уведомлены об этом заранее, и от них должно быть получено письменное согласие. Директор гимназии должен сообщить родителям о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных.

3.2.5. Администрация гимназии не имеет права получать и обрабатывать персональные данные обучающегося о его политических, религиозных и иных убеждениях.

3.3. К обработке, передаче и хранению персональных данных обучающегося могут иметь доступ сотрудники:

администратор

- директор гимназии;
- администратор безопасности информационных систем персональных данных (назначается приказом по Гимназии).
- заместитель директор по УВР;
- заместитель директор по ВР;
- заместитель директор по АХЧ;
- преподаватель – организатор ОБЖ;
- классный руководитель;
- социальный педагог;

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных обучающихся возможна только с согласия родителей обучающегося или законных представителей в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных обучающегося администрация гимназии должна соблюдать следующие требования:

- не сообщать персональные данные обучающегося третьей стороне без письменного согласия родителей или законных представителей, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью ребенка, а также в случаях, установленных федеральным законом;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные обучающегося, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными обучающихся в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по школе, при этом указанные лица должны иметь право получать только те персональные данные обучающегося, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья

3.5.2. Передача персональных данных от держателя или внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.5.3. При передаче персональных данных обучающегося потребителям за пределы учреждения администрация гимназии не должна сообщать эти данные третьей стороне без их родителями обучающегося или законными представителями, так и путем получения их из иных источников

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных обучающегося распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8 Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4. Доступ к персональным данным

4.1 Внутренний доступ (доступ внутри учреждения).

4.1.1. Право доступа к персональным данным обучающегося имеют:

- директор гимназии;
- администратор безопасности информационных систем персональных данных.
- заместители директора;
- другие сотрудники гимназии при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц имеющих доступ к персональным данным работников, определяется приказом директора гимназии.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- управление образования;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;

- органы социального страхования;
- подразделения муниципальных органов управления.

4.2.2. Надзорно – контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Другие учреждения.

Сведения о месте учебы могут быть предоставлены другой организации только с письменного запроса на фирменном бланке организации.

5. Защита персональных данных.

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3 Защита персональных данных представляет собой жестко регламентированный и динамически - технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой деятельности гимназии.

5.4. Защита персональных данных обучающихся от неправомерного их использования или утраты должна быть обеспечена администрацией гимназии за счет его средств в порядке, установленном федеральными законами.

5.5. "Внутренняя защита".

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и работниками образовательного учреждения.

5.5.2. Для обеспечения внутренней защиты персональных данных обучающихся необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- воспитательная и разъяснительная работа с сотрудниками учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки содержащие персональные данные сотрудника, должны быть защищены паролем.

5.6. "Внешняя защита".

5.6.1 защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение

ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. ,

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности гимназии. Посторонние лица не должны знать распределение функций рабочие процессы, технологию составления, оформления, ведения и хранения документов

5.6.3. Для обеспечения внешней защиты персональных данных, обучающихся необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим гимназии;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств.

5.7. Все лица связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных обучающихся.

6. Права и обязанности родителей или их законных представителей

6.1. Закрепление прав родителей, регламентирующих защиту его персональных данных и данные о его ребенке, обеспечивает сохранность полной и точной информации о нем.

6.2. Родители должны быть ознакомлены под расписку с документами гимназии, устанавливающими порядок предоставления и перечень персональных данных на ребенка, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся в школе, родитель имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Родитель или законный представитель обязан:

- передавать администрации гимназии комплекс достоверных, документированных персональных данных, состав которых установлен Уставом гимназии.
- своевременно сообщать об изменении своих персональных данных.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными:

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник гимназии, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.