Утверждено
приказом МБОУ СОШ № 7 г. Сальска
от 30.08.2019 г. № 207/1
директор _____С.Ю.Лысикова

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г. Сальска

Настоящее Положение разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

Для целей настоящего Положения применяются следующие термины и определения:

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

Оператор Персональных данных – Муниципальное бюджетное общеобразовательное учреждение городского округа Тольятти «Школа с углубленным изучением отдельных предметов № 70» (далее Учреждение) – 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.

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

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, 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, применяемые в информационных системах.

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

Правила разграничения доступа к информационным системам персональных данных – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
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.
Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Конфиденциальность персональных данных – Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.
Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:
- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

1 Общие положения

Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников, обучающихся и их родителей (законных представителей) Учреждения.

Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.
Мероприятия по обеспечению безопасности ПДн формулируются на основании анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.
Обеспечение безопасности ПДн осуществляется путем выполнения Требований по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных Учреждения (Приложение № 1).
Структура, состав и основные функции СЗПДн определяются исходя из анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.
Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.
Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:
а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности информационных систем;
в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;
д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
ж) учет лиц, допущенных к работе с ПДн в информационной системе;
з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
к) описание системы защиты персональных данных.
Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.
Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.
По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:
– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;

– угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.
Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:
– обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;
– ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

2 Цели обеспечения информационной безопасности

Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:
– целостности информации;
– доступности обрабатываемой информации для зарегистрированных пользователей;
– конфиденциальности информации.

3 Объект защиты

Объектом защиты является информационная система персональных данных работников, обучающихся и их родителей (законных представителей) Учреждения:
а) Информационные ресурсы:
– персональные данные работников, обучающихся и их родителей (законных представителей) (исходная информация, информационные базы данных);
– инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;
б) технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;
в) помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;
г) технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.
Критичными свойствами объекта защиты являются:
а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;
б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;
в) несанкционированная доступность информации, выражающаяся в возможности:
– непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;
– прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);
– перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

4 Субъекты информационных отношений

4.1 Субъектами информационных отношений являются:
– Работники (субъекты) – физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением-оператором;
– Обучающиеся (субъекты персональных данных) - физические лица, которые состоят в договорных и иных гражданско-правовых отношениях с Учреждением-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом.
4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:
– конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
– достоверности (полноты, точности, адекватности, целостности) информации;
– защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
– своевременного доступа (за приемлемое для них время) к необходимой им информации;
– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
– защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

5 Возможные угрозы и участки вторжения

Общая классификация угроз.
1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.
2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.
3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

6 Порядок проведения контрольных мероприятий и действий по результатам контроля

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Контроль может проводиться комиссией, созданной в Учреждении, или на договорной основе сторонними организациями, при наличии лицензии на деятельность по технической защите конфиденциальной информации.
Решение основных вопросов обеспечения защиты ПДн предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения, а также, при необходимости, привлечение сторонней организации при наличии лицензий ФСТЭК и ФСБ.

Приложения к Положению по организации и проведению работ по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г. Сальска являются самостоятельными документами и его неотъемлемой частью.

Список приложений:

Приложение № 1. Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г. Сальска

Приложение № 2. Описание локальной сети МБОУ СОШ №7 г. Сальска.

Приложение № 3. Описание состава технических средств МБУ МБОУ СОШ №7 г. Сальска, участвующих в обработке персональных данных.

Приложение № 4. Сведения о программном обеспечении МБОУ СОШ №7 г. Сальска, установленном на рабочих станциях, участвующих в обработке персональных данных.

Приложение № 5. Сведения о программно-технических средствах защиты МБОУ СОШ №7 г. Сальска, установленных на рабочих станциях, участвующих в обработке персональных данных.

Приложение № 6. Сведения о пользователях систем общего пользования (СОП) МБОУ СОШ №7 г. Сальска.

Приложение № 7. Рекомендации по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Приложение № 8. Соглашение о неразглашении информации, содержащей персональные данные сотрудников и обучающихся МБОУ СОШ №7 г. Сальска.

Приложение № 9. Форма ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами МБОУ СОШ №7 г. Сальска по вопросам обработки персональных данных.

Приложение № 10. Инструкция по организации парольной защиты.

Приложение № 11. Правила работы с обезличенными персональными данными в МБОУ СОШ №7 г. Сальска.

Приложение № 12. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований.

Приложение № 13. Формы журналов учета в МБОУ СОШ №7 г. Сальска.

Приложение № 14. Разъяснение субъекту персональных данных (работнику) юридических последствий отказа предоставить свои персональные данные.

Приложение № 15. Уведомление о факте обработки персональных данных без использования средств автоматизации.

Приложение № 16. Инструкции.

Приложение № 1
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г. Сальска

При организации и осуществлении защиты персональных данных (ПДн) необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах (информационных системах персональных данных – ИСПДн), учитывая при этом, что ПДн, в соответствии с Федеральным Законом от 27 июля 2006 года № 152 – ФЗ «О персональных данных» и Указом Президента РФ № 188 от 06.03.97 г., отнесены к конфиденциальной информации.
Меры по обеспечению безопасности персональных данных при их обработке
1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.
2. Обеспечение безопасности персональных данных достигается, в частности:
1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5) учетом машинных носителей персональных данных;
6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
При проведении мероприятий по защите ПДн учитывается, что информационные ресурсы подвержены потенциальным внешним и внутренним угрозам, ведущим к потерям конфиденциальности, доступности и целостности информационных ресурсов.
Источники угрозы:
– люди (недобросовестные внешние и внутренние пользователи информационных ресурсов);

– аварии (ошибки пользователя, ошибки администратора);
– отказ аппаратного обеспечения (ошибки программного обеспечения, отказы индустриального оборудования);
– природные факторы (стихийные бедствия, астрофизические явления, биологические явления).

Угрозы увеличивают риски безопасности, представляющие собой:
– неавторизированный доступ в сеть;
– неавторизированное раскрытие информации;
– неавторизированную модификацию данных или программного обеспечения;
– разрушение функций сети (недоступность данных и сервисов).

Наличие рисков безопасности требуют введения мер безопасности. Меры безопасности должны гарантировать:
– конфиденциальность;
– целостность;
– доступность информации;
– своевременное получение отчетности;
– физическую безопасность информации;
– контроль доступа к информации. Информационная безопасность предусматривает:
– процедурную (административную и организационную безопасность);
– безопасность персонала;
– физическую безопасность;
– безопасность системы;
– безопасность коммуникаций.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн проводятся в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, с учетом возможного возникновения угроз безопасности жизненно важным интересам субъектов персональных данных.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:
– предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;
– своевременное обнаружение фактов НСД к ПДн;
– недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
– оперативного резервирования информации в ИСПДн;
– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
– постоянный контроль за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

Структура, состав и основные функции СЗПДн определяются в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, используемых в Учреждении.

СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн проводится путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

– оценку обстановки;

– обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

– разработку проекта обеспечения безопасности ПДн; выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и проектом защиты;

– решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

– обеспечение реализации принятого проекта защиты;

– планирование мероприятий по защите ПДн;

– организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

– разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн, в зависимости от класса информационной системы должны быть проведены мероприятия по защите от НСД к ПДн при их обработке в ИСПДн.

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

– защита от НСД при однопользовательском режиме обработки ПДн;

– защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;

– защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;

– защита информации при межсетевом взаимодействии ИСПДн;

– антивирусная защита.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты.

Меры безопасности ПДн должны гарантировать:

– конфиденциальность;

– целостность;

– доступность информации.

Мероприятия по обеспечению безопасности предусматривают:

– управление доступом;

– регистрацию и учет;

– обеспечение целостности;

– контроль отсутствия недекларированных возможностей;

– антивирусную защиту;
– обеспечение безопасного межсетевого взаимодействия;
– анализ защищенности.

Подсистемы управления доступом и регистрации и учета должны реализовываться на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз данных и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных действий пользователя или нарушителя.

Средства диагностики должны осуществлять тестирование файловой системы и баз данных, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и должны предусматривать аварийное уничтожение данных в случае угрозы несанкционированного доступа (НСД), которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов (пользователей) при их обращении к защищаемым данным и для предупреждения администратора при обнаружении факта НСД, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования.

Подсистема обеспечения целостности должна быть реализована операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей должна реализовываться на базе систем управления базами данных, средств защиты информации, антивирусных средств защиты информации.

Для осуществления разграничения доступа к информационным ресурсам при межсетевом взаимодействии должно применяться межсетевое экранирование, которое реализуется программными и/или программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран должен устанавливаться между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран должен входить в состав защищаемой сети. При его настройке отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Подсистема анализа защищенности должна реализовываться на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных в информационных системах персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, должны допускаться к соответствующим персональным данным на основании утвержденных Перечней должностных лиц, допущенных к работе с персональными данными.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в утвержденных Перечнях должностных лиц, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале

обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Учреждения или уполномоченными лицами.

При обнаружении нарушений порядка предоставления персональных данных Учреждения уполномоченные лица должны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

При хранении материальных носителей информации с персональными данными (или другой конфиденциальной информацией) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются отдельно.

Приложение № 2
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Описание локальной сети МБОУ СОШ №7 г. Сальска:

1. ЛС находится в пределах двух зданий и занимает три этажа.
2. Количество узлов, обрабатывающих персональные данные – 9.
3. Топология – звезда, тип – Ethernet 100Base–TX.
4. Участники сети являются источниками и потребителями информации.
5. Сеть использует стек протоколов TCP/IP.
6. Телекоммуникационные каналы предоставляются согласно Договору с провайдером ОАО «Ростелеком».
7. Скоростные характеристики: ЛС – 100 Мбит/с; Интернет – 2 Мбит/с.
8. Администрирование и перечень работ определяются ответственным за информационной безопасностью Учреждения.
9. Участники сети, которым необходим доступ в Интернет для выполнения служебных обязанностей, допускаются в локальную сеть в соответствии с разрешенными полномочиями.
10. Внесение изменений в телекоммуникационную схему ЛС производится работниками Учреждения (или сторонней организацией по договору или контракту).

Приложение № 3
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

1. Ввод в эксплуатацию, ремонт ТС, подключение ТС к сети осуществляется работниками Учреждения (или сторонней организацией по договору или контракту).
2. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ТС осуществляется работниками Учреждения (или сторонней организацией по договору или контракту).
3. ТС проверяется работниками Учреждения (или сторонней организацией по договору или контракту).
4. На этапах установки и настройки, обеспечением безопасности информации занимается техник Учреждения. На этапах эксплуатации за обеспечение безопасности отвечают пользователи ТС.

Описание состава технических средств МБОУ СОШ №7 г. Сальска, участвующих в обработке персональных данных:

№ п/п	Технические средства	Количество	Назначение	Приме-чание
1.	Рабочие станции	50 шт	обработка информации	
2.	Принтеры	8 шт.	распечатка документов	
3.	МФУ	6 шт.	сканирование, распечатка, тиражирование документов	
4.	Копировальные аппараты	5 шт.	тиражирование документов	
5.	Модем	1 шт.	обеспечение доступа к глобальной сети	

Приложение № 4
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

1. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ПО производится Администратором информационной безопасности Учреждения.
2. Настройка ПО производится работниками Учреждения (или сторонней организацией по договору или контракту).
3. При появлении новых версий ПО, изменения в ПО вносятся работниками Учреждения (или сторонней организацией по договору или контракту).
4. Изменения в ПО могут вносить только работники Учреждения.

Сведения о программном обеспечении МБОУ СОШ №7 г. Сальска, установленном на рабочих станциях, участвующих в обработке персональных данных

№ п/п	Программное обеспечение	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Приме-чание
1.	Microsoft Windows 7/8 Professional SP1 Microsoft Windows 5-10	Microsoft, США	Операционная система	Работники Учреждения	Работники Учреждения	
2.	Microsoft Office 2010-18	Microsoft, США	Офисный пакет приложений для работы с документами	Работники Учреждения	Работники Учреждения	
3.	Антивирус ESET NOD32	Международный разработчик антивирусных решений, Россия. Главный офис в Словакии	Антивирусная программа	Работники Учреждения	Работники Учреждения	
4.	РИС ГИА	Министерство образования и науки Российской Федерации	Информационная система персональных данных	Работники Учреждения	Работники Учреждения	
5.	РИС ЕГЭ	Министерство образования и науки Российской Федерации	Информационная система персональных данных	Работники Учреждения	Работники Учреждения	
6.	«1С: ХроноГраф Школа 2,5»	ЗАО «1С», г. Москва	Информационная система	Работники Учреждения	Работники Учреждения	
7.	КТ-Аттестат версия 1.0	ООО «НТЦ «АРМ-Регистр», Россия	Информационная система персональных данных	Работники Учреждения	Работники Учреждения	

Приложение № 5
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

1. Настройка СЗИ производится работниками Учреждения (или сторонней организацией по договору или контракту).
2. Разграничение доступа пользователей производится с помощью стандартных средств ОС.
3. Изменения в СЗИ производятся только Администратором информационной безопасности Учреждения

Сведения о программно-технических средствах защиты МБОУ СОШ №7 г. Сальска, установленных на рабочих станциях, участвующих в обработке персональных данных

№ п/п	Средства защиты информации	Сертификат безопасности информации	Разработчик СЗИ	Кто устанавливал	Кто сопровождает	Приме- чание
1.	Microsoft Windows 7/8 Professional SP1 Microsoft Windows 5-10	Нет	Microsoft, США	Работники Учреждения	Работники Учреждения	
2.	Антивирус ESET NOD32	Нет	ООО «Исет Софтвеа»	Работники Учреждения	Работники Учреждения	
3.	КриптоПро CSP 3.6	Идентификатор 690fe3785bbf48c6894642a64cb03dc9	Криптопровайдер ViPNet	Работники Учреждения	Работники Учреждения	

Приложение № 6
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Сведения о пользователях систем общего пользования МБОУ СОШ №7 г. Сальска

№ п/п	Подразделение	Количество допущенных работников	Кто осуществлял подключение	Кто сопровождает пользователей
1.	МБОУ СОШ №7 г. Сальска	Все педагогические работники	Работники Учреждения	Работники Учреждения

Приложение № 7
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

РЕКОМЕНДАЦИИ
по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают в себя:
- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений.

Для выполнения вышеназванных требований, необходимо наличие следующих средств защиты:
- средство защиты от несанкционированного доступа;
- межсетевой экран;
- антивирус.

При выборе того или иного средства защиты основными критериями отбора являются:
- наличие сертификатов ФСТЭК, ФСБ;
- обеспечение необходимого уровня защиты;
- производительность;
- совместимость;
- простота настройки и эксплуатации;
- техническая поддержка;
- цена.

Приложение № 8
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ СОТРУДНИКОВ И ОБУЧАЮЩИХСЯ
МБОУ СОШ №7 г. Сальска

Я, _____
(Ф.И.О.)
Проживающий по адресу: _____
_____
Паспорт серия_____ №_____, выданный (кем и когда) _____
_____
предупрежден (а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору, заключенному между мною и Муниципальным бюджетным общеобразовательным учреждением средней общеобразовательной школой №7 г. Сальска, и предусматривающих работу с персональными данными мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:
- не передавать (в любом виде) и не разглашать третьим лицам и работникам МБОУ СОШ №7 г. Сальска, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением директора МБОУ СОШ №7 г. Сальска, информацию, содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;
- в случае попытки третьих лиц или работников МБОУ СОШ №7 г. Сальска, не имеющих на это право, получить от меня информацию, содержащую персональные данные работников МБОУ СОШ №7 г. Сальска немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного руководителя) вышестоящему руководителю;
- не использовать информацию, содержащую персональные данные работников МБОУ СОШ №7 г. Сальска, с целью получения выгоды;
- выполнять требования закона и иных нормативных правовых актов Российской Федерации, а так же внутренних документов МБОУ СОШ №7 г. Сальска, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;
- в течение года после прекращения моих прав на допуск к информации, содержащей персональные данные работников МБОУ СОШ №7 г. Сальска (переход на должность, не предусматривающую доступ к персональным данным работников МБОУ СОШ №7 г. Сальска или прекращения Трудового договора), не разглашать и не передавать третьим лицам и неуполномоченным на это работникам МБОУ СОШ №7 г. Сальска, известную мне информацию, содержащую персональные данные.

Я ознакомлен(а) с положениями законодательства Российской Федерации, а так же внутренними организационно-распорядительными документами, в части защиты персональных данных.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

«__ _» _____ _____ г. _____/_____
(фамилия, инициалы) (подпись)

Приложение № 9
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Форма ознакомления с положениями законодательства Российской Федерации о персональных данных, локальными актами МБОУ СОШ №7 г. Сальска по вопросам обработки персональных данных

Я, _____ ,
(фамилия, имя, отчество)
паспорт серии _____ № _____
выдан _____

дата выдачи «____» _____ _____г.
работающий(ая) в должности _____

_____

(должность, наименование структурного подразделения)

ознакомлен(а) с

– положениями действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, в том числе с требованиями к защите персональных данных (Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– документом, определяющим политику МБОУ СОШ №7 г. Сальска в отношении обработки персональных данных (Политика в отношении обработки персональных данных в МБОУ СОШ №7 г. Сальска); – локальными актами МБОУ СОШ №7 г. Сальска по вопросам обработки персональных данных.

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Приложение № 10
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Инструкция
по организации парольной защиты

1. Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных в МБОУ СОШ №7 г. Сальска (далее - Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системе персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

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

-ИСПДн - информационная система персональных данных.

-Компрометация- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

- Объект доступа- единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

- Пароль- уникальный признак субъекта доступа, который является его (субъекта) секретом.

- Правила доступа- совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

- Несанкционированный доступ- доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, представляемых средствами вычислительной техники или АС.

2. Правила генерации паролей

2.1. Персональные пароли должны генерироваться самими пользователями с учетом данной инструкции.

2.2. В составе пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4.Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;
- при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.5. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

3. Порядок смены паролей

3.1. Полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

3.2. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

3.3. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4. Обязанности пользователей при работе с парольной защитой

4.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

4.3. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5. Случаи компрометации паролей

5.1. Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

5.2. Действия при компрометации пароля:
− скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
− о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6. Ответственность пользователей при работе с парольной защитой

6.1. Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
6.3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.4. Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Приложение № 11
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

ПРАВИЛА
работы с обезличенными персональными данными в МБОУ СОШ №7 г. Сальска

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Правила работы с обезличенными персональными данными в МБОУ СОШ №7 г. Сальска (далее – «Учреждение») разработаны с учетом Федерального закона от 27.07.2006 г. № 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».

Настоящие Правила определяют порядок работы с обезличенными данными «Учреждения». Настоящие Правила утверждаются директором «Учреждения» и действует постоянно.

2. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных «Учреждения и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:
– уменьшение перечня обрабатываемых сведений;

– замена части сведений идентификаторами;
– обобщение – понижение точности некоторых сведений;
– понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
– деление сведений на части и обработка в разных информационных системах;
– другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.

Перечень должностей «Учреждения», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в п.4 настоящих Правил.

Директор «Учреждения» принимает решение о необходимости обезличивания персональных данных.

Работники, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, если это необходимо.

Сотрудники, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

3. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:
– парольной политики;
– антивирусной политики;
– правил работы со съемными носителями (если они используется);
– правил резервного копирования;
– правил доступа в помещения, где расположены элементы информационных систем;
– иных предусмотренных законодательством РФ законов и правовых актов.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
– правил хранения бумажных носителей;
– правил доступа к ним и в помещения, где они хранятся;
– иных предусмотренных законодательством РФ законов и правовых актов.

4. ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ МБОУ СОШ №7 г. САЛЬСКА, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Директор
2. Заместитель директора по УВР
3. Заместитель директора по ВР
4. Заместитель директора по АХР
5. Библиотекарь
6. Секретарь
7. Старшая вожатая

8. Преподаватель-организатор ОБЖ
9. Педагог-психолог
10. Классные руководители

Приложение №12
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г. Сальска

ПОРЯДОК

уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение № 13
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

ЖУРНАЛ
учета ознакомления сотрудников МБОУ СОШ №7 г. Сальска с нормативными документами по вопросам обработки персональных данных

№ п/п	ФИО сотрудника	должность	Дата	подпись

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн
1.						

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых	Цель получения персональн	Отметка о передаче или отказе	Дата передачи/отказа в	Подпись запрашивающего лица

		персональных данных	ых данных	в передаче персональных данных	передаче персональных данных	

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение № 14
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Разъяснение субъекту персональных данных (работнику) юридических последствий отказа предоставить свои персональные данные

_____
(фамилия, имя, отчество)

паспорт серии _____ № _____ , выдан _____

_____

_____

_____ дата выдачи «___»_____ _____г.

Я, получил(а) разъяснения о юридических последствиях отказа предоставить свои персональные данные МБОУ СОШ №7 г. Сальска в соответствии с законодательством Российской Федерации. В соответствии со статьей 65 Трудового кодекса Российской федерации субъект персональных данных при приеме на работу и заключении трудового договора, обязан представить определенный перечень информации о себе. Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен. На основании пункта 11 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 15
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ №7 г.

Уведомление о факте обработки персональных данных без использования средств автоматизации

Я, _____ ,
(фамилия, имя, отчество)

паспорт серии _____ № _____
выдан _____
_____

дата выдачи «____»_____ ____г.

работающий(ая) в должности

_____
_____
_____
(должность, наименование структурного подразделения)

проинформирован(а):

– о факте обработки мною персональных данных, обработка которых осуществляется МБОУ СОШ №7 г. Сальска (далее - Оператор) без использования средств автоматизации*;

– о категориях обрабатываемых персональных данных;

– о правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора.

* обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

Я предупрежден(а) о том, что в случае нарушения установленного законодательством Российской Федерации порядка сбора, хранения, использования или распространения персональных данных я несу ответственность, предусмотренную ст. 13.11 КоАП РФ.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 16
К Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных МБОУ СОШ №7 г.

Инструкция
ответственного за организацию обработки персональных данных

I. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Ответственный за организацию обработки персональных данных в Муниципальном бюджетном образовательном учреждении средней общеобразовательной школе № 7 г. Сальска назначается приказом руководителя Организации.

1.3. Ответственный за организацию обработки персональных данных в Организации в своей деятельности руководствуется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, приказом Федеральной службы по техническому и экспортному контролю № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», другими законодательными и нормативно-правовыми актами по вопросам обработки и защиты персональных данных.

II. Обязанности ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки персональных данных обязан:

-осуществлять внутренний контроль за соблюдением работниками МБОУ СОШ № 7 г. Сальска законодательства Российской Федерации, локальных актов по обработке персональных данных, требований к защите персональных данных и принимать меры по устранению выявленных нарушений;

-организовывать проведение занятий и доведения до сведения работников МБОУ СОШ № 7 г. Сальска положений законодательства Российской Федерации о персональных данных, локальных актов Организации по вопросам обработки персональных данных, требований к защите персональных данных;

-руководить разработкой в МБОУ СОШ № 7 г. Сальска приказов, положений, инструкций, правил, порядков, перечней и других документов, регламентирующих порядок обработки персональных данных по вопросам защиты персональных данных в соответствии с требованиями законодательства и нормативно-правовых актов Российской Федерации;

-организовывать и контролировать прием и обработку обращений и запросов субъектов персональных данных или их представителей;

-при организации обработки персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного намеренного или случайного доступа к ним, уничтожения, изменения, блокирования,

копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;

-докладывать директору о выявленных нарушениях обработки персональных данных или требований по их защите, принимаемых мерах и способах устранения выявленных нарушений.

III. Ответственность лица, ответственного за организацию обработки персональных данных

3.1.В соответствии с законодательством Российской Федерации ответственный за организацию обработки персональных данных несёт дисциплинарную, административную и уголовную ответственность, за невыполнение или халатное выполнение обязанностей по

организации, контролю и обеспечению выполнения требований законодательства, нормативно правовых актов Российской Федерации по вопросам обработки и защиты персональных данных в Организации.

IV. Права ответственного за организацию обработки персональных данных

4.1. Ответственный за организацию обработки персональных данных имеет право:

-требовать от работников МБОУ СОШ № 7 г. Сальска письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

-вносить предложения руководителю МБОУ СОШ № 7 г. Сальска об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, в том числе об увольнении работников, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных информационных систем персональных данных в МБОУ СОШ № 7 г. Сальска

1. **Общие положения**

1.1.Настоящая инструкция определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных информационных систем персональных данных.

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Ответственный назначается приказом по МБОУ СОШ № 7 г. Сальска на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным в МБУО СОШ № 7 г. Сальска из числа штатных сотрудников

1.4. Ответственный подчиняется непосредственно Директору МБОУ СОШ № 7 г. Сальска

1.5. На время отсутствия Ответственного (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.6. Ответственный в своей работе руководствуется настоящей Инструкцией, Концепцией информационной безопасности, и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

1.7. Методическое руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в МБОУ СОШ № 7 г. Сальске

1.8. Ответственный является ответственным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию необходимого уровня защищенности ИСПДн в МБОУ СОШ № 7 г. Сальска и их ресурсов на этапах промышленной эксплуатации и модернизации.

2. **Организация работы**

2.1. Ответственный должен иметь специальное рабочее место, размещённое на территории МБОУ СОШ №7 г. Сальска, установленной приказом директора от «30» августа 2019 г. № 200\3 «О назначении ответственных лиц за обеспечение безопасности персональных данных в МБОУ СОШ № 7 г. Сальска», таким образом, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников МБОУ СОШ № 7 г. Сальска.

2.2. Рабочее место ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля технических средств защиты информации.

3. Обязанности

Ответственный должен:

3.1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки

персональных данных» и других нормативных документов в области обработки и защиты персональных данных.
3.2. Поддерживать необходимый уровень защищенности персональных данных при их обработке в ИСПДн согласно «Инструкции по обеспечению безопасности персональных данных».
3.3. Наделять и изменять права доступа всех групп пользователей ИСПДн к персональным данным и защищаемым программным ресурсам, и портам ввода-вывода ИСПДн.
3.4. Осуществлять установку, настройку и сопровождение программных и технических СЗИ.
3.5. Осуществлять методическое руководство всех групп пользователей в вопросах функционирования СЗИ и введенного режима защиты.
3.6. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
3.7. Участвовать в приемке новых программных и технических средств, в том числе СЗИ.
3.8. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений «Правил обработки персональных данных».
3.9. Обеспечить доступ к защищаемой информации всем группам пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
3.10. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.
3.11. Вести контроль над процессом осуществления резервного копирования баз данных и настроек комплекса средств автоматизации ИСПДн согласно «Инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных в РИСО, ФИС ФРДО.
3.12. Осуществлять контроль порядка учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.
3.13. Осуществлять контроль выполнения «Плана мероприятий по обеспечению защиты персональных данных в МБОУ СОШ № 7 г. Сальска».
3.14. Анализировать состояние защиты ИСПДн и их отдельных подсистем.
3.15. Контролировать неизменность состояния СЗИ, их параметров и режимов защиты.
3.16. Контролировать физическую сохранность СЗИ и оборудования ИСПДн.
3.17. Контролировать исполнение всеми группами пользователей ИСПДн введённого режима защищенности, а также правильность работы с элементами ИСПДн и СЗИ.
3.18. Контролировать исполнение всем группами пользователей ИСПДн парольной политики согласно «Инструкции по организации парольной защиты».
3.19. Организовывать антивирусную защиту всех элементов ИСПДн согласно «Инструкции по организации антивирусной защиты».
3.20. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.
3.21. Не допускать установку, использование, хранение и размножение в ИСПДн ПО, не связанных с выполнением функциональных задач.
3.22. Не допускать к работе на элементах ИСПДн посторонних лиц.
3.23. Регистрировать факты выдачи внешних носителей в «Журнале учета мобильных технических средств».
3.24. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.
3.25. Периодически представлять руководству отчёт о состоянии защиты АИС МБОУ СОШ № 7 г. Сальска СПО и о нештатных ситуациях на объектах ИСПДн и допущенных всеми группами пользователей нарушениях и установленных требований по защите информации.
3.26. В случае отказа работоспособности СЗИ ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
3.27. Принимать меры по реагированию в случае возникновения нештатных или аварийных ситуаций с целью ликвидации их последствий.

3.28. Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

4. Права

Ответственный имеет право

4.1. Требовать от всех групп пользователей ИСПДн соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов в области обработки и защиты персональных данных.

4.2. Запрещать всем группам пользователей ИСПДн доступ к персональным данным при нарушении «Правил обработки персональных данных», при неисправностях в работе СЗИ и с целью предотвращения несанкционированного доступа к охраняемой информации

4.3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4.4. Вносить предложения руководству по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

4.5. В пределах своей компетенции сообщать руководству о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению.

4.6. Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.

4.7. Привлекать с разрешения руководства сотрудников всех структурных подразделений к решению задач, возложенных на него.

4.8. Запрашивать лично или через директора МБОУ СОШ № 7 г. Сальска информацию и документы, необходимые для выполнения своих должностных обязанностей.

5.Ответственность

Ответственный несет ответственность:

5.1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

5.2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

5.3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

5.4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.5. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

ИНСТРУКЦИЯ
пользователя ИСПДн (информационных систем)
в МБОУ СОШ № 7 г. Сальска

1.Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник школы, 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 настоящей инструкцией, и нормативными документами школы.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

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 об организации работы с персональными данными в МБОУ СОШ № 7 г. Сальска.

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 инструкции по организации парольной защиты

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

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 школы, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору ИСПДн .

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн .

2.9. 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.

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

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

3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей ИСПДн

4.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.
4.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ИНСТРУКЦИЯ

по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных)

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых органом исполнительной власти (далее наименование ОИВ) для использования в ИС.
1.2. Действие настоящего Положения распространяется на сотрудников органа исполнительной власти, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

1. **Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
2. **АРМ** – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
3. **ИБ** – информационная безопасность – комплекс организационнотехнических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
4. **ИС** – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
5. **Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.
6. **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
7. **ПК** – персональный компьютер.
8. **ПО** – Программное обеспечение вычислительной техники.

9. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

10. **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

11. **Пользователь** – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС органа исполнительной власти понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью органа исполнительной власти и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным органам исполнительной власти носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители конфиденциальной информации предоставляются сотрудникам органа исполнительной власти по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника органа исполнительной власти производственной необходимости.

3.5. Процесс предоставления сотрудникам органа исполнительной власти носителей конфиденциальной информации состоит из следующих этапов:

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в органе исполнительной власти подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.4. Сотрудники органа исполнительной власти получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5. При использовании сотрудниками носителей конфиденциальной информации необходимо:

5.1. Соблюдать требования настоящего Положения.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

5.4. Бережно относится к носителям конфиденциальной информации.

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.
5.6. Извещать администраторов ИС о фактах утраты (кражи) носителей конфиденциальной информации.
6. При использовании носителей конфиденциальной информации запрещено:
6.1. Использовать носители конфиденциальной информации в личных целях.
6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).
6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
6.4. Выносить съемные носители с конфиденциальной информацией
(персональными данными) из служебных помещений для работы с ними на дому и т. д.
7.1. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником органа исполнительной власти между ИС и неучтенными (личными) носителями информации, рассматривается как **несанкционированное** (за исключением случаев оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.
7.2. Информация об использовании сотрудником органа исполнительной власти носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также Руководителю органа исполнительной власти.
7.3. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем органа исполнительной власти.
7.4. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Организации и действующему законодательству.
7.5. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.
7.6. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.
7.7. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.
7.8. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).
7.9. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется

«уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме

7.10. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

8. Ответственность

8.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами органа исполнительной власти.

ИНСТРУКЦИЯ
по организации резервного копирования

Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в информационной системе «АРМ государственная (итоговая) аттестация выпускников Муниципального бюджетного образовательного учреждения средней общеобразовательной школы № 7 г. Сальска, а также к резервированию аппаратных средств.

1.2. Настоящая Инструкция разработана с целью:

-определения категории информации, подлежащей обязательному резервному копированию; определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

-определения порядка восстановления информации в случае возникновения такой необходимости;

-упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационной системы в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

-персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений);

-информация, обрабатываемая пользователями в информационной системе, а также информация, необходимая для восстановления работоспособности информационной системы, в т.ч. систем управления базами данных общего пользования и справочно-информационные системы общего использования;

-рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения информационной системы;

-информация, необходимая для восстановления систем управления базами данных информационной системы;

-регистрационная информация системы информационной безопасности информационной системы;

-другая информация информационной системы, по мнению пользователей и Администратора безопасности информации, являющаяся критичной для работоспособности информационной системы.

1.5. Резервное копирование автоматизированных систем производится на основании следующих данных:

-состав и объем копируемых данных, необходимая периодичность проведения резервного копирования по форме:

Перечень резервируемой информации

№ п/п	Резервируемые ресурсы	Оценочный объем данных, Гб	Адрес хранения информации	Срок хранения резервной копии	Примечание*
1	**2**	**3**	**4**	**5**	**6**
1					
2					

* Описание резервируемой информации

-максимальный срок хранения резервных копий;

-требований к надежности и защищенности хранения резервных копий;

-требований к резервируемым аппаратным средствам информационной системы (при необходимости, в случае предъявления высоких требований к обеспечению доступности данных, обрабатываемых в информационной системе и значительного ущерба МСОШ№10 при нарушении заданных характеристик безопасности информации).

1.6. Резервные копии хранятся вне пределов помещения, в котором установлена рабочая станция, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники МБОУ СОШ № 7 г. Сальска, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам информационной системы.

Список лиц, имеющих доступ к резервируемым программным и аппаратным средствам информационной системы

№ п/п	Выполняемая роль	ФИО ответственного работника
1	**2**	**3**
1	Первоначальная настройка системы резервного копирования (создание медиа-сетов, расписаний, selection lists, оповещений). Запуск в эксплуатацию системы резервного копирования	
2	Внесение существенных изменений в настройку системы резервного копирования	
3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротации носителей	
4	Ротация носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне помещения на случай катастрофы	

Список лиц формируется на основании письменной заявки руководителя подразделения, согласованной с Администратором безопасности информации. Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании заявки руководителя подразделения, согласованной с Администратором безопасности информации.

О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается руководителю МСОШ№10 в течение рабочего дня после обнаружения указанного события.

Общие требования к резервному копированию

2.1. В настоящей Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:

-резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

-контроль резервного копирования:

-хранение резервных копий;

-полное или частичное восстановление данных.

2.2.Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.5. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

-это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

-имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:

-обеспечивает выполнение функций, перечисленных в п. 2.1;

-средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. Требования к программному обеспечению систем резервного копирования:

-лицензионное системное программное обеспечение и программное обеспечение резервного копирования;

-программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.5. Сопровождение системы резервного копирования возлагается на Администратора информационной системы, который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с инструкцией по эксплуатации.

2.6. Доступ к носителям архивных копий имеют только Администратор безопасности информации и Администратор информационной системы, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

Ответственность за состояние резервного копирования

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на Администратора информационной системы, осуществляющего резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора безопасности информации.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается руководителю МСОШ№10 в течение рабочего дня после обнаружения указанного события.

Периодичность резервного копирования

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после её изменения, но не реже одного раза в месяц.

4.3. Информация, содержащаяся в постоянно изменяемых базах данных МБОУ СОШ №7 г. Сальска, сохраняется в соответствии со следующим графиком:

-ежедневно проводится копирование изменённой и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;

-еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

-ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

Контроль результатов резервного копирования

5.1. Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности информации и Администратором информационной системы, в срок до 16 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает руководителю МБОУ СОШ № 7 г. Сальска до 17 часов текущего рабочего дня.

5.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем, располагающих необходимыми объемами дискового пространства для её хранения.

Ротация носителей резервной копии

6.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации информационной системы в случае отказа любого из устройств резервного копирования.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются Администратором информационной системы. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

Восстановление информации из резервных копий

7.1. В случае необходимости, восстановление данных из резервных копий производится Администратором информационной системы.

7.2. Восстановление данных из резервных копий происходит в случае её исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок пользователей и аппаратных сбоев.

7.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

7.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.
7.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.
7.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

ИНСТРУКЦИЯ

пользователей информационной системы персональных данных при возникновении нештатных ситуаций в МБОУ СОШ № 7 г. Сальска

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных в МБОУ СОШ № 7 г. Сальска, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.
2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.
3. Задачами данной Инструкции являются:
-определение мер защиты от прерывания работоспособности;
-определение действий по восстановлению в случае прерывания работоспособности.
4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на 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.
5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.
6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:
- Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;
- Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;
- Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.
7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.
8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности

оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.
9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, 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 вентиляции и кондиционирования;
-системы резервного питания.
Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.
Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных ИСПДн.
10. Ответственный за организацию обработки персональных данных:
- знакомит всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;
- обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.
11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных. Директор МБОУ СОШ № 7 г. Сальска согласует сроки и порядок их обучения.

Приложение 1
к Инструкции пользователя ИСПДн при возникновении нештатной ситуации

Источники угроз безопасности персональных данных
Технологические угрозы:
- Пожар в здании;
-Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
-Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);
-Химический выброс в атмосферу.
Внешние угрозы:
-Массовые беспорядки;
-Сбои общественного транспорта;
-Эпидемия;
-Массовое отравление персонала;
-Теракт.
Стихийные бедствия:
-Удар молнии;
-Сильный снегопад;
- Сильные морозы;
-Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;
-Затопление водой в период паводка;

- Наводнение, вызванное проливным дождем;
-Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).
ИТ-угрозы:
-Сбой системы кондиционирования в серверном помещении;
-Выход из строя файлового сервера ;
-Частичная потеря информации на сервере без потери его работоспособности;
-Выход из строя локальной сети;
-Выход из строя рабочей станции;
-Частичная потеря информации на рабочей станции без потери её работоспособности.
Угроза, связанная с человеческим фактором:
- Ошибка персонала, имеющего доступ к элементам ИСПДн;
-Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.
Угрозы, связанные с внешними поставщиками:
- Отключение электроэнергии;
-Сбой в работе интернет-провайдера;
-Физический разрыв внешних каналов связи.

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационной системе персональных данных

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационной системы персональных данных от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников подразделений, эксплуатирующих и сопровождающих информационную систему за их выполнение.
1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, прошедшие установленным образом процедуру оценки соответствия и централизованно закупленные у разработчиков (поставщиков) указанных средств.
1.3. Установка средств антивирусного контроля на компьютерах серверах ЛВС ИСПДн осуществляется администратором ИСПДн. Настройка параметров средств антивирусного контроля осуществляется администратором ИСПДн и контролируется администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех критичных областей ЭВМ (файлы автозагрузки, оперативная память, загрузочные сектора жестких дисков, каталоги операционных систем).
2.2. Обязательному антивирусному контролю подлежат любые файлы, которые могут содержать вредоносный код (анализ файлов производится по содержанию файлов, а не по файловому расширению), информация, получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM , DVD-ROM, Flash cards и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
2.3. Установка (изменение) системного и прикладного программного обеспечения осуществляется только Администратором ИСПДн.

2.4. Факт выполнения установки (изменения) программного обеспечения должен регистрироваться средствами СЗИ от НСД в специальном электронном журнале и контролируется подразделением по защите информации.

2.5. 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.) работник обязан привлечь Администратора ИСПДн для определения им факта наличия или отсутствия компьютерного вируса.