РФ

Муниципальное бюджетное общеобразовательное учреждение
«Стекляннорадицкая средняя общеобразовательная школа» Брянского района

Приказ

От 04 марта 2022 года **№ 52**

О принятии организационных мер по обеспечению безопасности персональных данных в информационных системах МБОУ «Стекляннорадицкая СОШ»

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказом МБОУ «Стекляннорадицкая СОШ» от 04 марта 2020 года № 51 «Об организации обработки персональных данных в МБОУ «Стекляннорадицкая СОШ»

ПРИКАЗЫВАЮ:

1. Утвердить положение о комиссии для организации работ по защите персональных данных в информационных системах МБОУ «Стекляннорадицкая СОШ» (Приложение № 1).
2. Утвердить Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» (Приложение № 2).
3. Утвердить Инструкцию пользователя информационных систем персональных данных МБОУ «Стекляннорадицкая СОШ» (Приложение № 3).
4. Утвердить Инструкцию по парольной защите информации в МБОУ «Стекляннорадицкая СОШ» (Приложение № 4).
5. Утвердить Инструкцию по организации антивирусной защиты информации в МБОУ «Стекляннорадицкая СОШ» (Приложение № 5).
6. Утвердить Инструкцию по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ» (Приложение № 6).
7. Утвердить Порядок обращения со съемными машинными носителями персональных данных в МБОУ «Стекляннорадицкая СОШ» (Приложение № 7).
8. Утвердить Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных в МБОУ «Стекляннорадицкая СОШ» (Приложение № 8).
9. Утвердить Положение о разрешительной системе доступа в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ» (Приложение № 9).
10. Утвердить Матрицу доступа работников к ресурсам информационных систем персональных данных МБОУ «Стекляннорадицкая СОШ» (Приложение № 10).
11. Ответственному за организацию обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» ознакомить с настоящим приказом заинтересованных лиц.
13. Контроль за исполнением настоящего приказа возложить на Колбасову Лидию Геннадьевну, заместителя директора по УВР.

Директор школы - _____ Панькевич С.В.

С приказом ознакомлены

Приложение 1

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

План проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ»

№	Мероприятие	Регулярность проведения
1.	Анализ актуальности локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных: – Проверка соответствия локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных МБОУ «Стекляннорадицкая СОШ» действующему законодательству РФ по защите персональных данных; – Учет в локальных нормативных актах (внутренних документах) по вопросам обеспечения безопасности персональных данных изменений в деятельности по обработке и защите персональных данных.	1 раз в три года или по мере обновления законодательства РФ
2.	Проверка ознакомления работников с положениями законодательства РФ по защите персональных данных, документами, определяющими политику МБОУ «Стекляннорадицкая СОШ» в отношении обработки персональных данных и организационно-распорядительными документами по вопросам персональных данных.	1 раз в год
3.	Проверка выполнения работниками – пользователями информационных систем персональных данных инструкций по эксплуатации информационных систем персональных данных, положения о разрешительной системе доступа.	1 раз в год
4.	Проверка актуальности прав разграничения доступа пользователей информационных систем персональных данных, необходимых для выполнения должностных обязанностей.	1 раз в год
5.	Проверка актуальности определенных угроз безопасности персональных данных для информационных систем персональных данных.	1 раз в год
6.	Проверка полноты реализованных технических мер по обеспечению безопасности персональных данных в информационных системах персональных данных с учетом структурно-функциональных характеристик информационных системах персональных данных, информационных технологий, особенностей функционирования информационных системах персональных данных.	1 раз в год
7.	Проверка наличия сертифицированных средств защиты информации, в случаях, когда применение таких средств	1 раз в год

№	Мероприятие	Регулярность проведения
	необходимо для нейтрализации актуальных угроз безопасности персональных данных.	
8.	Проверка правил обращения со съемными машинными носителями персональных данных.	1 раз в год
9.	Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.	1 раз в год
10.	Проверка соответствия условий использования средств криптографической защиты (при их использовании) условиям, предусмотренным эксплуатационной и технической документацией к ним.	1 раз в год
11.	Выявление уязвимостей в информационных системах персональных данных в т.ч. в системе защиты с использованием средства инструментального анализа защищенности.	1 раз в год

Приложение 2

Утверждено
приказом по
МБОУ «Стекляннорадицкая СОШ»
от 04.03.2022 № 52

АКТ

«___» _____ 20__ г. № _____

Брянск

О проведении контроля соответствия обработки
персональных данных

Комиссия в составе:
Председатель:
_____ _____
Члены комиссии:
1. _____ _____
2. _____ _____
3. _____ _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данныхв _____ *(Наименование организации)* требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

Таблица 1

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

Внутренний контроль проводился в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в _____ *(Наименование организации)* требованиям к защите персональных данных».

Председатель:
_____ _____ _____
Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

Приложение 3

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

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

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

Настоящая Инструкция пользователя информационных систем персональных данных МБОУ «Стекляннорадицкая СОШ» (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

Требования настоящей Инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных (далее – ПДн) в ИСПДн – пользователей ИСПДн (далее – Пользователи).

К защищаемой информации, обрабатываемой в ИСПДн МБОУ «Стекляннорадицкая СОШ» (далее – Учреждение), относятся ПДн, служебная

(технологическая) информация системы защиты и другая информация ограниченного доступа.

Все пользователи ИСПДн Учреждения должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с «Перечнем должностей работников МБОУ «Стекляннорадицкая СОШ», допущенных к обработке персональных данных».

К самостоятельной работе на автоматизированных рабочих местах (далее –АРМ), входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и локальных нормативных актов по защите информации, освоившие правила эксплуатации АРМ и технических средств защиты.

Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

4. Обязанности пользователя

Каждый Пользователь имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

4.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

4.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн.

4.3. Выполнять требования по антивирусной защите в части, касающейся действий Пользователей.

4.4. Немедленно ставить в известность ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн:

при подозрении компрометации личного пароля;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн;

некорректного функционирования установленных средств защиты;

обнаружения непредусмотренных отводов кабелей и подключенных устройств;

обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

4.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4.6. Пользователям ИСПДн запрещается:

отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;

производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;

работать в ИСПДн при обнаружении каких-либо неисправностей;

оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;

производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;

вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация работы со съемными машинными носителями информации

5.1. Организация работы со съемными машинными носителями информации (далее – СМНИ), содержащие ПДн и иную информацию конфиденциального характера, осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации в МБОУ «Стекляннорадицкая СОШ».

5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.

5.3. СМНИ должны быть зарегистрированы в «Журнале учета съемных машинных носителей информации».

5.4. СМНИ закрепляется за определенным лицом, несущим ответственность за сохранность и местонахождение данного СМНИ.

5.5. При необходимости передачи информации на СМНИ, лицо ответственное за хранение уведомляет ответственного за обеспечение безопасности ПДн в ИСПДн о необходимости передачи информации с помощью СМНИ, доставляет СМНИ по месту назначения, передает информацию с него и возвращает его на место хранения.

5.6. Хранение СМНИ осуществляется:

для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;

для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

5.7. Пользователям запрещается:

записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;

оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передачаСМНИ;

хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

6. Организация парольной защиты

6.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в МБОУ «Стекляннорадицкая СОШ».

6.2. Лица, использующие пароли, обязаны:

хранить в тайне свой пароль

четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;

своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

6.3. Во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в

прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.)

6.4. Для предотвращения доступа к персональным данным, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Delete и кнопки «Блокировать» или нажатием комбинации Win+L.

6.5. Блокирование сеанса доступа пользователя в ИСПДн осуществляется после 15 минут его бездействия (неактивности).

6.6. В случае утери пароля работник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

6.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

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

7.1. Работа в сетях общего доступа и на элементах ИСПДн, должна осуществляться исключительно в служебных целях.

7.2. При работе в сетях общего доступа запрещается:

осуществлять работу при отключенных средствах защиты;

передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;

запрещается скачивать из сети Интернет программное обеспечение и другие файлы, если это не определено его должностными обязанностями;

запрещается посещение и использование сети Интернет в личных целях.

8. Порядок установки обновлений программного обеспечения

8.1. Установке крупных обновлений программного обеспечения должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от устанавливаемых обновлений.

8.2. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно по согласованию с администратором ИСПДн.

8.3. Установке новых версий программного обеспечения или внесению серьезных изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

8.4. Установка протестированных обновлений, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение может быть произведено только по согласованию с администратором ИСПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

9. Технология обработки персональных данных

9.1. При первичном допуске к работе в ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает Инструкцию, получает персональный идентификатор или личный пароль у ответственного за обеспечение безопасности ПДн в ИСПДн.

9.2. В процессе работы Пользователь производит обработку ПДн в ИСПДн.

9.3. При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

копированием ПДн на учтенные СМНИ;

передача ПДн по каналам связи с обязательным применением средств криптографической защиты.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ИНСТРУКЦИЯ
по парольной защите информации в МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

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

1.3. 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.

1.4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

1.6. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество· или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по парольной защите информации в МБОУ «Стекляннорадицкая СОШ» (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн МБОУ «Стекляннорадицкая СОШ» (далее – Учреждение), использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под роспись.

2.4. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

3.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

3.2. Требования к формированию паролей и обращению с ними.

3.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

3.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

3.2.3. Пароли генерируются с учетом следующих требований:

–пароль должен знать только его владелец;

–длина пароля должна быть не менее 8 символов;

–в пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;

–пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);

–максимальный срок действия пароля составляет 120 дней;

–минимальный срок действия пароля составляет 2 дня;

–количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

3.2.4. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

3.2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

3.2.6. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.

3.2.7. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. По возвращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).

3.3. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

3.3.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.

3.3.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.

3.4. Порядок действий при компрометации идентификаторов и паролей.

3.4.1. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).

3.4.2. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.

4. Права и обязанности

4.1. Основные задачи администратора ИСПДн:

- организация установки средств идентификации и аутентификации;
- организация парольной защиты во всех ИСПДн;
- выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
- осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.

4.2. Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
- принимать участие в планировании мероприятий по парольной защите информации в ИСПДни планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
- инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

4.3. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.

4.4. Пользователям ИСПДн в своей работе запрещается:

- сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;
- осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

4.5. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного заобеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.

5.Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.2. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ИНСТРУКЦИЯ
по антивирусной защите МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

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

1.4. 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.

1.5. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

1.7. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.8. Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.9. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по антивирусной защите МБОУ «Стекляннорадикая СОШ» (далее – Инструкция) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля.

2.2. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

2.3. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками МБОУ «Стекляннорадикая СОШ» (далее – Учреждения), использующими в своей работе средства вычислительной техники.

2.4. Все работники Учреждения, использующие антивирусные средства, должны быть ознакомлены с требованиями настоящей Инструкцией под роспись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования к антивирусным средствам

3.1. В Учреждении к применению допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров.

3.2. Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

3.3. Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн).

4. Права и обязанности

4.1. Антивирусной защите подлежит вся обрабатываемая в Учреждении при помощи средств вычислительной техники, информация, независимо от ограничений доступа к ней.

4.2. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

4.4. В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

4.5. Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на ответственного за обеспечение безопасности ПДн в ИСПДн.

4.6. Основные задачи ответственного за обеспечение безопасности ПДн в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;
- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);
- контроль состояния системы антивирусной защиты информации в Учреждении.

4.7. Ответственный за обеспечение безопасности ПДн в ИСПД несет ответственность за:

- за своевременную установку антивирусных средств;
- за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;
- за своевременное обновление лицензий на антивирусные средства;
- за своевременное обновление антивирусных баз.

4.8. Ответственный за обеспечение безопасности ПДн в ИСПДнимеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;
- осуществлять контроль состояния средств антивирусной защиты информации в Учреждении;
- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

4.9. Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство.

4.10. Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;
- использовать средства антивирусной защиты, отличные от установленных средств;
- без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5. Порядок и периодичность обновления антивирусных баз

5.1. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

5.2. Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

5.3. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения.

5.4. Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика

антивирусного средства, либо собственный централизованный сетевой *источник обновлений, получающий обновления с сервера разработчика* антивирусного средства.

- обновление антивирусных баз для ИСПДн, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.

6. Порядок и периодичность проведения антивирусного контроля

6.1. Объектами антивирусного контроля являются:

- жесткие магнитные диски рабочих станций и серверов ИСПДн;
- сетевые хранилища (системы хранения данных);
- оперативная и системная память средств вычислительной техники;
- съемные машинные носители информации;
- входящий и исходящий контент (веб-трафик);
- файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена;
- почтовые сообщения электронной почты.

6.2. Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверятся во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

6.3. Виды и периодичность антивирусных проверок представлены в таблице 1.

Таблица 1

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
1	Жесткие магнитные диски рабочих станций и серверов ИСПДн	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
2	Сетевые хранилища (системы хранения данных)	Полная проверка	1 раз в месяц
3	Оперативная и системная память средств вычислительной техники	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
4	Съемные машинные носители информации	Полная проверка	При каждом подключении

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
5	Веб-трафик	Минимально необходимое требование - настройка антивирусного средства по умолчанию	Постоянно
6	Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена	Полная проверка	При каждом получении и отправке
7	Почтовые сообщения электронной почты	Минимально необходимое требование - настройка антивирусного средства по умолчанию	При каждом получении и отправке

7. Порядок действий при обнаружении вирусов

7.1. Основными путями проникновения вирусов в ИСПДн являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

7.2. В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своей рабочей станции;
- сообщить ответственному за обеспечение безопасности ПДн в ИСПДн о факте обнаружения вируса;
- принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

7.3. При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности ПДн в ИСПД необходимо:

- сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации.

7.4. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

7.5. Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

7.6. Служебное расследование проводится комиссией, назначаемой приказом ДиректораУчреждения. В состав комиссии в обязательном порядке включается администратор ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие работники.

7.7. Результаты работы комиссии оформляются актом. Акт подлежит утверждению ДиректораУчреждения.

7.8. В процессе работы комиссии обязательными для установления являются:

- дата и время заражения (обнаружения заражения);
- ФИО, должность и подразделение работника, техническое средство которого заражено вирусной программой;
- уровень критичности заражения;
- обстоятельства, способствовавшие заражению;
- информационные ресурсы, затронутые заражением;
- характер и размер реального и потенциального ущерба.

7.9. В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

7.10. Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел.

8. Ответственность

8.1. Пользователи и Ответственный за обеспечение безопасности ПДн в ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

Приложение 6

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ИНСТРУКЦИЯ
по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

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

1.3. 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.

1.4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

1.6. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.7. Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.8. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ» (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) МБОУ «Стекляннорадицкая СОШ» (далее – Учреждение), а также к резервированию аппаратных средств.

2.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн 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.

2.3. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения технических средств;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных.

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

2.5. Резервному копированию подлежит информация следующих основных категорий:

- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования;
- рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация систем защиты информации;
- другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.

2.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Общие требования к резервному копированию

3.1. В 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.

3.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования. Система резервного копирования должна обеспечить производительность, достаточную для сохранения информации, указанной в п. 2.5, в установленные сроки и с заданной периодичностью.

3.3. Требования к техническому обеспечению систем резервного копирования:

- комплекс взаимосвязанных технических средств на единой технологической платформе, обеспечивающих процессы сбора, передачи, обработки и хранения информации;
- 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. 3.1.

3.4. 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.

3.5. Хранение отдельных магнитных носителей архивных копий организуется в отдельном хранилище. Физический доступ к архивным копиям строго ограничен.

3.6. Доступ к носителям архивных копий имеют только уполномоченные работники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то полномочий.

3.7. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательным составлением акта об уничтожении.

4. Ответственность за состояние резервного копирования

4.1. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

4.2. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.

5. Периодичность резервного копирования

5.1. 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.

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

5.3. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной 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.

5.4. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.

6. Восстановление информации из резервных копий

6.1. В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

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

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

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. 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.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ПОРЯДОК
обращения со съемными машинными носителями персональных данных в МБОУ «Стекляннорадицкая СОШ».

1. Термины и определения

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

Съемный машинный носитель персональных данных – сменный носитель персональных данных, предназначенный для записи и считывания персональных данных, представленных в стандартных кодах;

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;

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Порядок обращения со съемными машинными носителями персональных данных в МБОУ «Стекляннорадицкая СОШ» (далее – Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Порядок определяет:

- Правила обращения со съемными машинными носителями информации, в том числе и ПДн (далее – СМНИ);
- Порядок организации учета СМНИ;
- порядок уничтожения СМНИ.

2.3. Под СМНИ в настоящем Порядке понимаются следующие носители информации:

- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (флэш-память, съемные жесткие диски);
- иные носители информации.

2.4. Требования настоящего Порядка являются обязательными для исполнения всеми работниками МБОУ «Стекляннорадицкая СОШ» (далее – Учреждение), использующими в своей работе СМНИ.

2.5. Все работники Учреждения, использующие СМНИ, должны быть ознакомлены с требованиями настоящим Порядком под роспись.

2.6. Настоящий Порядок является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности

сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

2. Правила обращения со съемными машинными носителями персональных данных

3.1. Обращение со СМНИ должно осуществляется таким образом, чтобы исключались их утрата, порча и несанкционированный доступ к ним посторонних лиц.

3.2. При обращении со СМНИ, выполняются следующие основные правила:

- СМНИ учитываются и выдаются под роспись;
- СМНИ, срок эксплуатации которых истек, уничтожаются в установленном порядке;
- для выноса СМНИ за пределы контролируемой зоны, запрашивается специальное разрешение у ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный), а факт выноса фиксируется;
- право на перемещение СМНИ за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- все СМНИ должны хранится в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособленными для опечатывания замочных скважин или кодовыми замками;
- допускается хранение СМНИ вне сейфов (металлических шкафов) при условиях уничтожения (стирания) ПДн и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации, либо если на съемном машинном носителе ПДн хранятся только ПДн в зашифрованном виде с использованием средств криптографической защиты информации.

3.3. СМНИ должен использоваться, не более срока эксплуатации, установленного изготовителем материального носителя.

3. Порядок хранения и учета съемных машинных носителей персональных данных

4.1. СМНИ, должны иметь специальную маркировку. Тип маркировки выбирается Ответственным.

4.2. Все находящиеся на хранении и в обращении СМНИ учитываются Ответственным в «Журнале учета съемных машинных носителей персональных данных в МБОУ «Стекляннорадицкая СОШ»., форма которого установлена в Приложении 1 к настоящему Порядку.

4.3. В нерабочее время и время отсутствия необходимости использования ПДнСМНИ должны храниться в хранилищах СМНИ.

4.4. Перечень хранилищ определяется в «Журнале учета хранилищ носителей персональных данных в МБОУ «Стекляннорадицкая СОШ».

4.5. Пользователи для выполнения работ получают СМНИ у Ответственного. При получении делаются соответствующие записи в «Журнале учета съемных машинных носителей персональных данных в МБОУ «Стекляннорадицкая СОШ»

4. Порядок уничтожения съемных машинных носителей персональных данных

5.1. Уничтожение ПДн производится только в следующих случаях:

- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.

5.2. СМНИ, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

5.3. Уничтожение СМНИ осуществляется комиссией по уничтожению, назначенной приказом Директора Учреждения.

5.4. При уничтожении СМНИ необходимо:

- убедиться в необходимости уничтожения СМНИ;
- убедиться в том, что уничтожаются только та информация, которая предназначена для уничтожения;
- уничтожить СМНИ подходящим способом, в соответствии с настоящим Порядком или способом, указанным в соответствующем требовании или распорядительном документе.

5.5. При уничтожении СМНИ применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов, исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) информации, подлежащей уничтожению – для сохранения возможности обработки иных данных, зафиксированных в документе;
- измельчение в специальной мультирезательной (мультиуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для СМНИ на оптических дисках;
- физическое уничтожение частей СМНИ – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

5.6. По результатам уничтожения СМНИ комиссией составляется «Акт уничтожения съемных машинных носителей персональных данных», форма которого установлена в Приложении 2 к настоящему Порядку.

5. Ответственность

6.1. Ответственным за хранение, учет и выдачу СМНИ, является Ответственный.

6.2. Все работники Учреждения, использующие СМНИ и Ответственный несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

Приложение 1

к порядку обращения со съемными машинными носителями персональных данных в _____ *(Наименование организации)*

ФОРМА

Журнал учета съемных машинных носителей персональных данных

в _____ *(Наименование организации)*

№ п/п	Тип носителя	Номер (серийный/ инвентарный)	Отметка о получении			Подпись ответственного лица	Место хранения	Примечание	Дата и номер акта уничтожения
			ФИО	Дата	Подпись				
1	2	3	4	5	6	7	8	9	10

Приложение 2
к Порядку обращения со съемными машинными носителями персональных данных в _____ *(Наименование организации)*

ФОРМА

АКТ

«___» _____ 20__ г. № _____

Брянск

Об уничтожении съемных машинных носителей персональных данных

Комиссия в составе:
Председатель:
_____ _____

Члены комиссии:
1. _____ _____
2. _____ _____
3. _____ _____

составили настоящий акт о том, что в результате проведеннойэкспертной оценки подлежат уничтожению следующие съемные машинные носители персональных данных:

№ п/п	Дата окончания срока обработки зафиксированных на носителе персональных данных	Учетный номер съемного носителя или наименование технического средства, на котором уничтожаются файлы	Примечание
1	2	3	4

Всего съемных носителей_____
(цифрами и прописью)

Перечисленные съемные носители уничтожены путем_____
(механического уничтожения, сжигания, разрезания, деформирования и т.п.)

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

Приложение 8

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

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

1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

1.3. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.4. 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.

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

1.6. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ» (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее –ИСПДн).

2.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

2.3. Регламент обязателен для исполнения всеми работниками МБОУ

«Стекляннорадицкая СОШ» (далее – Учреждение), непосредственно осуществляющими защиту ПДн в ИСПДн.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:

- несоблюдение требований по защите ПДн:
  - использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
  - утрата носителя ПДн;
  - утрата ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков.
- попытки НСД к ПДн:
  - подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
  - изменение настроек, состава, паролей технических средств ИСПДн;
  - изменение (увеличение) полномочий доступа;
  - нарушение целостности установленных защитных пломб;
  - копирование ПДн на неучтенные съемные носители ПДн;
  - заражение рабочего места и/или сервера ИСПДн вредоносной программой;
  - хищение носителей ПДн;
  - хищение технических средств ИСПДн;
  - умышленное нарушение работоспособности технических средств ИСПДн;
  - хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
  - несанкционированное проникновение в помещения ИСПДн;
  - очистка электронных журналов мониторинга.
- сбои в работе технических средств ИСПДн Общества.

3.2. К инцидентам ИБ не относятся:

- неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
- неудачные попытки заражения рабочих мест и/или серверов ИСПДн вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ

4. Порядок регистрации событий безопасности

4.1. Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
3) Сбор, запись и хранение информации о событиях безопасности.
4) Реагирование на сбои при регистрации событий безопасности.
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
6) Генерирование временных меток и (или) синхронизация системного времени в ИСПДн.
7) Защита информации о событиях безопасности.

4.2. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДн для ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность

нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).

4.3. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.

4.4. В ИСПДн подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
- подключение съемных машинных носителей ПДн и вывод ПДн на носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
- обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
- попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

4.5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

4.6. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

4.7. При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.

4.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДн состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4.9. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

4.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа

к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

4.11. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.

4.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДни (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 4.6–4.11настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3настоящего Регламента.

4.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 4.7 – 4.11настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

4.14. В ИСПДндолжно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

4.15. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения Ответственным за обеспечение безопасности ПДн в ИСПДни (или) Администратором ИСПДнпараметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

4.16. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в ИСПДн.

4.17. В случае выявление признаков инцидентов информационной безопасности в ИСПДн осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИСПДн.

4.18. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИСПДн, достигается посредством применения внутренних системных часов ИСПДн.

4.19. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

4.20. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за обеспечение безопасности ПДн в ИСПДн;
- администратору ИСПДн.

5. Порядок выявления инцидентов информационной безопасности и реагирования на них

5.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за обеспечение безопасности ПДн в ИСПДн;
- администраторИСПДн.

5.2. Работники Учреждения, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработкаПДн, и к хранилищам ПДн;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн.

5.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в МБОУ «Стекляннорадицкая СОШ», форма которого установлена в Приложении 1 к настоящему Регламенту или в электронные журналы операционной системы и СЗИ.

5.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн.

5.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентовинформационной безопасности.

6. Основные этапы процесса реагирования на инциденты

6.1. Лица, занимающиеся реагированием на инциденты, должны обеспечить защиту ИСПДн и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.

6.2. Лица, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов программного обеспечения и другие источники

информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы.

6.3. Лица, занимающиеся реагированием на инциденты, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИСПДн могли продолжать работать без зараженных машин.

6.4. Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИСПДн.

6.5. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и ИСПДн в целом, чтобы убедиться в полном устранении угрозы.

6.6. Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

7. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

– Проведение разбирательств по фактам возникновения инцидентов информационной безопасности осуществляет Комиссия для организации работ по защите персональных данных в информационных системах МБОУ «Стекляннорадицкая СОШ», состав которой утверждается приказом руководителя МБОУ «Стекляннорадицкая СОШ».

7.1. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение руководителю МБОУ «Стекляннорадицкая СОШ».

7.2. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- тналичие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;
-цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

7.3. В целях проведения разбирательства все работники обязаны по требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

7.4. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

7.5. Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

7.6. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

7.7. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

7.8. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения сведений;
- лица, виновные в разглашении сведений;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ПДн;
- иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

7.9. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

7.10. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

7.11. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

ПОЛОЖЕНИЕ
о разрешительной системе доступа в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ»

1. Термины и определения

1.1. Дискреционный метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

1.2. Доступ к информации - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

1.3. Матрица доступа – таблица, отображающая правила разграничения доступа.

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

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

1.6. Ролевой метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

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

1.9. Типы доступа – операции, разрешенные к выполнению субъектом доступа при доступе к объектам доступа.

2. Общие положения

2.1. Настоящее Положение о разрешительной системе доступа в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ» (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа в ИСПДн.

2.3. Положение обязательно для исполнения всеми работниками МБОУ «Стекляннорадицкая СОШ» (далее –Учреждение), непосредственно осуществляющими защиту ПДн.

3. Субъекты и объекты доступа

3.1. К субъектам доступа ИСПДн, относятся работники, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИСПДн в соответствии с должностными инструкциями и которым в ИСПДн присвоены учетные записи.

3.2. К объектам доступа в ИСПДн, относятся:

- средства вычислительной техники;
- средства связи и передачи данных;

- средства обеспечения бесперебойной работы средств вычислительной техники и средств связи и передачи данных;
- основные конфигурационные файлы операционных систем, средств связи и передачи данных и средств защиты информации (далее – СЗИ);
- средства настройки и управления операционной системой, средств связи и передачи данных и СЗИ;
- прикладное программное обеспечение;
- периферийные устройства;
- машинные носители информации;
- обрабатываемые, хранимые данные.

4. Методы разграничения доступа

4.1. Методы разграничения доступа к ИСПДн реализуются в соответствии с особенностями функционирования ИСПДн и включают комбинацию следующих методов:

- ролевой метод управления доступом;
- дискреционный метод управления доступом.

4.2. Реализация ролевого метода управления доступом в ИСПДн представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор безопасности	- обладает полной информацией о конфигурации системы защиты ПДн (структуре системы защиты ПДн, составе, местах установки и параметров настройки СЗИ); - обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств); - обладает правами настройки и конфигурирования СЗИ; - обладает правами настройки и конфигурирования средств связи передачи данных; - обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; - обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения.
2	Администратор	- обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, составе, местах установки и параметров программного обеспечения и технических средств); - обладает правами настройки и конфигурирования средств связи передачи данных; - обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; - обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения.
3	Пользователь	- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ИСПДн.

4.3. Реализация дискреционного метода управления доступом достигается путем назначения прав доступа для каждой пары «Роль субъекта доступа» – «Объект доступа» явного и недвусмысленного перечисления допустимых типов доступа в соответствии с

Матрицей доступа работников к ресурсам информационных систем персональных данных (далее – Матрица доступа),форма которой установлена в Приложении к настоящему Положению.

5. Типы доступа

5.1. В ИСПДн определены следующие типы доступа субъектов доступа к объектам доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) – субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.

5.2. Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в ИСПДн, типы доступа, определены в Матрице доступа.

6. Правила разграничения доступа

6.1. В ИСПДн правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам доступа в ИСПДн:

- разделение обязанностей и назначение минимально необходимых прав пользователям и администраторам;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей ИСПДн;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками в ИСПДн;
- ограничение неуспешных попыток доступа в ИСПДн;
- разрешение (запрет) действий пользователей ИСПДн, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- контроль использования в ИСПДн технологий беспроводного доступа;
- контроль использования в ИСПДн мобильных технических средств;
- управление взаимодействием с ИСПДн организаций (внешние информационные системы).

6.2. Права и обязанности пользователей зафиксированы в «Инструкции пользователя информационных систем персональных данных МБОУ «Стекляннорадицкая СОШ»

6.3. Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей ИСПДн, осуществляет администратор ИСПДн.

6.4. Администратор ИСПДн определяет и назначает права доступа субъектов к объектам доступа в ИСПДн в соответствии с исполняемой ролью субъекта в ИСПДн и Матрицей доступа.

6.5. В ИСПДн реализованы следующие функции управления учетными записями пользователей ИСПДн:

- определение типа учетной записи (пользователь, администратор, системная);
- объединение учетных записей в группы (пользователи, администраторы);
- верификация пользователя при заведении учетной записи пользователя;

- заведение, активация, блокирование и уничтожение учетных записей пользователей ИСПДн;
- пересмотр и корректировка учетных записей пользователей ИСПДн;
- порядок заведения и контроля использования временных учетных записей Пользователей ИСПДн;
- оповещение администратора ИСПДн, осуществляющего управление учетными записями пользователей ИСПДн, об изменении сведений о пользователях ИСПДн, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей ИСПДн, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн;
- предоставление пользователям ИСПДн прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых пользователями ИСПДн.

6.6. Временная учетная запись может быть заведена для пользователя ИСПДн на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям ИСПДн с временным доступом к ИСПДн).

6.7. В ИСПДн осуществляется автоматическое блокирование временных учетных записей Пользователей ИСПДн по окончании установленного периода времени для их использования.

6.8. При передаче информации между устройствами, сегментами в рамках ИСПДн, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в ИСПДн только по установленному маршруту;
- изменение (перенаправление) маршрута передачи информации только в установленных случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях.

6.9. Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между пользователями ИСПДн, устройствами, сегментами в рамках ИСПДн, а также при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИСПДн, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

6.10. Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционировано исходящие из ИСПДн и (или) входящие в ИСПДн.

6.11. В ИСПДн установлено и зафиксировано в «Инструкции по парольной защите информации в МБОУ «Стекляннорадицкая СОШ»:

- количество неуспешных попыток входа (доступа) ИСПДн за установленный период времени;
- блокирование сеанса доступа пользователя ИСПДн после установленного времени его бездействия (неактивности).

6.12. В ИСПДн обеспечивается блокирование сеанса доступа пользователя ИСПДн по запросу.

6.13. Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

6.14. Администратору ИСПДн и ответственномуза обеспечение безопасности ПДн в ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

6.15. Регламентация и контроль использования съемных машинных носителей ПДн, описаны в «Порядке обращения со съемными машинными носителями персональных данных в МБОУ «Стекляннорадицкая СОШ» .

6.16. В ИСПДн при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования ИСПДн, предоставление доступа к ИСПДн осуществляется только авторизованным (уполномоченным) пользователям ИСПДн в соответствии с Матрицей доступа.

7. Ответственность

7.1. Все работники Учреждения, осуществляющие обработку и защиту ПДн обязаны ознакомиться с данным Положением под роспись.

7.2. Работники Учреждения несут персональную ответственность за выполнение требований настоящего Положения.

7.3. Контроль выполнения работниками Учреждения правил разграничения доступа в ИСПДн осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн.

Приложение
к Положению о разрешительной системе доступа в информационных системах персональных данных

ФОРМА

Матрица доступа
субъектов к ресурсам информационных систем персональных данных
МБОУ «Стекляннорадицкая СОШ»

Субъект доступа	Объект доступа								
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные	Настройки BIOS / UEFI
Администратор									
Администратор безопасности									
Пользователь									

Типы доступа:
чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
печать (P) – субъекту доступа разрешена печать;
сканирование (S) – субъекту доступа разрешено сканирование;
полный (F) – субъект доступа имеет полный доступ к объектам доступа.

Приложение №10
к приказу МБОУ
«Стекляннорадицкая СОШ»
от «04» марта 2022 г. № 52

Матрица доступа
субъектов к ресурсам информационных систем персональных данных
_____ *(Наименование организации)*

Субъект доступа	Объект доступа								
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные	Настройки BIOS / UEFI
Администратор	F	F	-	-	F	P/S	-	-	F
Администратор безопасности	F	F	F	F	F	P/S	F	F	F
Пользователь	R-E	-	-	-	R-E	P/S	F	F	-

Типы доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» требованиям к защите персональных данных

1. Термины и определения

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

1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.

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

1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» требованиям к защите персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.

2.3. Регламент обязателен для исполнения ответственным за организацию обработки ПДн, ответственным за обеспечение безопасности ПДн и администратором информационных систем персональных данных.

3. Порядок проведения внутреннего контроля

3.1. Внутренний контроль в ИСПДн осуществляет комиссия для организации работ по защите персональных данных в информационных системах МБОУ

«Стекляннорадицкая СОШ», состав которой утверждается приказом директора учреждения.

3.2. Допускается привлечение к проверкам сторонних экспертных организаций.

3.3. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Учреждения, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение директору Учреждения.

3.4. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом МБОУ «Стекляннорадицкая СОШ», форма которого приведена в Приложении 1 к настоящему Регламенту.

3.5. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.

3.6. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Учреждения, осуществляющих обработку ПДн, осматривает рабочие места.

3.7. При проведении внутреннего контроля должен присутствовать руководитель проверяемого подразделения.

3.8. В ходе проведения внутреннего контроля осуществляется:

- контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
- анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
- проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
- контроль состава технических средств, программного обеспечения и СЗИ;
- состояние учета СЗИ;
- состояние учета средств шифровальной (криптографической) защиты информации;
- состояние учета съемных машинных носителей ПДн;
- соблюдение правил доступа к ПДн;
- контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
- соблюдение пользователями ИСПДн парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн;
- контроль соблюдения работниками требований локальных нормативных актов, в т.ч. требований законодательства по вопросам обработки и защиты ПДн;
- выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности.

3.9. Все работники обязаны по требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.

3.10. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого приведена в Приложении 2 к настоящему Регламенту.

3.11. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:

- перечень проведенных мероприятий;
- выявленные нарушения;
- мероприятия по устранению нарушений;
- решения по результатам внутреннего контроля;
- сроки устранения нарушений.

3.12. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.

3.13. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются Руководителю МБОУ «Стекляннорадицкая СОШ» ответственным за организацию обработки ПДн и ответственнымза обеспечение безопасности ПДн в ИСПДн.

3.14. Внеплановый контроль проводится в следующих случаях:

- наличие подозрений на нарушение требований по защите ПДн;
- наличие подозрений на осуществление попыток несанкционированного доступа к ПДн;
- наличие подозрений на сбой в работе технических средств ИСПДн, в т.ч. средств защиты информации;
- предстоящая проверка надзорными органами.

3.15. Порядок проведения внепланового контроля совпадает с порядком проведения планового контроля.

3.16. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите ПДн осуществляется оперативное устранение выявленных нарушений.

3.17. Выявленные нарушения должны быть устранены в срок не превышающий 30 дней с момента утверждения «Акта о проведении контроля соответствия обработки персональных данных».

3.18. По истечению срока, данного на устранение замечаний, комиссия проводит повторный контроль.

4. Ответственность

4.1. Ответственный за организацию обработки ПДн в Учреждении несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в Учреждении требованиям к защите ПДн.

Принято на педагогическом совете
Протокол от 04.03.2022 № 04

Утверждено
приказом по МБОУ «Стекляннорадицкая СОШ» от 04.03.2022 № 52

Положение
о комиссии по защите персональных данных в информационных системах МБОУ « Стекляннорадицкая СОШ»

1.Комиссии при работе руководствуется следующими нормативными документами:

– Федеральным законом от 27 июля 2006 г. №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»;

– приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Порядком обращения со съемными машинными носителями персональных данных в МБОУ «Стекляннорадицкая СОШ»;

– Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» требованиям к защите персональных данных;

- Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБОУ «Стекляннорадицкая СОШ».

1. Комиссии необходимо:

– определить уровень защищенности персональных данных, обрабатываемых в информационных системах в соответствии с 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»;

– провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации в области персональных данных;

– отбирать и уничтожать материальные носители персональных данных, обработка которых в МБОУ «Стекляннорадицкая СОШ» прекращена;

– проводить внутренний контроль соответствия обработки персональных данных в соответствии с планом, утвержденном в «Регламенте проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Стекляннорадицкая СОШ» требованиям к защите персональных данных»;

– проводить разбирательства по фактам возникновения инцидентов информационной безопасности, фиксировать их в журнале учета нештатных ситуаций и своевременно реагировать на инциденты информационной безопасности в информационных системах персональных данных.