РЕСПУБЛИКА КРЫМ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ

(МИНОБРАЗОВАНИЯ КРЫМА)

П Р И К А З

03. 02. **2026 г.** **№** 148

г. Симферополь

Об обеспечении информационной безопасности при проведении ГИА в 2026 году

В соответствии с федеральными законами от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 29.11.2021 № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования», приказами Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки от 04.04.2023 № 232/551 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования», от 04.04.2023 № 233/552 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования», приказами Федеральной службы по надзору в сфере образования и науки от 11.06.2021 № 805 «Об установлении требований к составу и формату сведений, вносимых и передаваемых в процессе репликации в федеральную информационную систему обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для

получения среднего профессионального и высшего образования и региональные информационные системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, а также к срокам внесения и передачи в процессе репликации сведений в указанные информационные системы», приказами Министерства образования, науки и молодежи Республики Крым от 03.10.2025 № 1491 «Об утверждении Дорожной карты «Организация и проведение государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Республике Крым в 2026 году», от 28.10.2025 № 1610 «О внесении сведений в Региональную информационную систему обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования», от 27.01.2026 № 115 «О создании Регионального центра обработки информации в Республике Крым в 2026 году», в целях обеспечения соблюдения информационной безопасности при подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Республике Крым в 2026 году

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обеспечении информационной безопасности при подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в 2026 году (далее – Положение) (прилагается).

2. Государственному казенному учреждению Республики Крым «Центр оценки и мониторинга качества образования» (Типакова Е.О.), выполняющему функции Регионального центра обработки информации (далее – РЦОИ):

2.1. Организовать мероприятия по соблюдению информационной безопасности при подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования (далее – ГИА) согласно Положению, утверждённому пунктом 1 настоящего приказа.

2.2. Осуществить организационно-технические и технологические мероприятия по обеспечению информационной безопасности в РЦОИ.

2.3. Осуществить консультационно-методическое сопровождение организационно-технических, технологических мероприятий по обеспечению информационной безопасности в органах управления образованием муниципальных районов, муниципальных и городских округов Республики Крым, пунктах проведения экзаменов.

2.4. Обеспечить меры по соблюдению особого пропускного режима в РЦОИ в период подготовки и проведения ГИА.

2.5. Обеспечить соблюдение условий конфиденциальности и требований информационной безопасности при работе с экзаменационными материалами.

3. Руководителям органов управления образованием муниципальных районов, муниципальных и городских округов Республики Крым:

3.1. Принять меры по обеспечению информационной безопасности при проведении мероприятий по организации и проведению ГИА в общеобразовательных организациях согласно Положению, утверждённому пунктом 1 настоящего приказа.

3.2. Обеспечить соблюдение мер информационной безопасности при получении, учете, хранении, доставке и приемке-передаче экзаменационных материалов и иных документов, используемых при проведении ГИА.

3.3. Обеспечить техническую защиту информации муниципального сегмента региональной информационной системы обеспечения проведения ГИА и пунктов проведения экзаменов.

3.4. Организовать проведение инструктажа лиц, привлекаемых к проведению ГИА по соблюдению требований информационной безопасности.

3.5. Обеспечить доступ к персональным данным, содержащимся в Региональной информационной системе «Планирование ГИА» (далее – РИС ГИА) и обработку указанных данных в соответствии с федеральным законодательством.

4. Руководителям государственных общеобразовательных организаций, находящихся в ведении Министерства образования, науки и молодежи Республики Крым:

4.1. Принять меры по обеспечению информационной безопасности при проведении мероприятий по подготовке и организации проведения ГИА согласно Положению, утверждённому пунктом 1 настоящего приказа.

4.2. Организовать проведение инструктажа лиц, привлекаемых к проведению ГИА по соблюдению требований информационной безопасности.

4.3. Обеспечить доступ к персональным данным, содержащимся в РИС ГИА, и обработку указанных данных в соответствии с федеральным законодательством.

5. Контроль за исполнением приказа возложить на заместителя министра образования, науки и молодежи Республики Крым Беспалову С.Э.

Министр **В.В. Лаврик**

Приложение к приказу
Министерства образования, науки и
молодежи Республики Крым
от 03.02.2026 г. № 148

Положение
об обеспечении информационной безопасности при подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в 2026 году

1. Общие положения

1.1. Положение об обеспечении информационной безопасности при подготовке и проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в 2026 году (далее – Положение) разработано в соответствии с:

– Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– постановлением Правительства Российской Федерации от 29 ноября 2021 года № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;

– приказом Министерства Просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) от 4 апреля 2023 года № 233/552 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования»;

– приказом Министерства Просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) от 4 апреля 2023 года № 232/551 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования»;

– приказом Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) от 11 июля 2021 от № 805 «Об установлении требований к составу и формату сведений, вносимых и передаваемых в процессе репликации в федеральную информационную систему обеспечения проведения государственной итоговой аттестации обучающихся, освоивших

основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональные информационные системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, а также к срокам внесения и передачи в процессе репликации сведений в указанные информационные системы»;

– приказом Министерства образования, науки и молодежи Республики Крым от 25.11.2024 № 1797 «О внесении сведений в Региональную информационную систему обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;

– аттестатом соответствия Государственной информационной системы «Планирование ГИА» (далее – РИС ГИА) № 2854.0106.2024 от 16 сентября 2024 года.

1.2. Положение разработано с целью соблюдения информационной безопасности, конфиденциальности при организации подготовки и проведения мероприятий государственной итоговой аттестации обучающихся по образовательным программам основного общего и среднего общего образования (далее – ГИА) в 2026 году.

1.3. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА в 2026 году между:

– Государственным казенным учреждением Республики Крым «Центр оценки и мониторинга качества образования» (Типакова Е.О.), выполняющему функции Регионального центра обработки информации (далее – РЦОИ);

– органами управления образованием муниципальных районов, муниципальных и городских округов Республики Крым (далее – МОУО); пунктами проведения экзаменов, общеобразовательными организациями, (далее – ППЭ, ОО);

– государственными общеобразовательными организациями (далее ГОО), подведомственными Министерству образования, науки и молодежи Республики Крым.

2. Средства защиты информации

2.1. Средства защиты информации (далее – СЗИ) подразделяются на:

2.1.1. Технические (компьютерное оборудование, серверное оборудование, сканерное оборудование, принтеры, флеш-накопители, защищенные внешние флеш-накопители с записанным ключом шифрования, USB-модемы, внешние CD-ROM, аудиооборудование);

2.1.2. Программно-аппаратные комплексы (далее – ПАК);

2.1.3. Программное обеспечение (далее – ПО) для:

– формирования РИС ГИА;

– технологии передачи экзаменационных материалов (далее – ЭМ) ЕГЭ по сети «Интернет»;

– технологии печати полного комплекта ЭМ в аудитории ППЭ;

– технологии проведения устной части экзамена по иностранным языкам (раздел «Говорение»);

– технологии проведения ЕГЭ по учебному предмету «Информатика» в компьютерной форме (далее – КЕГЭ);

– технологии сканирования ЭМ в аудитории ППЭ;

– технологии сканирования в штабе ППЭ;

– технологии передачи экзаменационных материалов из РЦОИ, получения, расшифровки, печати, сканирования и отправки ЭМ на обработку в РЦОИ.

3. Направления обеспечения информационной безопасности, содержащие перечень материалов и условия их хранения

3.1. РЦОИ обеспечивает информационную безопасность, конфиденциальность информации на региональном уровне на всех этапах проведения ГИА, в том числе при:

– формировании сведений в РИС ГИА, обработке персональных данных в РИС ГИА;

– обмене информацией, содержащей персональные данные, по защищенным каналам связи между РЦОИ и Федеральным государственным бюджетным учреждением «Федеральный центр тестирования» (далее – ФЦТ), РЦОИ и МОУО, РЦОИ и ППЭ ЕГЭ;

– получении, учете, приеме-передаче ЭМ в РЦОИ;

– сканировании, верификации и экспертизе бланков участников ГИА в РЦОИ;

– сопровождении деятельности предметных комиссий Республики Крым (далее – ПК) при осуществлении проверки экзаменационных работ участников ГИА;

– обработке машиночитаемых форм ППЭ, обрабатываемых в специализированном программном обеспечении;

– обеспечении деятельности апелляционной комиссии Республики Крым (далее – АК).

3.2. Помещения РЦОИ, используемые для осуществления обработки, сканирования, верификации, хранения ЭМ, а также для осуществления деятельности ПК, АК, оборудуются программно-аппаратными комплексами на базе ip-камер (далее – ПАК), работающими в режиме «онлайн» и ведущими круглосуточную видеозапись, что обеспечивает круглосуточное наблюдение в режиме реального времени за процессами, происходящими в указанных помещениях, на порталах smotriege.ru.

3.3. За обеспечение информационной безопасности при подготовке и проведении ГИА в РЦОИ назначается ответственное лицо.

3.4. В МОУО назначается ответственное лицо за обеспечение информационной безопасности, конфиденциальности информации на муниципальном уровне при:

– формировании сведений, вносимых в РИС ГИА (муниципальный уровень);

– обработке персональных данных в РИС ГИА;

– обмене информацией, содержащей персональные данные, по защищенным каналам связи между МОУО и РЦОИ и с соблюдением требований информационной безопасности между МОУО и ППЭ, МОУО и ГОО, МОУО и ОО;

– получении ЭМ ГИА для ППЭ по защищенным каналам связи от РЦОИ;

– отправке ЭМ ГИА в ППЭ с соблюдением требований информационной безопасности;

– отправке пакетов с электронными образами бланков и форм ППЭ из ППЭ по защищенным каналам связи в РЦОИ;

– получении доступа (пароля) к ЭМ ГИА от РЦОИ;

– получении, доставке и передаче ключа шифрования, записанного на защищенный внешний носитель (далее – токен) членов государственной экзаменационной комиссии (далее – ГЭК).

3.5. ППЭ (ОО) обеспечивают информационную безопасность, конфиденциальность информации на всех этапах проведения ГИА, в том числе при:

– получении ЭМ ГИА с соблюдением требований информационной безопасности;

– получении ЭМ в форме ЕГЭ по сети «Интернет»;

– печати полного комплекта ЭМ в форме ЕГЭ в аудиториях ППЭ;

– печати полного комплекта ЭМ в форме ОГЭ, ГВЭ-9, ГВЭ-11 в штабе ППЭ;

– получении членами ГЭК доступа (пароля) к ЭМ ГИА;

– переводе бланков ответов участников ГИА в электронный вид в аудитории ППЭ;

– отправке пакетов с электронными образами бланков и форм ППЭ в формах ОГЭ и ГВЭ-9, в форме ГВЭ-11 с соблюдением требований информационной безопасности в штабе ППЭ в РЦОИ;

– отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ в форме ЕГЭ в РЦОИ через личный кабинет ППЭ;

– получении и хранении токенов членов ГЭК;

– хранении использованных/неиспользованных бланков и форм ППЭ, использованных контрольных измерительных материалов и контрольных листов, испорченных/бракованных индивидуальных комплектов и использованных/неиспользованных электронных носителей, использованных черновиков в местах, определенных распорядительным актом Министерства, до 1 марта года, следующего за годом проведения экзамена.

3.6. Государственные общеобразовательные организации обеспечивают информационную безопасность, конфиденциальность информации на всех этапах проведения ГИА, в том числе при:

– формировании сведений, вносимых в РИС ГИА;

– обработке персональных данных в РИС ГИА;

– обмене информацией, содержащей персональные данные между ГОО и МОУО;

– получении ЭМ ГИА с соблюдением требований информационной безопасности;

– печати полного комплекта ЭМ форме ЕГЭ в аудиториях ППЭ;

– печати полного комплекта ЭМ в форме ОГЭ, ГВЭ-9, ГВЭ-11 в штабе ППЭ;

– переводе бланков ответов участников ГИА в электронный вид в аудитории ППЭ или штабе ППЭ;

– получении доступа (пароля) к ЭМ ГИА;

– отправке пакетов с электронными образами бланков и форм ППЭ в формах ОГЭ, ГВЭ-9, ГВЭ-11 в РЦОИ через защищенный канал связи ViPNet «Деловая почта»;

– отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ в форме ЕГЭ в РЦОИ через личный кабинет ППЭ;

– получении и хранении токенов членов ГЭК;

– хранении использованных/неиспользованных бланков и форм ППЭ, контрольно-измерительных материалов и контрольных листов, испорченных/бракованных индивидуальных комплектов использованных/ неиспользованных электронных носителей, использованных черновиков в местах, определенных распорядительным актом Министерства, до 1 марта года, следующего за годом проведения экзамена.

4. Методы и способы защиты информации

4.1.Методами и способами защиты информации в РЦОИ, МОУО, ППЭ, ОО, ГОО от несанкционированного доступа являются:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также в помещения, где хранятся носители информации;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– учет и хранение съемных носителей информации и их обращение и использование, исключающее хищение, подмену и уничтожение;

– использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

– организация физической защиты помещений и технических средств, позволяющих осуществлять обработку персональных данных; осуществление антивирусной защиты АРМ, используемых при обработке персональных данных;

– до момента начала обработки защищаемой информации на АРМ обновление антивирусных баз сигнатур антивирусов, установленных на рабочих местах.

4.2. Для соблюдения информационной безопасности в РЦОИ, МОУО, ОО, ГОО разрабатывается и утверждается распорядительными актами (приказами) комплекс мероприятий, в том числе назначаются лица, ответственные за обеспечение информационной безопасности. Позиции, изложенные в организационно-распорядительных документах, должны соответствовать единой технологии обработки информации.

5. Комплекс мероприятий по обеспечению информационной безопасности в РЦОИ

В целях осуществления информационной безопасности РЦОИ обеспечивает реализацию комплекса мероприятий.

3.1. В период подготовки к ГИА осуществляет разработку, издание распорядительных актов (приказов) и контроль за их исполнением, по вопросам:

– назначения лица, ответственного за обеспечение защиты информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на региональном уровне;

– назначения администратора безопасности, в том числе по осуществлению технического обеспечения функционирования СЗИ и организационных действий в соответствии с организационно-распорядительными документами;

– назначения ответственных лиц за внесение сведений на региональном уровне для передачи в процессе репликации в Федеральную информационную систему обеспечения проведения ГИА и приема граждан в образовательные организации для получения среднего профессионального и высшего образования в региональные информационные системы обеспечения проведения ГИА (далее – ФИС ГИА) и в РИС ГИА в соответствии со срокам внесения и передачи в процессе репликации сведений в указанные информационные системы;

– периодического обновления общесистемного и прикладного программного обеспечения, а также СЗИ;

– утверждения списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

– утверждения списка допущенных пользователей РИС ГИА;

– утверждения для каждого пользователя списков доступных информационных ресурсов (матрица доступа);

– утверждения списка сотрудников, допущенных в помещения, где установлены технические средства информационной системы и системы защиты;

– установления границы контролируемой зоны информационной системы.

3.2. Перед началом проведения ГИА, с целью обеспечения информационной безопасности, бесперебойной работы оборудования в РЦОИ осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также СЗИ, в том числе:

– проверка автоматизированного рабочего места АРМ и сервера сертифицированных технических средств защиты от несанкционированного доступа (с целью доступа пользователей только через идентификаторы и пароли), формирование и ведение журнала учета СЗИ;

– проверка технических средств защиты от несанкционированного доступа в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;

– проведение постоянной работы с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями организационно-распорядительных документов по защите информации, в том числе обязательная смена паролей в соответствии с инструкцией о парольной защите (не реже одного раза в 90 дней) (на доступ к информационным системам РИС ГИА два раза в год – перед началом сбора баз данных и перед началом проведения ГИА);

– формирование и ведение журнала учета смены паролей;

– повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, тренинги, регламентация прав и ответственности);

– установка и настройка межсетевого экрана (экранов);

– обеспечение безопасного хранения ключевой информации ПО ViPNet (файл с расширением .dst), применяемой для связи с ФЦТ;

– блокировка доступа к информационно-телекоммуникационной сети «Интернет» на АРМ пользователей, имеющих доступ к РИС ГИА;

– установка и настройка на АРМ пользователей и сервера/серверов сертифицированного антивирусного программного обеспечения; удаление или блокировка на АРМ (сервере/серверах, в случае наличия) средств беспроводного доступа;

– эксплуатация средств антивирусной защиты в соответствии с требованиями организационно-распорядительных документов по защите

информации, в том числе регулярное обновление базы средств антивирусной защиты;

– регулярное обновление программного обеспечения, а также средств защиты информации в соответствии с разработанным регламентом;

– отключение автоматического обновления операционной системы Microsoft Windows на всех АРМ, задействованных при обработке ЭМ, в том числе на рабочих ПК;

– проведение работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно требованиям организационно-распорядительных документов по защите информации;

– исключение нахождения в помещениях, где идет обработка информации, в том числе персональных данных, и в границах контролируемой зоны посторонних лиц;

– проведение мероприятий по обследованию, защите и аттестации в соответствии с требованиями безопасности информации РИС ГИА;

– организация и обеспечение выдачи членам ГЭК токена, необходимого для применения технологий печати полного комплекта ЭМ ЕГЭ в аудиториях ППЭ, сканирования ЭМ в аудитории ППЭ, проведения устной части экзамена по учебному предмету «иностранный язык» (раздел «Говорение») и КЕГЭ;

– обеспечение соблюдения информационной безопасности при формировании, шифровании и отправке по защищенным каналам связи ЭМ ГИА в формах ОГЭ, ГВЭ-9, ГВЭ-11.

3.3. В РЦОИ реализуется комплекс мер для сохранения свойств информации защиты её конфиденциальности, сохранения целостности, обеспечения доступности, а также противодействия нарушителям информационной безопасности в соответствии с согласованной «Моделью угроз» от 03.09.2024 (письмо Управления Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 03.09.2024 №2/838).

6. Комплекс мероприятий по обеспечению информационной безопасности в МОУО

В целях осуществления мероприятий по информационной безопасности на территории муниципального образования МОУО обеспечивает реализацию комплекса мер, в том числе для сохранения свойств информации, защиты её конфиденциальности, сохранения целостности, обеспечения доступности, а также противодействия нарушителям информационной безопасности.

6.1. В период подготовки к ГИА осуществляется разработка, издание правовых актов (приказов, другое) и контроль за их исполнением по вопросам:

назначения ответственного за обеспечение защиты информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на муниципальном уровне;

назначения администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационных действий в соответствии с организационно-распорядительными документами;

назначения лиц, имеющих доступ к сегменту РИС ГИА, на муниципальном уровне;

регулярного обновления общесистемного программного обеспечения, а также СЗИ;

отключения автоматического обновления операционной системы Microsoft Windows на всех АРМ, задействованных при проведении ГИА;

утверждения списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

утверждения списка сотрудников, допущенных в помещения, где установлены технические средства информационной системы и системы защиты, а также границы контролируемой зоны указанных помещений.

6.2. Для обеспечения информационной безопасности на территории муниципального образования МОУО осуществляются мероприятия по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного программного обеспечения, а также СЗИ, в том числе:

– установка на АРМ и сервер сертифицированных технических средств защиты от несанкционированного доступа (только через идентификаторы и пароли), формирование и ведение журнала учета СЗИ;

– настройка технических средств защиты от несанкционированного доступа в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;

– проведение постоянных работ с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями организационно-распорядительных документов по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на муниципальном уровне два раза в год: перед началом сбора баз данных и перед началом ГИА, ЕГЭ;

– формирование и ведение журнала учета смены паролей;

– повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, тренинги, регламентация прав и ответственности);

– установка и настройка на АРМ пользователей и сервер/серверы сертифицированного антивирусного программного обеспечения;

– эксплуатация средств антивирусной защиты в соответствии с требованиями организационно-распорядительных документов по защите информации;

– присвоение машинным носителям информации идентификационных номеров, в том числе ведение журнала учета машинных носителей информации;

– осуществление работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно

требованиям организационно-распорядительных документов по защите информации;

– исключение нахождения в помещениях, где идет обработка информации, в том числе персональных данных и в границах контролируемой зоны, посторонних лиц;

– обследование, защита и аттестация в соответствии с требованиями безопасности информации на АРМ РИС ГИА на муниципальном уровне;

– организация и обеспечение получения членам ГЭК токена члена ГЭК, необходимого для применения технологий печати полного комплекта ЭМ ЕГЭ в аудиториях ППЭ, сканирования ЭМ в аудиториях ППЭ, проведения устной части экзамена по учебному предмету «иностранный язык» (раздел «Говорение») и КЕГЭ;

– обеспечение соблюдения информационной безопасности при получении и отправке по защищенным каналам связи ЭМ ГИА.

7. Комплекс мероприятий по обеспечению информационной безопасности в государственных общеобразовательных организациях

В целях осуществления информационной безопасности, ГОО обеспечивают реализацию комплекса мероприятий, в том числе комплекс мер для сохранения свойств информации защиты её конфиденциальности, сохранения целостности, обеспечения доступности, а также противодействия нарушителям информационной безопасности.

7.1. В период подготовки к ГИА в ГОО осуществляется комплекс мероприятий по разработке, изданию и контролю исполнения локальных распорядительных актов по следующим вопросам:

– назначения ответственного за обеспечение защиты информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на уровне образовательной организации в период внесения сведений об участниках ГИА;

– назначения администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационные действия в соответствии с организационно-распорядительными документами;

– назначения лиц, имеющих доступ к сегменту РИС ГИА на уровне образовательной организации;

– регулярного обновления общесистемного программного обеспечения, а также средств защиты информации;

– отключения автоматического обновления операционной системы Microsoft Windows на всех АРМ, задействованных при проведении ГИА;

– утверждения списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

– утверждения списка сотрудников, допущенных в помещения, где установлены технические средства информационной системы и системы защиты с указанием границы контролируемой зоны.

7.2. Для обеспечения информационной безопасности в ГОО обеспечивается реализация мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного программного обеспечения, а также СЗИ, в том числе:

– установка на АРМ сертифицированных технических средств защиты от несанкционированного доступа (доступ пользователей только через идентификаторы и пароли);

– настройка технических средств защиты от несанкционированного доступа в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;

– проведение постоянных работ с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями организационно-распорядительных документов по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на уровне образовательной организации два раза в год: перед началом сбора баз данных и перед началом ГИА;

– формирование и ведение журнала учета смены паролей;

– повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, тренинги, регламентация прав и ответственности);

– установка и настройка на АРМ пользователей сертифицированного антивирусного программного обеспечения;

– эксплуатация средств антивирусной защиты в соответствии с требованиями организационно-распорядительных документов по защите информации;

– присвоение машинным носителям информации идентификационных номеров (журнал учета машинных носителей информации);

– осуществление работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно требованиям организационно-распорядительных документов по защите информации;

– исключение нахождения в помещениях, где идет обработка информации, в том числе персональных данных и в границах контролируемой зоны, посторонних лиц;

– проведение обследования, защиты и аттестации в соответствии с требованиями безопасности информации на АРМ РИС ГИА (уровень образовательной организации);

– обеспечение рабочих мест технических специалистов, организаторов в аудитории, руководителей ППЭ, членов ГЭК оборудованием и ПО, необходимым для организации технологий получения ЭМ, печати полного комплекта ЭМ в аудиториях ППЭ, сканирования ЭМ в аудиториях ППЭ, проведения устной части экзамена по учебному предмету «иностранный язык» (раздел «Говорение») и КЕГЭ в соответствии с требованиями к оборудованию и программному обеспечению;

– обеспечение штаба ППЭ необходимым оборудованием и ПО для проведения ГИА в соответствии с технологией проведения ГИА;

– обеспечение соблюдения информационной безопасности при получении и отправке ЭМ в форме ГВЭ-9, ОГЭ, ГВЭ-11;

– обеспечение специально выделенных и оборудованных помещений (кабинетов), в том числе металлическими шкафами, сейфами, металлическими стеллажами, позволяющими обеспечить сохранность ЭМ и документов, используемых для проведения ГИА, с соблюдением информационной безопасности в условиях, исключающих доступ к ним посторонних лиц, с учетом требований противопожарной безопасности.

8. Комплекс мероприятий по обеспечению информационной безопасности в ППЭ (ОО)

В целях осуществления информационной безопасности в ППЭ (ОО) обеспечивается реализация комплекса мероприятий, в том числе комплекса мер для сохранения свойств информации, защиты её конфиденциальности, сохранения целостности, обеспечения доступности, а также противодействия нарушителям информационной безопасности.

8.1. В период подготовки к ГИА ОО осуществляется разработка, издание распорядительных актов (приказов, другое) и контроль за их исполнением по вопросам:

– назначения лица, ответственного за обеспечение защиты информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на уровне ОО в период внесения сведений об участниках ГИА;

– назначения администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационных действий в соответствии с организационно-распорядительными документами;

– назначения лиц, имеющих доступ к сегменту РИС ГИА на уровне ОО;

– регулярного обновления общесистемного и прикладного программного обеспечения, а также средств защиты информации;

– отключения автоматического обновления операционной системы Microsoft Windows на всех АРМ, задействованных при проведении ГИА;

– утверждения списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

– утверждения списка сотрудников, допущенных в помещения, где установлены технические средства информационной системы и системы защиты с указанием границы контролируемой зоны;

8.2. Для обеспечения информационной безопасности в ППЭ (ОО) обеспечивается реализация мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также СЗИ, в том числе:

– установка на АРМ и сервер сертифицированных технических средств защиты от несанкционированного доступа (доступ пользователей только через идентификаторы и пароли), ведение журнала учета СЗИ;

– настройка технических средств защиты от несанкционированного доступа в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;

– проведение постоянных работ с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями организационно-распорядительных документов по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на уровне образовательной организации два раза в год: перед началом сбора баз данных и перед началом ГИА;

– формирование и ведение журнала учета смены паролей;

– повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, тренинги, регламентация прав и ответственности);

– блокировка доступа к информационно-телекоммуникационной сети «Интернет» на АРМ пользователей, задействованных в проведении ГИА, кроме АРМ «Личный кабинет ППЭ» для проведения ЕГЭ;

– эксплуатация средств антивирусной защиты в соответствии с требованиями организационно-распорядительных документов по защите информации;

– присвоение машинным носителям информации идентификационных номеров (журнал учета машинных носителей информации);

– осуществление работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно требованиям организационно-распорядительных документов по защите информации;

– исключение нахождения в помещениях, где идет обработка информации, в том числе персональных данных и в границах контролируемой зоны, посторонних лиц;

– проведение обследования, защиты и аттестации в соответствии с требованиями безопасности информации на АРМ РИС ГИА (уровень образовательной организации);

– обеспечение рабочих мест технических специалистов, организаторов в аудитории, руководителей ППЭ, членов ГЭК оборудованием и ПО, необходимым для организации экзаменов с использованием технологий получения ЭМ по информационно-телекоммуникационной сети «Интернет», печати полного комплекта ЭМ в аудиториях ППЭ, сканирования ЭМ в аудиториях ППЭ, проведения устной части экзамена по учебному предмету «иностранный язык» (раздел «Говорение») и КЭГЭ в соответствии с требованиями к оборудованию и программному обеспечению;

– обеспечение штаба ППЭ необходимым оборудованием и ПО для проведения ГИА, в соответствии с технологиями проведения;

– обеспечение соблюдения информационной безопасности при получении и отправке ЭМ в форме ГВЭ, ОГЭ;

– обеспечение специально выделенных и оборудованных помещений (кабинетов), в том числе металлическими шкафами, сейфами, металлическими стеллажами, позволяющими обеспечить сохранность ЭМ и документов, используемых для проведения ГИА, с соблюдением информационной безопасности, в условиях, исключающих доступ к ним посторонних лиц, с учетом требований противопожарной безопасности.

9. Ответственность лиц за обеспечение информационной безопасности

9.1. Информационная безопасность при проведении ГИА, ЕГЭ обеспечивается на всех этапах организации и проведения ГИА.

9.2. К информации конфиденциального характера относятся:

– сведения, содержащие персональные данные участников ГИА, выпускников прошлых лет, находящиеся на бумажных носителях (заявления, копии (скан копии) личных документов: паспорт, СНИЛС, документ об образовании, другое), электронных файлах РИС ГИА;

– персональные данные участников ГИА, содержащиеся на бумажных носителях (оригиналы и копии бланков регистрации, бланков ответов № 1, бланков ответов № 2, в том числе дополнительный бланк ответов № 2);

– контрольные измерительные материалы ГИА по всем учебным предметам ЕГЭ, ОГЭ, ГВЭ;

– тексты, задания на электронных и бумажных носителях;

– формы ППЭ на бумажных и электронных носителях;

– критерии оценивания для оценивания экзаменационных работ участников ГИА по учебным предметам ГИА;

– протоколы проверок экспертов РПК;

– сведения, содержащиеся в РИС ГИА, об организаторах и руководителях ППЭ ГИА, членах ГЭК, экспертах ПК, общественных наблюдателях;

– аутентификационные данные, выданные операторам станции экспертизы, операторам станции сканирования, операторам станции верификации.

9.3.Специалисты, привлекаемые к работе, связанной со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ППЭ (ОО), ГОО, обязаны:

– знать и выполнять требования настоящего Положения;

– знать перечень сведений конфиденциального характера;

– не разглашать ставшие известными им сведения конфиденциального характера, информировать непосредственных руководителей (лиц их замещающих) о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших им известными попытках несанкционированного доступа к информации; соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц;

– знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения служебных обязанностей;

– не допускать утечки информации конфиденциального характера на всех этапах работы с данной информацией;

– работать с документами и информацией конфиденциального характера в помещениях, определенных для работы с данной информацией;

– представлять письменные объяснения о допущенных нарушениях установленного порядка работы, учета и хранения документов, а также о фактах разглашения конфиденциальных сведений.

9.4. Специалистам, привлекаемым к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ППЭ (ОО), ГОО, запрещается:

– использовать конфиденциальные сведения при ведении телефонных переговоров;

– передавать документы, содержащие сведения конфиденциального характера по открытой информационно-телекоммуникационной сети «Интернет»;

– использовать конфиденциальные сведения в личных интересах;

– снимать копии с документов и других носителей информации, содержащих конфиденциальные сведения, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру и др.) для записи конфиденциальных сведений;

– выполнять на дому работы, связанные с информацией конфиденциального характера;

– работать с документами и информацией конфиденциального характера в помещениях, не определенных для работы с данного вида информацией.

9.5. В случае выявления факта разглашения конфиденциальных сведений специалисты, привлекаемые к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ППЭ (ОО), ГОО, обязаны незамедлительно поставить в известность руководителя РЦОИ, МОУО, ППЭ (ОО), ГОО о сложившейся ситуации, для обеспечения проведения служебной проверке по данному факту.

9.6. Комиссия, в полномочия которой входит проведение указанного служебного расследования, устанавливает:

– обстоятельства разглашения конфиденциальных сведений;

– лиц, виновных в разглашении конфиденциальных сведений;

– причины и условия, способствовавшие разглашению конфиденциальных сведений.

9.7. Служебное расследование проводится в минимально короткий срок со дня выявления факта разглашения конфиденциальных сведений.

Одновременно с работой комиссии принимаются меры по локализации нежелательных последствий разглашения конфиденциальных сведений.

9.8. К лицам, нарушающим правила и порядок информационной безопасности, принимаются меры в соответствии с действующим законодательством Российской Федерации.