Автономное учреждение
дополнительного профессионального образования
Ханты-Мансийского автономного округа - Югры
«Институт развития образования»

ПРИКАЗ

Об обеспечении информационной безопасности при проведении мероприятий по подготовке и организации проведения государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена на территории Ханты-Мансийского автономного округа – Югры в 2023/2024 учебном году, дополнительном (сентябрьском) периоде 2024 года

29.12.2023 10/42-П-74
г. Ханты-Мансийск

В соответствии с федеральными законами от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлениями 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», приказами Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки от 04 апреля 2023 года № 232/551 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования», № 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 июня 2021 года № 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 Департамента образования и науки Ханты-Мансийского автономного округа – Югры от 23 октября 2023 года № 10-П-2637 «Об утверждении плана мероприятий (дорожной карты) по подготовке к проведению государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования, иных процедур оценки качества образования в Ханты-Мансийском автономном округе – Югре в 2023-2024 учебном году, дополнительном периоде 2024 года», от 23 октября 2023 года № 10-П-2642 «О возложении некоторых функций на автономное учреждение дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования», в целях обеспечения соблюдения информационной безопасности при проведении мероприятий по подготовке и организации проведения государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2023-2024 учебном году, дополнительном периоде 2024 года

ПРИКАЗЫВАЮ:

1. Утвердить положение об обеспечении информационной безопасности при проведении мероприятий по подготовке и организации проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования, единого государственного экзамена (далее ГИА, ЕГЭ) в Ханты-Мансийском автономном округе – Югре в 2023-2024 учебном году, дополнительном периоде 2024 года (далее – Положение).

2. Назначить Ефременко О.В., начальника отдела организационно-

технического, технологического сопровождения оценочных процедур и информационной безопасности (далее – ОТТСОП и ИБ) ответственным лицом за:

2.1. Соблюдение информационной безопасности в РЦОИ при проведении мероприятий по подготовке и организации проведения ГИА, ЕГЭ согласно Положению, утверждённому пунктом 1 настоящего приказа.

2.2. Реализацию организационно-технических, технологических мероприятий по обеспечению информационной безопасности в РЦОИ.

2.3. Консультационно-методическое сопровождение организационно-технических, технологических мероприятий по обеспечению информационной безопасности в органах местного самоуправления, осуществляющих управление в сфере образования, Ханты-Мансийского автономного округа – Югры, пунктах проведения экзаменов.

2.4. Обеспечение особого пропускного режима в РЦОИ в период организации и проведения ГИА, ЕГЭ.

3. Назначить Торощина Д.А., инженера по автоматизированным системам управления производством отдела ОТТСОП и ИБ ответственным лицом за проведение инструктажа лиц, привлекаемых к организации проведения ГИА, ЕГЭ, по соблюдению требований информационной безопасности.

4. Назначить Магрычева А.А., инженера отдела ОТТСОП и ИБ ответственным лицом за соблюдение условий конфиденциальности и требований информационной безопасности при работе с экзаменационными материалами.

5. Рекомендовать руководителям органов местного самоуправления, осуществляющих управление в сфере образования Ханты-Мансийского автономного округа – Югры:

5.1. Принять меры по обеспечению информационной безопасности при проведении мероприятий по подготовке и организации проведения ГИА, ЕГЭ согласно Положению, утверждённому пунктом 1 настоящего приказа, в том числе:

5.1.1. При получении, учете, хранении, доставке и приемке-передаче экзаменационных материалов;

5.1.2. Оснащение абонентских пунктов муниципального сегмента региональной информационной системы обеспечения проведения ГИА (далее – РИС ГИА) и пунктов проведения экзаменов программным обеспечением и средствами технической защиты информации.

5.2. Организовать проведение инструктажа лиц, привлекаемых к

проведению ГИА, ЕГЭ, по соблюдению требований информационной безопасности.

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

6. Рекомендовать руководителям государственных образовательных организаций, находящихся в ведении Департамента (Сарабаров А.Б., Хидирлясов Г.К., Наумов М.Н., Жуков А.В., Мамбетов Б.Т., Петрова О.В., Свайкина Н.В., Елфимова О.В.):

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

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

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

7. Рекомендовать руководителям государственных образовательных организаций Ханты-Мансийского автономного округа – Югры, находящихся в ведении иных органов исполнительной власти Ханты-Мансийского автономного округа – Югры (А.В. Тарасов, К.А. Васильев, А.А. Кобцева), обеспечить исполнение подпунктов 6.1 – 6.3 настоящего приказа, в части касающейся.

6. Контроль за исполнением настоящего приказа возложить на заместителя директора Котельникову Г.Н.

Директор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00877260D06C85D290324379FA8EEF429C
Владелец Клюсова Виктория Викторовна
Действителен с 07.07.2023 по 29.09.2024

В.В. Клюсова

Приложение к письму
АУ «Институт развития образования»
от « » декабря 2023 г. № 10/42-П-____

Положение об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Ханты-Мансийском автономном округе – Югре в 2024 году (далее – Положение)

1. Общие положения

1.1. Настоящее Положение разработано с целью соблюдения информационной безопасности, конфиденциальности при подготовке и проведении мероприятий государственной итоговой аттестации обучающихся по образовательным программам основного общего и среднего общего образования (далее – ГИА) в 2024 году.

1.2. Настоящее 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 № 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, 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 Рособрнадзора от 4 апреля 2023 года № 232/551 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования»;

приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказом Рособрнадзора от 11 июля 2021 года № 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»;

аттестатом соответствия Государственной информационной системы «Центральный сегмент региональной информационной системы, задействованной в работе по обеспечению ГИА Ханты-Мансийского автономного округа – Югры» (далее – ГИС «ЦС РИС ГИА ХМАО-Югры») автономного учреждения дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» требованиям по безопасности информации № 123/72 от 18 мая 2021 года;

информационным письмом Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 28 января 2021 года № 01.08-Исх-260.

1.3. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА в 2024 году между:

автономным учреждением дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» - организации, уполномоченной осуществлять функции Регионального центра обработки информации (далее – РЦОИ);

органами местного самоуправления муниципальных образований Ханты-Мансийского автономного округа – Югры, осуществляющими управление в сфере образования (далее – МОУО);

пунктами проведения экзаменов, образовательными организациями, расположенными на территории Ханты-Мансийского автономного округа – Югры (далее – ППЭ, ОО).

государственными образовательными организациями, подведомственными Департаменту образования и науки Ханты-Мансийского автономного округа – Югры (далее – Департамент), иным органам исполнительной власти Ханты-Мансийского автономного округа – Югры (далее – государственные образовательные организации).

2. Средства защиты информации

2.1. Средства защиты информации 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, аудио оборудование);

2.1.2. Программно-аппаратные (программно-аппаратные комплексы);

2.1.3. Программное обеспечение (далее – ПО) для:

формирования Региональной информационной системы обеспечения проведения ГИА (далее – РИС ГИА);

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

технологии печати полного комплекта ЭМ в аудитории ППЭ;

технологии печати полного комплекта ЭМ в аудитории и (или) штабе ППЭ;

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

технологии проведения основного государственного экзамена (далее – ОГЭ) по учебному предмету «информатика» в компьютерной форме;

технологии сканирования ЭМ в аудитории ППЭ;

технологии сканирования в штабе ППЭ;

технологии формирования, шифрования, отправки из РЦОИ, получения, расшифровки, печати, сканирования и отправки ЭМ на обработку в РЦОИ в форме государственного выпускного экзамена (далее – ГВЭ).

3. Направления обеспечения информационной безопасности

3.1. РЦОИ обеспечивают 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 выделенным линиям и защищенным каналам связи между РЦОИ и Федеральным государственным бюджетным учреждением «Федеральный центр тестирования» (далее – ФЦТ), РЦОИ и МОУО, РЦОИ и ППЭ (ОО);

получении, учете, приеме-передаче ЭМ в РЦОИ;

сканировании, верификации и экспертизе бланков участников ГИА в РЦОИ;

обеспечении осуществления деятельности региональных предметных комиссий Ханты-Мансийского автономного округа – Югры (далее – РПК) при обработке и проверке экзаменационных работ участников ГИА;

обработке машиночитаемых форм ППЭ, обрабатываемых в специализированном программном обеспечении;

обеспечении деятельности Апелляционной комиссии Ханты-Мансийского автономного округа – Югры (далее – АК), в том числе через технологическое программное решение Апелляционной комиссии (далее – ТПР АК);

хранение на бумажных носителях апелляционных комплектов участников ГИА.

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

3.3. За обеспечение информационной безопасности при подготовке и проведении ГИА, ЕГЭ 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, ППЭ (ОО) и РЦОИ, МОУО и ППЭ (ОО);

получении ЭМ по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ по защищенным каналам связи от РЦОИ;

отправке ЭМ по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ по защищенным каналам связи в ППЭ;

отправке пакетов с электронными образами бланков и форм ППЭ по образовательным программам основного общего образования в форме ГВЭ, среднего общего образования в форме ГВЭ по защищенным каналам связи в РЦОИ;

получении доступа (пароля) к ЭМ по образовательным программам основного общего образования в форме ГВЭ, среднего общего образования в форме ГВЭ 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 по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ по защищенным каналам связи;

получении ЭМ по образовательным программам среднего общего образования в форме ЕГЭ по сети «Интернет»;

печати полного комплекта ЭМ по образовательным программам среднего общего образования в форме ЕГЭ в аудиториях ППЭ;

печати полного комплекта ЭМ по образовательным программам основного общего образования в форме ОГЭ, ГВЭ в аудитории и (или) штабе ППЭ;

печати полного комплекта ЭМ по образовательным программам среднего общего образования в форме ГВЭ;

получении доступа членами ГЭК (пароля) к ЭМ в форме ГВЭ;

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

отправке пакетов с электронными образами бланков и форм ППЭ по образовательным программам основного общего образования и среднего общего образования в форме ГВЭ по защищенным каналам связи в штабе ППЭ, в РЦОИ;

отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ по образовательным программам основного общего образования в форме ОГЭ в РЦОИ с помощью станции авторизации ППЭ;

отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ по образовательным программам среднего общего образования в форме ЕГЭ в РЦОИ через личный кабинет ППЭ;

получении и хранении токенов членов ГЭК;

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

3.6. Государственные образовательные 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, по защищенным каналам связи между ОО и РЦОИ;

получении ЭМ по образовательным программам среднего общего образования в форме ЕГЭ по сети «Интернет»;

получении ЭМ по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ по защищенным каналам связи;

печати полного комплекта ЭМ по образовательным программам среднего общего образования в форме ЕГЭ в аудиториях ППЭ;

печати полного комплекта ЭМ по образовательным программам основного общего образования в форме ОГЭ, ГВЭ в аудитории и (или) штабе ППЭ;

печати полного комплекта ЭМ по образовательным программам среднего общего образования в форме ГВЭ;

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

получении доступа (пароля) к ЭМ в форме ГВЭ по защищенным каналам связи;

отправке пакетов с электронными образами бланков и форм ППЭ по образовательным программам основного общего и среднего общего образования в форме ГВЭ по защищенным каналам связи в штабе ППЭ, в РЦОИ;

отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ по образовательным программам основного общего образования в форме ОГЭ в РЦОИ с помощью станции авторизации ППЭ;

отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ по образовательным программам среднего общего образования 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 и использованных/неиспользованных электронных носителей, использованных черновиков в местах, определенных распорядительным актом Департамента, 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, государственных ОО) 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, исключающее хищение, подмену и уничтожение;

резервирование технических средств, дублирование массивов и носителей информации;

использование средств защиты информации, 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 собственно технических средств, позволяющих осуществлять обработку персональных данных;

осуществление антивирусной защиты АРМ используемых при обработке персональных данных

4.2. Для соблюдения информационной безопасности в РЦОИ, МОУО, ОО, государственных ОО разрабатывается и утверждается правовыми актами комплекс мероприятий, в том числе назначаются лица, ответственные за обеспечение информационной безопасности.

5. Комплекс мероприятий по обеспечению информационной безопасности в РЦОИ

В целях осуществления информационной безопасности РЦОИ обеспечивает реализацию комплекса мероприятий.

5.1. В период подготовки к ГИА РЦОИ осуществляется комплекс мероприятий по разработке и изданию и контролю исполнения правовых актов по следующим вопросам:

- о назначении 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;

- о назначении администратора безопасности, в том числе по осуществлению технического обеспечения функционирования средств защиты информации (далее – СЗИ) и организационных действий в соответствии с организационно-распорядительными документами;

- о назначении 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 сроками внесения и передачи в процессе репликации сведений в указанные информационные системы;

- о периодическом обновлении общесистемного и прикладного программного обеспечения, а также средств защиты информации;

- об утверждении списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

- об утверждении списка допущенных пользователей РИС ГИА;

- об утверждении для каждого пользователя списков доступных информационных ресурсов (матрица доступа);

- об утверждении списка сотрудников, допущенных в помещения, где установлены технические средства информационной системы и системы защиты.

- об установлении границы контролируемой зоны информационной системы.

5.2. Для информационного взаимодействия между поставщиками информации заключается соглашение об информационном взаимодействии между РЦОИ и МОУО, ОО, по обмену информацией в «Центральном сегменте РИС ГИА ХМАО-Югры» в соответствии с техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югра от 28 января 2021 года № 01.08-Исх-260).

5.3. Перед началом 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 средств защиты информации, в том числе:

установка автоматизированного рабочего места (далее – 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;

настройка 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);

формирование и ведение журнала учета смены паролей;

повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, дополнительное обучение, 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 общесистемного и прикладного программного обеспечения, а также средств защиты информации в соответствии с разработанным регламентом;

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

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

установка мониторов АРМ с учетом ограничения доступа к видеоинформации иных лиц, за исключением оператора АРМ;

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 экзамена по учебному предмету «информатика и информационно-коммуникационные технологии» в компьютерной форме;

обеспечение соблюдения информационной безопасности при формировании, шифровании и отправке ЭМ по защищенным каналам связи по программам основного общего и среднего общего образования в форме ГВЭ;

обеспечение соблюдения информационной безопасности при получении ЭМ из ФЦТ и отправке ЭМ в ППЭ по защищенным каналам связи по программам основного общего образования в форме ОГЭ.

6. Комплекс мероприятий по обеспечению информационной безопасности в МОУО

В целях осуществления информационной безопасности на территории муниципального образования, МОУО обеспечивает реализацию комплекса мероприятий.

6.1. В период подготовки к ГИА МОУО осуществляется комплекс мероприятий по разработке и изданию и контролю исполнения правовых актов по следующим вопросам:

о назначении ответственного за защиту информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на муниципальном уровне;

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

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

регулярное обновление общесистемного и прикладного программного обеспечения, а также средств защиты информации;

об утверждении списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

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

6.2. Заключение соглашений об информационном взаимодействии между РЦОИ и МОУО поставщиками сведений в «Центральный сегмент РИС ГИА ХМАО-Югры», в соответствии с техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югра от 28 января 2021 года № 01.08-Исх-260).

6.3. Для обеспечения информационной безопасности в МОУО осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также средств защиты информации, 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;

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, имеющих доступ к РИС ГИА на муниципальном уровне;

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

удаление или блокировка на АРМ (и сервере/серверах если есть) средств беспроводного доступа;

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

присвоение машинным носителям информации идентификационных номеров, в том числе ведение 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;

установка мониторов АРМ с учетом ограничения доступа к видеоинформации любых лиц, кроме оператора АРМ;

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 выдачи членам ГЭК токена, 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 экзамена по учебному предмету «информатика и информационно-коммуникационные технологии» в компьютерной форме;

обеспечение соблюдения информационной безопасности при получении и отправке ЭМ по защищенным каналам связи по программам основного общего и среднего общего образования в форме ГВЭ, ОГЭ.

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

В целях осуществления информационной безопасности, государственные ОО обеспечивает реализацию комплекса мероприятий.

7.1. В период подготовки к ГИА государственными ОО осуществляется комплекс мероприятий по разработке и изданию и контролю исполнения правовых актов по следующим вопросам:

о назначении ответственного за защиту 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;

о назначении администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационные действия в соответствии организационно-распорядительных документов;

о назначении лиц, имеющих доступ к сегменту РИС ГИА на уровне образовательной организации;

о регулярном обновлении общесистемного и прикладного программного обеспечения, а также средств защиты информации;

об утверждении списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

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

7.2. Заключение соглашений об информационном взаимодействии между РЦОИ и государственными образовательными организациями - поставщиками сведений в «Центральный сегмент РИС ГИА ХМАО-Югры», в соответствии с техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югра от 28 января 2021 года № 01.08-Исх-260).

7.3. Для обеспечения информационной безопасности в государственных образовательных организациях осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновления общесистемного и прикладного программного обеспечения, а также средств защиты информации, 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, имеющих доступ к РИС ГИА на уровне образовательной организации;

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

удаление или блокировка на АРМ (и сервере/серверах если есть) средств беспроводного доступа;

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;

установка мониторов АРМ с учетом ограничения доступа к видеоинформации иных лиц, за исключением оператора АРМ;

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 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 экзамена по учебному предмету «информатика и информационно-коммуникационные технологии» в компьютерной форме в соответствии с требованиями к оборудованию и программному обеспечению по программам среднего общего образования в форме ЕГЭ;

обеспечение рабочих мест технических специалистов, организаторов в аудитории, руководителей ППЭ, членов ГЭК оборудованием и ПО, необходимым для организации печати полного комплекта ЭМ в аудиториях и (или) штабе ППЭ, сканирования ЭМ в штабе ППЭ, проведения устной части экзамена по учебному предмету «иностранный язык» (раздел «Говорение») и экзамена по учебному предмету «информатика и информационно-коммуникационные технологии» в компьютерной форме в соответствии с требованиями к оборудованию и программному обеспечению по программам основного общего образования в форме ОГЭ;

обеспечение штаба и аудиторий ППЭ необходимым оборудованием и ПО для проведения ГИА, в соответствии с технологией проведения в Ханты-Мансийском автономном округе – Югре;

обеспечение соблюдения информационной безопасности при получении и отправке ЭМ по защищенным каналам связи по программам основного общего и среднего общего образования в форме ГВЭ;

обеспечение соблюдения информационной безопасности при получении ЭМ по защищенным каналам связи по программам основного общего образования в форме ОГЭ;

обеспечение соблюдения информационной безопасности при отправке ЭМ в РЦОИ через станцию авторизации по программам основного общего образования в форме 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.

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

В целях осуществления информационной безопасности, ОО обеспечивают реализацию комплекса мероприятий.

8.1. В период подготовки к ГИА ОО осуществляется комплекс мероприятий по разработке и изданию и контролю исполнения правовых актов по следующим вопросам:

о назначении ответственного за защиту 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;

о назначении администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационные действия в соответствии организационно-распорядительных документов;

о назначении лиц, имеющих доступ к сегменту РИС ГИА на уровне образовательной организации;

о регулярном обновлении общесистемного и прикладного программного обеспечения, а также средств защиты информации;

об утверждении списка съемных машинных носителей информации и мест хранения съемных машинных носителей информации;

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

8.2 Заключение соглашений об информационном взаимодействии между МОУО и ОО - поставщиками сведений в «Центральный сегмент РИС ГИА ХМАО-Югры», в соответствии с техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югра от 28 января 2021 года № 01.08-Исх-260).

8.3. Для обеспечения информационной безопасности в ОО осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также средств защиты информации, 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, имеющих доступ к РИС ГИА на уровне образовательной организации;

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

удаление или блокировка на АРМ (и сервере/серверах если есть) средств беспроводного доступа;

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;

установка мониторов АРМ с учетом ограничения доступа к видеоинформации иных лиц, за исключением оператора АРМ;

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 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 экзамена по учебному предмету «информатика и информационно-коммуникационные технологии» в компьютерной форме в соответствии с требованиями к оборудованию и программному обеспечению по программам среднего общего образования в форме ЕГЭ;

обеспечение штаба и аудиторий ППЭ необходимым оборудованием и ПО для проведения ГИА, в соответствии с технологией проведения в Ханты-Мансийском автономном округе – Югре;

обеспечение соблюдения информационной безопасности при получении и отправке ЭМ по защищенным каналам связи по программам основного общего и среднего общего образования в форме ГВЭ, ОГЭ;

обеспечение соблюдения информационной безопасности при получении ЭМ по защищенным каналам связи по программам основного общего образования в форме ОГЭ;

обеспечение соблюдения информационной безопасности при отправке ЭМ в РЦОИ через станцию авторизации по программам основного общего образования в форме 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 обеспечивается на всех этапах организации и проведения ГИА.

9.2. К информации конфиденциального характера относятся:

персональные данные участников ГИА, находящиеся на бумажных носителях (заявления, копии паспортных данных), электронных файлах РИС ГИА;

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

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

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

тексты, билеты, задания на электронных и бумажных носителях;

ЭМ ГВЭ за курс основного общего и среднего общего образования;

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 РПК, 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), государственных образовательных организаций обязаны:

знать и выполнять требования настоящего Положения;

знать перечень сведений конфиденциального характера;

не разглашать ставшие известные 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 утечек 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), государственных образовательных организаций запрещается:

использовать конфиденциальные сведения при ведении телефонных переговоров;

передавать документы, содержащие сведения конфиденциального характера по каналам факсимильной связи и в открытую информационно-телекоммуникационную сеть «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;

выносить документы и другие носители информации из здания;

работать с документами и информацией конфиденциального характера в помещениях, не определенных для работы с данного рода 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), государственных образовательных организаций обязаны немедленно поставить в известность руководителя РЦОИ, МОУО, ППЭ (ОО), государственной образовательной организации для служебного расследования по данному факту.

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

обстоятельства разглашения конфиденциальных сведений;

виновных в разглашении конфиденциальных сведений;

причины и условия, способствовавшие разглашению конфиденциальных сведений.

9.7. Служебное расследование проводится в минимально короткий срок со дня обнаружения 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.