ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ

ПРИКАЗ

Об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2022 году

24.01.2022 10-П-55

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 «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» от 31 августа 2013 года № 755, от 29 ноября 2021 года № 2085, приказами Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки от 7 ноября 2018 года № 189/1513 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования», № 190/1512 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования», приказами Федеральной службы по надзору в сфере образования и науки от 18 июня 2018 года № 831 «Об утверждении

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», 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 молодежной политики Ханты-Мансийского автономного округа – Югры от 29 октября 2021 года № 10-П-1485 «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 2021/2022 учебном году, дополнительном (сентябрьском) периоде 2022 года», от 20 октября 2021 года № 10-П-1415 «О возложении некоторых функций на автономное учреждение дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования», от 19 ноября 2021 года № 10-П-1569 «О формировании и ведении региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования, в 2021/2022 учебном году, дополнительном экзаменационном периоде 2022 года», учитывая письмо автономного учреждения дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования», – организации, уполномоченной осуществлять функции Регионального центра обработки

информации (далее – РЦОИ) от 15 декабря 2021 года № 10/42-Исх-946, в целях обеспечения соблюдения информационной безопасности в период проведения государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2022 году

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое положение об обеспечении информационной безопасности при проведении государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2022 году (далее – Положение).

2. Отделу адаптированных образовательных программ и итоговой аттестации Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры (далее – Департамент) обеспечить соблюдение мер информационной безопасности в период проведения государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена (далее – ГИА, ЕГЭ) в пределах полномочий, установленных Положением, утверждённым пунктом 1 настоящего приказа.

3. РЦОИ (В.В. Клюсова):

3.1. Организовать мероприятия по соблюдению информационной безопасности при проведении ГИА, ЕГЭ согласно Положению, утверждённому пунктом 1 настоящего приказа.

3.2. Осуществлять реализацию организационно-технических, технологических мероприятий по обеспечению информационной безопасности в РЦОИ.

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

3.4. Принять меры по обеспечению особого пропускного режима в РЦОИ в период организации и проведения ГИА, ЕГЭ.

3.5. Обеспечить проведение инструктажа лиц, привлекаемых к организации проведения ГИА, ЕГЭ, по соблюдению требований информационной безопасности.

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

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

4.1. Принять меры по обеспечению информационной безопасности при проведении ГИА, ЕГЭ согласно Положению, утверждённому пунктом 1 настоящего приказа, в том числе:

при получении, учете, хранении, доставке и приемке-передаче экзаменационных материалов;

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.

4.2. Организовать проведение инструктажа лиц, привлекаемых к проведению ГИА, ЕГЭ 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. Руководителям государственных образовательных организаций, находящихся в ведении Департамента (А.Б. Сарабаров, Г.К. Хидирлясов, О.Р. Савичева, А.В. Жуков, Л.В. Балвакова, Н.Н. Брусенцева, А.А. Еганова, Л.Б. Козловская):

5.1. Принять меры по обеспечению информационной безопасности при проведении ГИА, ЕГЭ согласно Положению, утверждённому пунктом 1 настоящего приказа.

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 организаций профессионального образования, реализующих основные образовательные программы основного общего и среднего общего образования, находящихся в ведении Департамента физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Л.Н. Керимуллова), Департамента культуры Ханты-Мансийского автономного округа – Югры (А.В. Тарасов, А.А. Кобцева), обеспечить исполнение подпунктов 5.1 – 5.3 настоящего приказа, в части касающейся.

7. Отделу организационной работы и защиты информации Департамента обеспечить рассылку и размещение настоящего приказа на сайте Департамента.

8. Контроль за исполнением настоящего приказа возложить на заместителя директора Департамента И.В. Святченко.

Директор Департамента

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 6BC06BC2746EC69D2E82DFBB39D142389152F0A2
Владелец Дренин Алексей Анатольевич
Действителен 29.10.2021 с по 29.01.2023

А.А. Дренин

Приложение к приказу Депобразования и молодежи Югры
24.01.2022 10-П-55

Положение об обеспечении информационной безопасности при проведении государственной итоговой аттестации по образовательным программам основного общего, среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2022 году
(далее – Положение)

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с:

федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;

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

федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

постановлениями Правительства Российской Федерации «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» от 31 августа 2013 года № 755, от 29 ноября 2021 года № 2085;

приказом Министерства просвещения Российской Федерации, Федеральной службы по надзору в сфере образования и науки (далее – Минпросвещения России, Рособрнадзор) от 7 ноября 2018 года № 189/1513 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования»;

приказом Минпросвещения России, Рособрнадзора от 7 ноября 2018 года № 190/1512 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего 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»;

приказами Рособрнадзора от 18 июня 2018 года № 831 «Об утверждении 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», 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»,

а также с учетом:

аттестата соответствия Государственной информационной системы «Центральный сегмент региональной информационной системы государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования Ханты-Мансийского автономного округа – Югры» (далее – ГИС «ЦС РИС ГИА ХМАО – Югры») требованиям по безопасности информации № 123/78, полученного автономным учреждением дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» – организацией, уполномоченной осуществлять функции Регионального центра обработки информации (далее – РЦОИ), действующего до 18 мая 2023 года;

информационного письма Управления защиты информации и специальной документальной связи Аппарата Губернатора

Ханты-Мансийского автономного округа – Югры от 28 января 2021 года № 01.08-Исх-260**.**

1.2. Настоящее Положение разработано с целью соблюдения информационной безопасности, конфиденциальности информации при подготовке и проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования, единого государственного экзамена (далее – ГИА, ЕГЭ) в 2022 году.

1.3. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА, ЕГЭ в 2022 году между:

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 молодежной политики Ханты-Мансийского автономного округа – Югры (далее – Департамент), иным органам исполнительной власти Ханты-Мансийского автономного округа – Югры (далее – государственные ОО).

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 (программно-аппаратные комплексы (далее – ПАК));

2.1.3. Программное обеспечение (далее – ПО) для:

формирования Региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования Ханты-Мансийского автономного округа – Югры (далее – РИС ГИА);

технологии передачи экзаменационных материалов (далее – ЭМ) ЕГЭ на дисковых носителях;

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 и информационно-коммуникационные технологии» в компьютерной форме (далее – КЕГЭ);

технологии сканирования ЭМ в штабе ППЭ;

технологии формирования, шифрования, отправки из РЦОИ, получения, расшифровки, печати, сканирования и отправки ЭМ на обработку в РЦОИ в формах ОГЭ, ГВЭ.

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

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 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, государственные ОО);

получении, учете, приеме-передаче ЭМ в РЦОИ;

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

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

обработке машиночитаемых форм ППЭ, обрабатываемых в специализированном программном обеспечении;

обеспечении деятельности Конфликтной комиссии Ханты-Мансийского автономного округа – Югры (далее – КК), в том числе с использованием программного комплекса для автоматизации работы конфликтных комиссий при рассмотрении апелляций участников ГИА, ЕГЭ (далее – ТПР КК);

хранение на бумажных носителях апелляционных комплектов участников ГИА, ЕГЭ.

3.2. За обеспечение информационной безопасности при подготовке и проведении ГИА, ЕГЭ в РЦОИ назначается ответственное лицо.

3.3. Помещения РЦОИ, используемые для осуществления обработки, сканирования, верификации, хранения ЭМ, а также для осуществления деятельности РПК, КК оборудуются ПАК на базе ip-камер, работающих в режиме on-line и ведущих круглосуточную видеозапись, что обеспечивает круглосуточное наблюдение на портале smotriege.ru в режиме реального времени за процессами, происходящими в указанных помещениях.

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, МОУО и ППЭ (ОО, государственные ОО);

получении ЭМ ГИА по образовательным программам среднего общего образования в форме ЕГЭ на дисковых носителях и последующей доставки в ОО (ППЭ);

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

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

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

получении доступа (пароля) к ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, ГИА по образовательным программам среднего общего образования в форме ГВЭ от РЦОИ;

получении, доставке и передаче токенов членов ГЭК, используемых при проведении ГИА по образовательным программам среднего общего образования в форме ЕГЭ, ЕГЭ.

3.5. ППЭ (ОО) обеспечивают информационную безопасность, конфиденциальность информации при:

получении ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, ГИА по образовательным

программам среднего общего образования в форме ГВЭ по защищенным каналам связи;

получении ЭМ ГИА по образовательным программам среднего общего образования в форме ЕГЭ, ЕГЭ на дисковых носителях;

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

печати полного комплекта ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ, ГВЭ в штабе ППЭ;

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

получении доступа (пароля) членами ГЭК к ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ;

переводе (сканировании) бланков ответов участников ГИА в электронный вид в штабе ППЭ;

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

отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ ГИА по образовательным программам среднего общего образования в форме ЕГЭ, ЕГЭ обратно в РЦОИ с помощью станции авторизации в штабе ППЭ;

получении и хранении токенов членов ГЭК;

хранении использованных/неиспользованных бланков и форм ППЭ, использованных КИМ и контрольных листов, испорченных/бракованных индивидуальных комплектов (далее – ИК) и использованных/неиспользованных электронных носителей, использованных черновиков в местах, определенных региональным правовым актом (приказом) Департамента, до 1 марта года, следующего за годом проведения экзамена.

3.6. Государственные ОО обеспечивают информационную безопасность, конфиденциальность информации 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 ГИА по образовательным программам среднего общего образования в форме ЕГЭ, ЕГЭ на дисковых носителях;

получении ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, ГИА по образовательным

программам среднего общего образования в форме ГВЭ по защищенным каналам связи;

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

печати полного комплекта ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ, ГВЭ в штабе ППЭ;

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

переводе (сканировании) бланков ответов участников ГИА в электронный вид в штабе ППЭ;

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

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

отправка пакетов с зашифрованными электронными образами бланков и форм ППЭ ГИА по образовательным программам среднего общего образования в форме ЕГЭ обратно в РЦОИ с помощью станции авторизации в штабе ППЭ;

получении и хранении токенов членов ГЭК;

хранении использованных/неиспользованных бланков и форм ППЭ, использованных КИМ и контрольных листов, испорченных/бракованных ИК и использованных/неиспользованных электронных носителей, использованных черновиков в местах, определенных региональным правовым актом (приказом) 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 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 собственно технических средств, позволяющих осуществлять обработку персональных данных;

предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

4.2. Для соблюдения информационной безопасности в РЦОИ, МОУО, ОО, государственных ОО разрабатывается и правовыми актами (приказами, другое) утверждается 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, ЕГЭ осуществляет разработку, издание правовых 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 сроками 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, а также границы контролируемой зоны указанных помещений.

5.2. Для информационного взаимодействия между поставщиками информации заключается соглашение об информационном взаимодействии между РЦОИ и МОУО, ОО, государственными 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 – Югры от 28 января 2021 года № 01.08-Исх-260).

5.3. Перед началом проведения ГИА, ЕГЭ, с целью обеспечения информационной безопасности, бесперебойной работы оборудования в РЦОИ реализуются мероприятия по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также СЗИ, 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 на доступ к информационным системам РИС ГИА два раза в год – перед началом сбора баз данных и перед началом проведения 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 межсетевого экрана (экранов);

обеспечение безопасного хранения ключевой информации программного обеспечения 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 сервере/серверах 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 СЗИ 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 штабе 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 по программам основного общего образования в формах ОГЭ, ГВЭ, и ГИА по образовательным программам среднего общего образования в форме ГВЭ.

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, ЕГЭ осуществляет разработку, издание правовых актов (приказов, другое) и контроль за их исполнением, по вопросам:

назначения муниципального 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 и прикладного программного обеспечения, а также СЗИ;

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. В рамках взаимодействия между РЦОИ, исполняющим функции оператора РИС ГИА, и МОУО, являющимися поставщиками информации в «Центральный сегмент РИС ГИА ХМАО – Югры» осуществляется заключение соглашения об информационном взаимодействии, в соответствии с Техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 28 января 2021 года № 01.08-Исх-260).

6.3. Для обеспечения информационной безопасности на территории муниципального образования, МОУО осуществляются мероприятия 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 сервере 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 сведений и формирования 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);

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 сервере/серверах 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 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;

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 получения членами ГЭК токена члена ГЭК, необходимого для применения технологий печати полного комплекта ЭМ в аудиториях ППЭ, сканирования ЭМ в штабе 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 по образовательным программам основного общего образования в формах ГВЭ, ОГЭ и ГИА по образовательным программам среднего общего образования в форме ГВЭ.

7. Комплекс мероприятий по обеспечению информационной безопасности в государственных ОО

В целях осуществления информационной безопасности в ППЭ (государственных ОО), государственные ОО обеспечивают реализацию комплекса мероприятий.

7.1. В период подготовки к ГИА, ЕГЭ 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 уровне государственной ОО в период внесения сведений об участниках ГИА, ЕГЭ;

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 государственной ОО;

регулярного обновления общесистемного и прикладного программного обеспечения, а также СЗИ;

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. В рамках взаимодействия между РЦОИ, исполняющим функции оператора РИС ГИА, и государственными ОО, являющимися поставщиками информации в «Центральный сегмент РИС ГИА ХМАО – Югры», осуществляется заключение соглашения об информационном взаимодействии, в соответствии с Техническими условиями (письмо Управления защиты информации и специальной документальной связи

Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 28 января 2021 года № 01.08-Исх-260).

7.3. Для обеспечения информационной безопасности в государственных ОО обеспечивается реализации 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 сервере 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 государственной ОО два раза в год: перед началом сбора сведений и формирования баз данных, перед началом ГИА, ЕГЭ;

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 государственной ОО;

установка и настройка на АРМ пользователей и сервере/серверах 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 государственной ОО);

обеспечение рабочих мест технических специалистов, организаторов в аудитории, руководителей ППЭ, членов ГЭК оборудованием и программным обеспечением, необходимым для организации применения технологий получения ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ, ГВЭ и ГИА по образовательным программам среднего общего образования в форме ГВЭ, по защищенным каналам связи, получения ЭМ ЕГЭ на дисковых носителях, печати полного комплекта ЭМ ЕГЭ в аудиториях ППЭ и печати полного комплекта ЭМ ГИА по образовательным программам основного общего в формах ОГЭ, ГВЭ, а также ЭМ ГИА по образовательным программам среднего общего образования в форме ГВЭ, в штабе ППЭ, сканирования ЭМ в штабе ППЭ, проведения устной части иностранного языка (раздел «Говорение») и КЕГЭ в соответствии с требованиями к оборудованию и программному обеспечению;

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

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

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), ОО обеспечивают реализацию комплекса мероприятий.

8.1. В период подготовки к ГИА, ЕГЭ осуществляется разработка, издание правовых 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 организационные действия 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 СЗИ;

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 реализации 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 сервере 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 ОО два раза в год: перед началом сбора сведений и формирования 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);

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

установка и настройка на АРМ пользователей и сервере/серверах 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 ОО);

обеспечение рабочих мест технических специалистов, организаторов в аудитории, руководителей ППЭ, членов ГЭК оборудованием
и программным обеспечением, необходимым для организации применения технологии получения ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ, ГВЭ, ГИА по образовательным программам среднего общего образования в форме ГВЭ по защищенным каналам связи, печати полного комплекта ЭМ ЕГЭ в аудиториях ППЭ и печати полного комплекта ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ, ГВЭ, ГИА по образовательным программам среднего общего образования в форме ГВЭ в штабе ППЭ, сканирования ЭМ ГИА, ЕГЭ в штабе ППЭ, проведения устной части иностранного языка (раздел «Говорение») и КЕГЭ в соответствии с требованиями к оборудованию и программному обеспечению;

обеспечение штаба ППЭ (ОО) необходимым оборудованием и программным обеспечением для проведения ГИА в соответствии с технологией проведения в Ханты-Мансийском автономном округе – Югре, в том числе, токенами членов ГЭК;

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

обеспечение специально выделенных и оборудованных помещений (кабинетов), в том числе металлическими шкафами, сейфами, металлическими стеллажами, позволяющими обеспечить сохранность ЭМ и документов, используемых при проведении ГИА, ЕГЭ, 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 проведения ГИА, ЕГЭ.

9.2. К информации конфиденциального характера относятся:

сведения, содержащие персональные данные участников ГИА, ЕГЭ, находящиеся на бумажных носителях (заявления, копии (сканкопии) личных документов: паспорт, документ об образовании, другое), электронных файлах РИС ГИА;

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

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

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

контрольные измерительные материалы ЕГЭ, ОГЭ по всем учебным предметам, содержащие комплексы заданий стандартизированной формы;

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 экзаменационных работ участников ГИА, ЕГЭ по всем учебным предметам;

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, государственной ОО) обязаны:

знать и выполнять требования настоящего Положения;

знать перечень сведений конфиденциального характера;

соблюдать требования по неразглашению сведений конфиденциального характера, ставших известными им при исполнении обязанностей в период организации проведения ГИА, ЕГЭ, 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 соответствующей 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, государственной ОО) запрещается:

использовать конфиденциальные сведения при ведении телефонных переговоров;

передавать документы, содержащие сведения конфиденциального характера по каналам факсимильной связи и в 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 другое) для записи конфиденциальных сведений;

выполнять на дому работы, связанные с информацией конфиденциального характера;

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, государственные ОО) обязаны незамедлительно поставить в известность руководителя РЦОИ, МОУО, ППЭ (ОО, государственной ОО) (соответственно) о сложившейся ситуации, для обеспечения проведения служебной проверки по соответствующему факту.

9.6. Комиссия, в полномочия которой входит проведение служебной проверки, устанавливает:

обстоятельства разглашения конфиденциальных сведений;

виновных в разглашении конфиденциальных сведений;

причины и условия, способствовавшие разглашению конфиденциальных сведений.

9.7. Служебная проверка 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 требования информационной безопасности, принимаются меры в соответствии с действующим законодательством Российской Федерации.