



**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 и среднего общего образования в Ханты-Мансийском автономном округе – Югре в 2019 году

г. Ханты-Мансийск
«20» 12 2018 г.

№ 1710

В соответствии с федеральными законами Российской Федерации 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», постановлением Правительства Российской Федерации от 31 августа 2013 года № 755 «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 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», 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 Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры (далее – Департамент) от 14 сентября 2018 года № 1245 «Об утверждении плана мероприятий («дорожной карты») по подготовке к проведению государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования и иных процедур оценки качества образования в Ханты-Мансийском автономном округе – Югре в 2019 году», от 26 сентября 2018 года № 1317 года «О возложении некоторых функций на автономное учреждение дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования», от 15 ноября 2018 года № 1537 «О формировании и ведении региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования, в 2019 году», в целях соблюдения информационной безопасности в период проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Ханты-Мансийском автономном округе – Югре в 2019 году

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое положение об обеспечении информационной безопасности при проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Ханты-Мансийском автономном округе – Югре в 2019 году (далее – Положение).

2. Отделу адаптированных образовательных программ и итоговой аттестации Департамента (О.И. Васяева) обеспечить соблюдение мер информационной безопасности в период проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования (далее – ГИА) в пределах полномочий, установленных Положением.

округа – Югры «Институт развития образования» (Г.В. Дивеева) - организации, уполномоченной осуществлять функции Регионального центра обработки информации (далее – РЦОИ):

3.1. Организовать мероприятия по соблюдению информационной безопасности при проведении ГИА согласно Положению.

3.2. Осуществлять реализацию организационно-технических мер по обеспечению информационной безопасности в РЦОИ.

3.3. Осуществлять консультационно-методическое сопровождение по организационно-техническим мерам, в части обеспечения информационной безопасности в органах местного самоуправления муниципальных образований Ханты-Мансийского автономного округа – Югры, осуществляющих управление в сфере образования (далее – МОУО), пунктах проведения экзамена.

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

3.5. Обеспечить проведение инструктажа лиц, привлекаемых к проведению ГИА, по соблюдению требований информационной безопасности.

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

4. Рекомендовать руководителям МОУО:

4.1. Принять меры по обеспечению информационной безопасности при проведении ГИА, 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) и пунктов проведения экзаменов программным обеспечением и средствами технической защиты информации.

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

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

5. Руководителям государственных образовательных организаций, находящихся в ведении Департамента (А.Б. Сарабаров, Г.К. Хидирлясов, И.В. Сосновская, Н.Н. Брусенцева, М.П. Энзель, Л.Б. Козловская, А.В. Жуков):

5.1. Принять меры по обеспечению информационной безопасности при проведении ГИА.

5.2. Организовать проведение инструктажа лиц, привлекаемых к проведению ГИА, 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. Отделу организационной работы и защиты информации Департамента (М.С. Русова) обеспечить рассылку и размещение настоящего приказа на сайте Департамента.

7. Ответственность за исполнение настоящего приказа возложить на начальника Управления общего образования Департамента.

Директор Департамента



А.А. Дренин

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 2019 году (далее – Положение)

1. Введение

Настоящее Положение разработано в соответствии с:

- федеральным законом Российской Федерации от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
- 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 31 августа 2013 года № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;
- приказом Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки (далее - Рособрнадзор) от 7 ноября 2018 № 190/1512 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования»;
- приказом Министерства просвещения Российской Федерации и Рособрнадзора от 7 ноября 2018 года № 189/1513 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования»;
- приказом Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 года № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

- приказом Рособнадзора 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»;

- приказом Рособнадзора от 17 декабря 2013 года № 1274 «Об утверждении порядка разработки, использования и хранения контрольных измерительных материалов при проведении государственной итоговой аттестации по образовательным программам основного общего образования и порядка разработки, использования и хранения контрольных измерительных материалов при проведении государственной итоговой аттестации по образовательным программам среднего общего образования»;

- приказом Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры от 15 ноября 2018 года № 1537 «О формировании и ведении региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования, в 2019 году»;

- аттестатом соответствия Государственной информационной системы «Центральный сегмент региональной информационной системы 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» (далее – АУ «Институт развития образования») требованиям по безопасности информации № 33800005/5-ДСП, действительным до 18 мая 2021 года;

- информационным письмом Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 6 апреля 2018 года № 01.08-Исх-252.

2. Общие положения

2.1. 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 (далее - ГИА) в 2019 году.

2.2. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА в 2019 году между:

- АУ «Институт развития образования» - организацией, 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, находящимися в ведении Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры (далее - Департамент).

3. Средства защиты информации

3.1. Средства защиты информации подразделяются на:

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

3.2.2. Программно-аппаратные (программно-аппаратные комплексы).

3.2.3. Программное обеспечение (далее – ПО) для:

- формирования региональной информационной системы обеспечения проведения ГИА (далее - РИС ГИА);

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

- технологии печати полного комплекта экзаменационных материалов в аудитории ППЭ;

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

- технологии сканирования в штабе ППЭ;

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

4. Перечень материалов, документов и условия их хранения

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

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

- формировании сведений и 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 экзаменационных материалов в РЦОИ;

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

- обеспечении осуществления деятельности предметных комиссий Ханты-Мансийского автономного округа – Югры (далее – ПК) при обработке и проверке экзаменационных работ участников ГИА, в том числе на бумажных носителях: оригиналы бланков ответов участников ГИА по технологии бумажный КИМ, протоколы проверок бланков ответов участников ГИА ПК, обезличенные копии бланков ответов № 2, дополнительных бланков ответов № 2, критерии оценивания экзаменационных работ, изображения бланков ответов участников ГИА, машиночитаемые формы ППЭ, обрабатываемые в ПО;

- обеспечении осуществления деятельности Конфликтной комиссии Ханты-Мансийского автономного округа – Югры (далее – КК), в том числе через технологическое программное решение конфликтной комиссии (далее – ТПР КК);

- хранение на бумажных носителях апелляционных комплектов участников ГИА.

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

4.4. МОУО обеспечивает информационную безопасность, конфиденциальность 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);
- переводе бланков ответов в электронный вид;
- отправке пакетов с электронными образами бланков и форм ППЭ по защищенным каналам связи;
- получении ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ;
- получении доступа (пароля) к ЭМ в формах ОГЭ и ГВЭ.

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

- получении пакетов с ЭМ на станции авторизации;
- печати полного комплекта ЭМ;
- отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ с помощью станции авторизации;
- получении ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ;
- получении доступа (пароля) к ЭМ в формах ОГЭ и ГВЭ.

4.6. Государственные образовательные организации, находящиеся в ведении Департамента, 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;
- переводе бланков ответов в электронный вид;
- отправке пакетов с электронными образами бланков и форм ППЭ по защищенным каналам связи;
- получении ЭМ ГИА по образовательным программам основного общего образования в формах ОГЭ и ГВЭ, среднего общего образования в форме ГВЭ;
- получении доступа (пароля) к ЭМ в формах ОГЭ и ГВЭ;
- получении пакетов с ЭМ на станции авторизации;
- печати полного комплекта ЭМ;
- отправке пакетов с зашифрованными электронными образами бланков и форм ППЭ с помощью станции авторизации.

5. Методы и способы защиты информации в РЦОИ, МОУО, ППЭ (ОО), государственных образовательных организациях, находящихся в ведении Департамента

5.1. Методами и способами защиты информации в РЦОИ, МОУО, ППЭ (ОО), государственных образовательных организациях, находящихся в ведении Департамента, 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, исключаящее 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;

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

5.2. Для соблюдения информационной безопасности разрабатывается комплекс мероприятий, издаются правовые акты, приказами назначаются ответственные лица.

6. Комплекс мероприятий по обеспечению информационной безопасности в РЦОИ

6.1. В целях обеспечения информационной безопасности АУ «Институт развития образования» осуществляется комплекс мероприятий по разработке и изданию локальных актов:

- о назначении ответственного лица за обеспечение защиты информации, в том числе по выполнению функций организации и обработки 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 (далее – ОРД);

- 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 (далее – ФИС ГИА) из РИС ГИА в соответствии со сроками и внесения и передачи в процессе репликации сведений в ФИС ГИА и РИС ГИА;

- 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, а также границы контролируемой зоны указанных помещений.

6.2. 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 – Югры от 06.04.2018 № 01.08-Исх-252).

6.3. 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 информации от несанкционированного доступа в соответствии с требованиями ОРД по защите информации, в том числе обязательная смена паролей на доступ к информационным системам РИС ГИА с периодичностью два раза в год: перед началом сбора баз данных и перед началом ГИА, в том числе в форме единого государственного экзамена (далее – ЕГЭ);

- формирование и ведение журнала учета смены паролей;

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

- установка и настройка межсетевых экранов (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 ПО;

- удаление или блокировка на АРМ (сервере/серверах, в случае наличия) средств беспроводного доступа;

- эксплуатация средств антивирусной защиты в соответствии с требованиями по защите информации, в том числе ежедневное обновление базы средств антивирусной защиты;

- регулярное обновление общесистемного и прикладного ПО, 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 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 Государственной экзаменационной комиссии Ханты-Мансийского автономного округа – Югры (далее – ГЭК) ключа шифрования, записанного на защищенный внешний носитель (далее – токен члена ГЭК), необходимого для применения технологий получения ЭМ по информационно-

телекоммуникационной сети «Интернет», печати полного комплекта ЭМ в аудиториях ППЭ, сканирования ЭМ в штабе ППЭ и проведения устной части иностранного языка (раздел «Говорение»):

- обеспечение соблюдения информационной безопасности при формировании, шифровании и отправке ЭМ ОГЭ и ГВЭ по программам основного общего и среднего общего образования.

7. Комплекс мероприятий по обеспечению информационной безопасности в МОУО

7.1. Для обеспечения информационной безопасности в МОУО осуществляется комплекс мероприятий по разработке и изданию правовых актов МОУО:

- о назначении ответственного лица за защиту информации, в том числе по выполнению функций по организации и обработке 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 ОРД;

- 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;

7.2. Заключение соглашений об информационном взаимодействии между РЦОИ и МОУО (поставщиками сведений в «Центральный сегмент РИС ГИА ХМАО-Югры») осуществляется в соответствии с Техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 06.04.2018 № 01.08-Исх-252);

7.3. 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 информации от несанкционированного доступа в соответствии с требованиями по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на муниципальном уровне с периодичностью 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 сервере/серверах сертифицированного антивирусного ПО;

- удаление или блокировка на АРМ (и сервере/серверах, при наличии) средств беспроводного доступа;

- эксплуатация средств антивирусной защиты в соответствии с требованиями 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 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 получения ЭМ по информационно-телекоммуникационной сети «Интернет», печати полного комплекта ЭМ в аудиториях ППЭ, сканирования ЭМ в штабе ППЭ и проведения устной части экзамена по иностранному языку (раздел «Говорение»);

- обеспечение соблюдения информационной безопасности при получении и отправке ЭМ ОГЭ и ГВЭ по программам основного общего и среднего общего образования.

8. Комплекс мероприятий по обеспечению информационной безопасности в государственных образовательных организациях, находящихся в ведении Департамента

8.1. Для обеспечения информационной безопасности в государственных образовательных организациях, находящихся в ведении Департамента, осуществляется комплекс мероприятий по разработке и изданию локальных актов ОО:

- о назначении ответственного лица за защиту информации, в том числе по выполнению функций по организации и обработке персональных данных в РИС ГИА на уровне ОО 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 с ОРД;

- 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 РЦОИ и ОО (поставщиками сведений в «Центральный сегмент РИС ГИА ХМАО-Югры») осуществляется в соответствии с Техническими условиями (письмо Управления защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 06.04.2018 № 01.08-Исх-252);

8.3. Для обеспечения информационной безопасности в ОО осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновления общесистемного и прикладного ПО, 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 по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на уровне образовательной организации с периодичностью 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 сервере/серверах сертифицированного антивирусного ПО;

- удаление или блокировка на АРМ (и сервере/серверах, при наличии) средств беспроводного доступа;

- эксплуатация средств антивирусной защиты в соответствии с требованиями 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 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 штабе ППЭ и проведения устной части иностранного языка (раздел «Говорение») в соответствии с требованиями к оборудованию и ПО;

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

- обеспечение соблюдения информационной безопасности при получении и отправке ЭМ ОГЭ и ГВЭ по программам основного общего и среднего общего образования.

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

9.1. Для обеспечения информационной безопасности в ППЭ (ОО) осуществляется комплекс мероприятий по разработке и изданию локальных актов ОО:

- о назначении ответственного лица за защиту информации, в том числе по выполнению функций по организации и обработке персональных данных в РИС ГИА на уровне ОО 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 с ОРД;

- 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 информации с указанием границы контролируемой зоны;

9.2. Для обеспечения информационной безопасности в ОО осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного ПО, 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 информации от несанкционированного доступа в соответствии с требованиями по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на уровне ОО с периодичностью 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 ОО;
- установка и настройка на АРМ пользователей и сервере/серверах сертифицированного антивирусного ПО;
- удаление или блокировка на АРМ (и сервере/серверах, при наличии) средств беспроводного доступа;
- эксплуатация средств антивирусной защиты в соответствии с требованиями 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 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 штабе ППЭ и проведения устной части экзамена по иностранному языку (раздел «Говорение») в соответствии с требованиями к оборудованию и программному обеспечению;
- обеспечение штаба ППЭ необходимым оборудованием и ПО 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 ЭМ ОГЭ и ГВЭ по программам основного общего и среднего общего образования.

10. Ответственность лиц за обеспечение информационной безопасности при работе с персональными данными, информацией конфиденциального характера

10.1. 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 дополнительные бланки 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 дополнительные бланки ответов № 2);

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

- тексты, билеты, задания на электронных и бумажных носителях;

- экзаменационные материалы ГИА по образовательным программам основного общего и среднего общего образования;

- формы ППЭ на бумажных и электронных носителях;

- критерии оценивания экзаменационных работ участников ГИА;

- протоколы проверок экспертов ПК;

- сведения об организаторах и руководителях ППЭ ГИА, членах ГЭК, экспертах РПК, общественных наблюдателях, содержащиеся в РИС ГИА.

10.2. Информационная безопасность при проведении ГИА обеспечивается на всех этапах организации и проведения ГИА.

10.3. Специалисты, привлекаемые к работе, связанной со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ППЭ (ОО), государственных образовательных организаций, находящихся в ведении Департамента, 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 информацией;

- работать с документами и информацией конфиденциального характера в помещениях, определенных для работы с конкретного рода информацией.

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

10.4. Специалистам, привлекаемым к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ППЭ (ОО), государственных образовательных организаций, находящихся в ведении Департамента, запрещается:

- использовать конфиденциальные сведения при ведении телефонных переговоров;

- передавать документы, содержащие сведения конфиденциального характера по каналам факсимильной связи и в 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 также использовать различные технические средства (видео- и звукозаписывающую аппаратуру и др.) 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, определенных для работы с конкретного рода информацией.

10.5. 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, находящихся в ведении Департамента, обязаны немедленно поставить в известность руководителя РЦОИ, МОУО, ППЭ (ОО), государственной образовательной организации, находящейся в ведении Департамента, для принятия управленческих решений, в том числе служебного расследования по данному факту.

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

- обстоятельства разглашения конфиденциальных сведений;

- виновных в разглашении конфиденциальных сведений;

- причины и условия, способствовавшие разглашению конфиденциальных сведений.

10.7. 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.

10.8. К лицам, нарушившим правила и порядок информационной безопасности, применяются меры в соответствии с действующим законодательством Российской Федерации.