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 2017 году

г. Ханты-Мансийск

«26» 01 2017 г. № 79

В соответствии с Федеральными законами от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации», постановлением Правительства Российской Федерации от 31 августа 2013 года № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших 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 образовательные программы основного общего и среднего общего образования», приказами Министерства образования и науки Российской Федерации от 25 декабря 2013 года № 1394 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования», от 26 декабря 2013 года № 1400 «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 декабря 2016 года № 1857 «О возложении некоторых функций на автономное учреждение дополнительного профессионального образования Ханты-Мансийского

автономного округа – Югры «Институт развития образования» - организацию, уполномоченную осуществлять функции Регионального центра обработки информации, в 2017 году», от 28 июля 2016 года № 1189 «Об утверждении плана мероприятий («Дорожная карта») по подготовке к проведению государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в Ханты-Мансийском автономном округе – Югре в 2017 году», от 30 декабря 2016 года № 2039 «Об утверждении регламента взаимодействия Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры и автономного учреждения дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» - организации, уполномоченной осуществлять функции Регионального центра обработки информации, по обеспечению проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в 2017 году», согласно методическим рекомендациям по организации и проведению государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования (далее – ГИА) в 2017 году (письмо Управления оценки качества общего образования Федеральной службы по надзору в сфере образования и науки от 20 января 2017 года № 10-30, в целях соблюдения информационной безопасности в период проведения ГИА на территории Ханты-Мансийского автономного округа – Югры в 2017 году

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое положение об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования на территории Ханты-Мансийского автономного округа – Югры в 2017 году (далее – Положение).

2. Отделу адаптированных образовательных программ и итоговой аттестации Департамента (О.И. Васяева) обеспечить соблюдение мер информационной безопасности в период проведения ГИА в пределах полномочий, установленных Положением, утвержденным пунктом 1 настоящего приказа.

3. Автономному учреждению дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» - организации, уполномоченной осуществлять функции Регионального центра обработки информации (далее – РЦОИ) (Г.В. Дивеева):

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

3.2. Осуществлять реализацию организационно-технических мер по обеспечению информационной безопасности в РЦОИ, консультационно-методическое сопровождение по вопросам организационно-технических мер, связанных с обеспечением информационной безопасности в органах местного самоуправления муниципальных образований Ханты-Мансийского автономного округа – Югры, осуществляющих управление в сфере образования (далее – МОУО), пунктах проведения экзаменов;

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

3.4. Обеспечить проведение инструктажа лиц, привлекаемых к проведению ГИА, по соблюдению информационной безопасности;

3.5. Обеспечить соблюдение условий конфиденциальности и 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;

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

4.3. Обеспечить доступ к персональным данным, содержащимся в региональной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования (далее – РИС ГИА), и обработку указанных данных в соответствии с федеральным законодательством.

5. Руководителям государственных образовательных организаций Ханты-Мансийского автономного округа – Югры, находящихся в ведении Департамента (А.В. Сенин, Г.К, Хидирлясов, М.П. Энзель, Л.Б.Козловская, М.М. Ишбаев, А.В. Жуков, А.Б. Сарабаров), на базе которых организованы пункты проведения экзаменов:

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

5.2. Организовать проведение инструктажа лиц, привлекаемых к проведению ГИА, по соблюдению 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 официальном сайте Департамента.

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

8. Контроль за исполнением настоящего приказа возложить на первого заместителя директора Департамента.

И.о. директора Департамента Л.В. Максимова

Приложение к приказу
Департамента образования и молодежной политики
Ханты-Мансийского автономного округа – Югры
«25» 01 2017 г. № 79

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 2017 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 образования и науки Российской Федерации от 26 декабря 2013 года № 1400 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования»;
- приказом Министерства образования и науки Российской Федерации от 25 декабря 2013 года № 1394 «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 Федеральной службы по надзору в сфере образования и науки (Рособрнадзор) 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»;

- методическими рекомендациями по подготовке, проведению и обработке материалов единого государственного экзамена в региональных центрах обработки информации субъектов Российской Федерации в 2017 году, методическими рекомендациями по подготовке и проведению единого государственного экзамена в пунктах проведения экзаменов в 2017 году, методическими рекомендациями по организации системы видеонаблюдения при проведении государственной итоговой аттестации по образовательным программам среднего общего образования, методическими рекомендациями по подготовке и проведению государственной итоговой аттестации по образовательным программам основного общего образования в форме основного государственного экзамена и государственного выпускного экзамена в 2017 году (далее – методические рекомендации) (письмо Рособрнадзора от 20 января 2016 года № 10-30).

2. Общие положения

2.1. Настоящее Положение разработано с целью соблюдения информационной безопасности, конфиденциальности информации при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования (далее – ГИА) в 2017 году.

2.2. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА в 2017 году между:

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

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

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

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 РИС ГИА;
- технологии печати контрольных измерительных материалов (далее – КИМ) в аудитории ППЭ;
- технологии проведения устной части экзамена по иностранным языкам (раздел «Говорение»);
- технологии сканирования в штабе ППЭ.

3.2. Ответственным за обеспечение информационной безопасности при проведении ГИА, определен РЦОИ.

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

- формировании сведений в РИС ГИА, обработке персональных данных в РИС ГИА;
- обмене информацией, содержащей персональные данные, по выделенным линиям и защищенным каналам связи между РЦОИ и Федеральным государственным бюджетным учреждением «Федеральный центр тестирования» (далее – ФЦТ), РЦОИ и МОУО, РЦОИ и ППЭ (ОО);
- получении, учете, приеме-передаче экзаменационных материалов (далее – ЭМ) в МОУО;
- сканировании, верификации и экспертизе бланков участников ГИА;
- обеспечении осуществления деятельности предметных комиссий Ханты-Мансийского автономного округа – Югры (далее – ПК) (обработке и проверке экзаменационных работ участников ГИА на бумажных носителях: оригиналы бланков ответов участников ГИА по технологии бумажный КИМ; протоколы проверок бланков ответов участников ГИА Региональными предметными комиссиями (далее – РПК); 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;
- хранении ЭМ на бумажном носителе и апелляционных комплектов участников ГИА.

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

3.3. МОУО обеспечивает информационную безопасность, конфиденциальность информации при:

- формировании сведений в РИС ГИА на муниципальном уровне;
- обработке персональных данных в РИС ГИА на муниципальном уровне;
- обмене информацией, содержащей персональные данные, по защищенным каналам связи между МОУО и РЦОИ, МОУО и ППЭ (ОО);
- отправке зашифрованных экзаменационных материалов и форм ППЭ по технологии ЕГЭ 2017, технологии ГИА - 9.

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

- формировании сведений, вносимых в РИС ГИА на уровне образовательной организации;
- отправке зашифрованных экзаменационных материалов и форм ППЭ по технологии ЕГЭ 2016, технологии ГИА-9.

4. Методы и способы защиты информации в РЦОИ, МОУО, ППЭ (ОО)

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

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также в помещения где хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей информации;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- использование защищенных каналов связи;

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

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

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

5. Комплекс мероприятий по обеспечению информационной безопасности в РЦОИ

5.1. В целях обеспечения информационной безопасности автономным учреждением дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» (далее – АУ «Институт развития образования») осуществляется комплекс мероприятий по разработке и изданию локальных актов:

- о назначении ответственного за обеспечение защиты информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на региональном уровне;

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

- о назначении лиц, имеющих доступ к федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования (далее – 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;

5.2. Для обеспечения информационной безопасности в РЦОИ осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновлению общесистемного и прикладного программного обеспечения, а также средств защиты информации, в том числе:

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

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

- проведение постоянной работы с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями ОРД 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 ГИА, в том числе в форме 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 ПО vipnet (файл с расширением .dst), применяемой для связи с ФЦТ;

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

- установка и настройка на АРМ пользователей и сервера/серверов сертифицированного антивирусного программного обеспечения;

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

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

- регулярное обновление общесистемного и прикладного программного обеспечения, а также средств защиты информации в соответствии с разработанным регламентом;

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

- проведение работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно требованиям ОРД 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) токена (ключа шифрования), необходимого для применения технологии печати КИМ в аудиториях ППЭ и проведения устной части иностранного языка (раздел «Говорение»).

6. Комплекс мероприятий по обеспечению информационной безопасности в МОУО

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

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

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

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

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

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

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

- формирование и ведение журнала учета смены паролей;

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

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

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

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

- эксплуатация средств антивирусной защиты в соответствии с требованиями ОРД по защите информации;

- присвоение машинным носителям информации идентификационных номеров, в том числе ведение журнал учета машинных носителей информации;

- осуществление работ, связанных с использованием машинных носителей информации (учет, хранение, выдача, уничтожение), согласно требованиям ОРД 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 (ключ шифрования), необходимого для применения технологии печати КИМ в аудиториях ППЭ и проведения устной части иностранного языка (раздел «Говорение»).

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

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

- о назначении ответственного за защиту информации, в том числе по выполнению функций ответственного за организацию и обработку персональных данных в РИС ГИА на уровне образовательной организации в период внесения сведений об участниках ГИА;
- о назначении администратора безопасности, в том числе по осуществлению действий по техническому обеспечению функционирования СЗИ и организационные действия в соответствии 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;

7.2. Для обеспечения информационной безопасности в ОО осуществляется комплекс мероприятий по настройке оборудования, проведению работ по обеспечению безопасного хранения информации, обновления общесистемного и прикладного программного обеспечения, а также средств защиты информации, в том числе:

- установка на АРМ и сервер сертифицированных технических средств защиты от несанкционированного доступа (доступ пользователей только через идентификаторы и пароли), ведение журнала учета СЗИ;
- настройка технических средств защиты от несанкционированного доступа в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;
- проведение постоянных работ с идентификаторами, паролями, техническими средствами защиты от несанкционированного доступа в соответствии с требованиями ОРД по защите информации, в том числе обязательная смена паролей доступа к информационным системам РИС ГИА на уровне образовательной организации два раза в год: перед началом сбора баз данных и перед началом ГИА;
- формирование и ведение журнала учета смены паролей;
- повышение осведомленности пользователей в вопросах информационной безопасности (инструктажи, тренинги, регламентация прав и ответственности);

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

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

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

- эксплуатация средств антивирусной защиты в соответствии с требованиями ОРД 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 ОРД 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, уполномоченных представителей Региональной экзаменационной комиссии Ханты-Мансийского автономного округа – Югры (далее – РГЭК), оборудованием и ПО, необходимым для организации технологии печати КИМ в аудиториях ППЭ, технологии сканирования ЭМ в штабе ППЭ, технологии проведения устной части иностранных языков (раздел «Говорение») в аудитории ППЭ 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.

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

8.1. 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 дополнительный бланк ответов № 2);

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

- контрольные измерительные материалы ГИА по всем учебным предметам;

- экзаменационные материалы государственного выпускного экзамена за курс основного общего и среднего общего образования;

- формы ППЭ на бумажных и электронных носителях;

- критерии оценивания экзаменационных работ участников ГИА;

- протоколы проверок экспертов региональных предметных комиссий;

- сведения, содержащиеся в РИС ГИА, об организаторах и руководителях ППЭ ГИА, членах ГЭК, уполномоченных членах Региональной государственной комиссии Ханты-Мансийского автономного округа – Югры (далее – РГЭК), экспертах РПК, общественных наблюдателях.

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

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

- знать и выполнять требования настоящего Положения;

- знать перечень сведений конфиденциального характера;

- хранить в тайне 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;

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

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

- использовать конфиденциальные сведения при ведении телефонных переговоров;

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

- использовать конфиденциальные сведения в личных интересах;

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

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

- выносить документы и другие носители информации из здания.

8.5. В случае выявления факта разглашения конфиденциальных сведений специалисты, привлекаемые к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне РЦОИ, МОУО, ОО (ППЭ) обязаны немедленно поставить в известность руководителя РЦОИ, МОУО, ОО (ППЭ) для служебного расследования по данному факту.

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

- обстоятельства разглашения конфиденциальных сведений;

- виновных в разглашении конфиденциальных сведений;

- причины и условия, способствовавшие разглашению конфиденциальных сведений.

8.7. 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.

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