УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ ГОРОДА БЛАГОВЕЩЕНСКА

**(УПРАВЛЕНИЕ ОБРАЗОВАНИЯ ГОРОДА**)

* + 1. **п р и к а з**

«20» мая 2021 года № 386

г. Благовещенск

**Об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования2021 году**

В соответствии с Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Постановлением Правительства Российской Федерации от 31.08.2013 г. № 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 от 07.11.2018 г. №  189/1513 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам основного общего образования», совместным приказом Минпросвещения России и Рособрнадзора от 07.11.2018 № 190/1512 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования», утвержденного в целях обеспечения надлежащей информационной безопасности при проведении государственной итоговой аттестации году

**п р и к а з ы в а ю:**

1. Утвердить прилагаемое Положение об обеспечении информационной безопасности при проведении государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования в городе Благовещенске в 2021 году.

2. Назначить ответственными лицами за обеспечение информационной безопасности, конфиденциальности информации на муниципальном уровне Акусок И.В., начальника отдела общего и дополнительного образования, Ильину О.А., консультанта отдела общего и дополнительного образования.

2. Руководителям общеобразовательных организаций города Благовещенска:

2.1. принять меры по обеспечению информационной безопасности при проведении ГИА согласно Положению об обеспечении информационной безопасности при проведении ГИА в городе Благовещенске, в том числе:

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

2.2. обеспечить проведение инструктажа лицам, привлекаемым к проведению государственной итоговой аттестации, по соблюдению информационной безопасности.

3. Контроль исполнения приказа возложить на Акусок И.В., начальника управления образования администрации города.

Начальник управления образования

администрации города Э.Б. Поцелуева

Приложение

к приказу управления образования города

от 20.05.2021 № 386

**Положение**

**об обеспечении информационной безопасности**

**при проведении**

**государственной итоговой аттестации**

**в городе Благовещенске в 2021 году**

**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».

**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 2021 году.

2.2. Положение регламентирует деятельность по соблюдению информационной безопасности, конфиденциальности информации при проведении мероприятий ГИА в 2021 году между управлением образования администрации города, общеобразовательными организациями и пунктами проведения экзаменов.

**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 к ГИА назначается ответственное лицо:

4.2. Управление образования 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 муниципалитетом и РЦОИ;
* 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.

4.3. 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.

4.4. Общеобразовательные организации обеспечивают информационную безопасность, конфиденциальность информации при:

* формировании сведений, вносимых в РИС ГИА;
* обработке персональных данных в РИС ГИА;
* 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. Комплекс мероприятий по обеспечению информационной**

**безопасности в управлении образования администрации города**

5.1. Для обеспечения информационной безопасности в управлении образования осуществляется комплекс мероприятий по разработке и изданию правовых актов:

* 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 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;

5.2. Для обеспечения информационной безопасности в управлении образования 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);

* 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);
* 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.

**6. Комплекс мероприятий по обеспечению информационной безопасности в общеобразовательных организациях**

6.1. Для обеспечения информационной безопасности в общеобразовательных организациях 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 лиц, имеющих доступ к сегменту РИС ГИА на уровне общеобразовательной 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;

6.2. 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:

* 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 общеобразовательной 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);
* установка и настройка на АРМ пользователей и сервере/серверах сертифицированного антивирусного ПО;

-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;

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

**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 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 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;

7.2. 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 регионе, 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.

**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 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 ГВЭ 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.

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, управления образования, ППЭ (ОО), общеобразовательных организаций:

* 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.

8.4. Специалистам, привлекаемым к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне муниципалитета, ППЭ (ОО), общеобразовательных организаций 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.

8.5. В случае выявления факта разглашения конфиденциальных сведений специалисты, привлекаемые к работам, связанным со сбором, учетом, хранением информации конфиденциального характера на уровне муниципалитета, ППЭ (ОО), общеобразовательных организаций обязаны немедленно поставить в известность руководителя управления образования администрации города, ППЭ (ОО), общеобразовательной организации для принятия управленческих решений, в том числе служебного расследования по данному факту.

8.6 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.

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