МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ
ГОРОДСКОЙ ОКРУГ СУРГУТ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ

АДМИНИСТРАЦИЯ ГОРОДА

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ

от 23.03.2022 № 12-03-159/2

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ «УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ ГОРОДА СУРГУТА»

от 23.03.2022 № 47-П

ПРИКАЗ

Об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования на территории города Сургута

Во исполнение приказа Департамента образования и молодежной политики Ханты-Мансийского автономного округа – Югры от 24.01.2022 № 55 «Об обеспечении информационной безопасности при проведении мероприятий государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования, единого государственного экзамена в Ханты-Мансийском автономном округе – Югре в 2022 году» (далее – приказ Департамента), в соответствии с распоряжением Администрации города Сургута от 29.12.2018 № 2453 «О реализации мер по защите конфиденциальных данных», в целях соблюдения информационной безопасности в период проведения государственной итоговой аттестации по образовательным программам основного общего и среднего общего образования на территории города Сургута
ПРИКАЗЫВАЕМ:

1. Утвердить:

1.1. Список лиц, имеющих доступ к сегменту региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего образования (далее – РИС ГИА - 9), среднего общего образования (далее – РИС ГИА - 11), на муниципальном уровне согласно приложению 1.

1.2. Форму журнала учета съемных носителей конфиденциальной информации (персональных данных) согласно приложению 2.

1.3. Форму журнала учета смены паролей согласно приложению 3.

2. Возложить на лиц, указанных в приложении 1, ответственность за соблюдение информационной безопасности, конфиденциальности информации при:

- формировании сведений, вносимых в РИС ГИА - 9, РИС ГИА - 11;
- обработке персональных данных в РИС ГИА - 9, РИС ГИА - 11;
- обмене информацией, содержащей персональные данные;
- переводе бланков ответов в электронный вид;
- отправке пакетов с электронными бланками и формами;
- получении и направлении в пункты проведения экзаменов экзаменационных материалов (далее – ЭМ);
- получении доступа (пароля) к ЭМ и формам.

3. Муниципальному казенному учреждению «Управление информационных технологий и связи города Сургута» (далее – МКУ «УИТС») – организации, уполномоченной осуществлять функции по обеспечению безопасности конфиденциальной информации и персональных данных при их обработке в информационных системах, установленных на автоматизированных рабочих местах (далее – АРМ) в структурных подразделениях Администрации города:

3.1.Обеспечить:

- функционирование и обновление средств антивирусной защиты в соответствии с требованиями по защите информации на АРМ РИС ГИА – 11, установленном в департаменте образования (отдел общего образования, кабинет № 310);
- содействие при проведении регламентных работ с идентификаторами (логинами, паролями), в том числе обязательную смену паролей доступа к АРМ РИС ГИА - 11 с периодичностью два раза в год: перед началом сбора баз данных (первая неделя ноября), перед началом государственной итоговой аттестации по образовательным программам среднего общего образования (далее – ГИА) (первая неделя марта);
- работоспособность АРМ РИС ГИА - 11;
- возможность межсетевого взаимодействия АРМ РИС ГИА - 11 с АРМ с установленной региональной информационной системой обеспечения проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего образования (далее – АРМ РИС ГИА - 9), на базе муниципального автономного учреждения «Информационно-методический центр» (далее – МАУ «ИМЦ»), абонентскими

пунктами автономного учреждения дополнительного профессионального образования Ханты-Мансийского автономного округа – Югры «Институт развития образования» (подсеть VipNet 3675);

- меры по ограничению доступа к информации, отображаемой на дисплее монитора, установленного на АРМ РИС ГИА - 11.

3.2. Организовать:

- проведение инструктажа специалистов отдела общего образования, имеющих доступ к сегменту РИС ГИА - 11 на муниципальном уровне, указанных в приложении 1 к настоящему приказу, по соблюдению требований информационной безопасности;

- проведение периодической аттестации автоматизированных рабочих мест на соответствие требованиям безопасности информации согласно действующим требованиям ФСЭК и ФСБ.

3.3. Блокировать для пользователя РИС ГИА – 11 доступ через браузер к информационно-телекоммуникационной сети «Интернет».

4. Департаменту образования (отдел общего образования) организовать:

- ведение журнала учета съемных носителей конфиденциальной информации (персональных данных) согласно приложению 2 к настоящему приказу;

- ведение журнала учета смены паролей на АРМ РИС ГИА – 11 по форме согласно приложению 3 к настоящему приказу.

5. МАУ «ИМЦ» - организации, ответственной за формирование и ведение РИС ГИА - 9:

5.1. Организовать:

- формирование и ведение журнала учета смены паролей на АРМ РИС ГИА-9 в МАУ «ИМЦ» по форме согласно приложению 3 к настоящему приказу;

- проведение инструктажа лиц, ответственных за внесение, редактирование, обработку и передачу сведений в РИС ГИА на уровне общеобразовательных организаций (далее – ОО), МАУ «ИМЦ», по соблюдению требований информационной безопасности (тренинги, регламентация прав и ответственности);

- присвоение машинным и съемным носителям информации (персональных данных), используемым на базе МАУ «ИМЦ» для хранения резервных копий РИС ГИА - 9, идентификационных номеров, ведение журнала учета съемных носителей конфиденциальной информации согласно приложению 2 к настоящему приказу.

5.2. Обеспечить:

- проведение регламентных работ с идентификаторами (логинами, паролями), техническими СЗИ от НСД в соответствии с требованиями по защите информации, в том числе обязательную смену паролей доступа к АРМ РИС ГИА - 9 с периодичностью два раза в год: перед началом сбора баз данных (первая неделя ноября), перед началом ГИА (первая неделя марта);

- работоспособность АРМ РИС ГИА - 9, а также возможность межсетевого взаимодействия с АРМ РИС ГИА - 11, абонентскими пунктами АУ «Институт развития образования» (подсеть VipNet 3675);

- регулярное обновление общесистемного и прикладного программного обеспечения, а также СЗИ на АРМ РИС ГИА - 9;

- работоспособность VipNet Coordinator (подсеть 4815);

- удаление или блокировку на АРМ РИС ГИА - 9 средств беспроводного доступа;

- установку монитора на АРМ РИС ГИА - 9 с учетом ограничения доступа к видеоинформации любых лиц, кроме лиц, ответственных за внесение, редактирование, обработку и передачу сведений на уровне МАУ «ИМЦ»;

- регулярное обследование, защиту и аттестацию в соответствии с требованиями безопасности информации на всех АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 в ОО;

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

- соблюдение информационной безопасности при получении и отправке ЭМ основного государственного экзамена, государственного выпускного экзамена по программе основного общего образования.

5.3. Произвести настройку средств защиты от НСД в соответствии со списками доступных информационных ресурсов на АРМ РИС ГИА - 9 с использованием идентификаторов, первичных паролей.

5.4. Блокировать доступ к информационно-телекоммуникационной сети «Интернет» на АРМ РИС ГИА - 9.

5.5. Утвердить список лиц, допущенных в помещения, где установлены технические средства информационной системы и системы защиты, а также границы контролируемой зоны указанных помещений на базе МАУ «ИМЦ».

5.6. Исключить нахождение в помещениях МАУ «ИМЦ», где идет обработка информации, в том числе персональных данных, и в границах контролируемой зоны, посторонних лиц.

6. Руководителям общеобразовательных учреждений, реализующих образовательные программы основного общего и среднего общего образования:

6.1. Обеспечить:

- присвоение машинным и съемным носителям информации, используемым в ходе проведения ГИА на базе ОО, идентификационных номеров, ведение журнала учета съемных носителей конфиденциальной информации (персональных данных) согласно приложению 2 к настоящему приказу;

- регулярное обновление общесистемного и прикладного программного обеспечения, а также СЗИ на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 на базе ОО;

- установку на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 на базе ОО сертифицированных технических средств защиты от НСД (только через

идентификаторы и пароли), обеспечение формирования и ведения журнала учета СЗИ;

- настройку технических средств защиты от НСД в соответствии с идентификаторами, первичными паролями и списками доступных информационных ресурсов;

- проведение постоянных работ с идентификаторами, паролями, техническими СЗИ от НСД в соответствии с требованиями по защите информации, в том числе обязательная смена паролей доступа к АРМ РИС ГИА - 9, АРМ РИС ГИА - 11, с периодичностью два раза в год: перед началом сбора баз данных (первая неделя октября), перед началом ГИА (первая неделя февраля);

- формирование и ведение журнала учета смены паролей на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 по форме согласно приложению 3 к настоящему приказу;

- блокирование доступа к информационно-телекоммуникационной сети «Интернет» на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11;

- удаление или блокировку на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 средств беспроводного доступа;

- установку монитора на АРМ РИС ГИА - 9, АРМ РИС ГИА - 11 с учетом ограничения доступа к видеоинформации любых лиц, кроме лиц, ответственных за внесение, редактирование, обработку и передачу сведений на уровне ОО;

- эксплуатацию средств антивирусной защиты в соответствии с требованиями по защите информации.

6.2. Утвердить список лиц, допущенных в помещения, где установлены технические средства информационной системы и системы защиты, а также границы контролируемой зоны указанных помещений.

6.3. Исключить нахождение в помещениях, где идет обработка информации, в том числе персональных данных, и в границах контролируемой зоны, посторонних лиц.

7. Руководителям общеобразовательных учреждений, на базе которых организованы пункты проведения ГИА, обеспечить соблюдение мер информационной безопасности, конфиденциальности информации в период подготовки и проведения ГИА в пределах полномочий, установленных положением 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, утвержденным приказом Департамента.

8. Определить местом хранения ЭМ единого государственного экзамена до момента их передачи в пункты проведения экзаменов кабинет № 210 департамента образования (улица Гагарина, дом 11).

9. Действие настоящего приказа распространить на правоотношения, возникшие с 01.01.2022 года.

10. Контроль за выполнением приказа возложить на заместителя директора департамента Соловей Л.Г., директора МКУ «УИТС г. Сургута» Зыкова П.М.

Директор департамента И.П. Замятина

Директор МКУ «УИТС» П.М. Зыков

Приложение 1
к приказу
от _____ № _____

Список лиц, имеющих доступ к сегменту РИС ГИА на муниципальном уровне

№ п/п	Ф.И.О.	Должность
к РИС ГИА - 11, РИС ГИА - 9		
1.	Ходовец Павел Александрович	Главный специалист отдела общего образования департамента образования
2.	Базарова Елена Ивановна	Главный специалист отдела общего образования департамента образования
3.	Анисимова Валентина Александровна	Главный специалист отдела общего образования департамента образования
к РИС ГИА - 9		
4.	Басистюк Оксана Юрьевна	Начальник отдела диагностики и анализа качества образовательного процесса МАУ «ИМЦ»
5.	Рущенко Яна Ивановна	Методист отдела диагностики и анализа качества образовательного процесса МАУ «ИМЦ»

Приложение 2
к приказу
от _____ № _____

ЖУРНАЛ

учета съемных носителей конфиденциальной информации (персональных данных)

Начат: _____

Окончен:_____

г. Сургут, 2022

№ п/п	Наименование/ Учетный номер носителя	Дата выдачи	Подпись сотрудника, выдавшего носитель	Подпись сотрудника, получившего носитель	Сведения об уничтожении носителя	Примечание

Приложение 3
к приказу
от _____ № _____

Журнала учета смены паролей на АРМ РИС ГИА

№ п/п	ФИО владельца (работника)	Должность	Логин (имя пользователя)	Дата генерации пароля	ФИО выдавшего пароль