МИНИСТЕРСТВО ОБРАЗОВАНИЯ КУЗБАССА

ПРИКАЗ

От «09» 03. 2023 г. № 681 г. Кемерово

Об утверждении порядка приема, передачи и учета КриптоПроРутокен CSP при проведении государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе

В соответствии с Порядком проведения государственной итоговой аттестации по образовательным программам среднего общего образования, утвержденным приказом Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки от 07.11.2018 № 190/1512, в целях организационно-технологического обеспечения процедуры проведения государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый порядок приема, передачи и учета носителей КриптоПроРутокен CSP при проведении государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе.

2. Назначить ответственным лицом за работу с ключами шифрования на носителях «КриптоПроРутокен CSP» в Кемеровской области - Кузбассе Демидова Сергея Сергеевича, заместителя директора государственного казенного учреждения «Кузбасский центр мониторинга качества образования».

3. Отделу правовой и кадровой работы Министерства образования Кузбасса (Е.В. Каменская) разместить настоящий приказ в информационно-телекоммуникационной сети «Интернет» на сайте «Электронный бюллетень Правительства Кемеровской области - Кузбасс» и на официальном интернет-портале правовой информации».

4. Признать утратившим силу приказ департамента образования и

науки Кемеровской области от 25.03.2020 №723 «Об утверждении порядка приема, передачи и учета носителей КриптоПроРутокен CSP при проведении государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе».

5. Контроль за исполнением приказа оставляю за собой.

Министр образования Кузбасса С.Ю. Балакирева

Утвержден
приказом Министерства
образования Кузбасса
от 09.03.2023 № 681

Порядок приема, передачи и учета носителей КриптоПроРутокен CSP при проведении государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе

1. Назначение и область действия

Настоящий порядок приема, передачи и учета носителей КриптоПроРутокен CSP при проведении государственной итоговой аттестации по образовательным программам среднего общего образования в Кемеровской области - Кузбассе (далее – Порядок) определяет порядок работы членов государственной экзаменационной комиссии Кемеровской области - Кузбасса для проведения государственной итоговой аттестации по образовательным программам среднего общего образования (далее – члены ГЭК) и сотрудников государственного казенного учреждения «Кузбасский центр мониторинга качества образования», выполняющего функции регионального центра обработки информации (далее – ГКУ КЦМКО), уполномоченных Министерством образования Кемеровской области - Кузбасса (далее – Министерство), ответственных за расшифрование бланков ответов участников единого государственного экзамена (далее – уполномоченные сотрудники ГКУ КЦМКО), переведенных в электронный вид в пункте проведения экзамена (далее – ППЭ) с электронными ключами шифрования, записанными на ключевые носители, ПИН-конвертами, использующимися при проведении единого государственного экзамена (далее – ЕГЭ) в рамках реализации технологии доставки экзаменационных материалов по сети «Интернет», обеспечения процессов печати полного комплекта экзаменационных материалов в аудиториях ППЭ, сканирования экзаменационных материалов в аудиториях ППЭ, а также подготовки и проведения ЕГЭ по иностранным языкам (раздел «Говорение»), по предмету «Информатика и ИКТ» в компьютерной форме.

2. Основные понятия, используемые в Порядке

Ключевой носитель – средство криптографической защиты информации (далее – СКЗИ) КриптоПроРутокен CSP.

Пароль ключа шифрования – код, выдаваемый члену ГЭК и уполномоченному сотруднику ГКУ КЦМКО в запечатанном ПИН-конверте, использующемуся для доступа к ключу шифрования и относящегося к категории информации ограниченного доступа.

Ключ шифрования – файл с информацией, относящейся к категории ограниченного доступа, используемый для шифрования данных.

3. Основные технологические решения

3.1. Федеральная служба по надзору в сфере образования и науки

определяет организацию, ответственную за прием и отправку ключевых носителей, изготовление ключей шифрования и ПИН-конвертов, запись ключей шифрования на ключевые носители (далее – специализированная организация).

3.2. Ключи шифрования изготавливаются и записываются на ключевые носители специализированной организацией с помощью специализированного программного обеспечения (далее – ПО), при этом формируются данные об обработанных ключевых носителях для последующей загрузки 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 (далее – ФИС ГИА и Приема).

3.3. Ключи шифрования не привязаны к членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО и не содержат их персональных данных.

3.4. Специализированная организация направляет ключевые носители с записанными на них ключами шифрования, а также ПИН-конверты в адрес ГКУ КЦМКО средствами специальной связи.

3.5. Ключи шифрования имеют уникальные пароли для доступа к ним, которые выдаются членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО в запечатанном ПИН-конверте.

3.6. Ключи шифрования предназначены для использования на всех экзаменах в течение года.

3.7. Распределение ключей шифрования членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО осуществляется в ПО «Планирование ГИА (ЕГЭ)».

4. Порядок работы с ключами шифрования

4.1. В процессе подготовки к проведению ЕГЭ Министерство назначает ответственное лицо из числа сотрудников ГКУ КЦМКО, ответственных за работу с ключами шифрования, ключевыми носителями и ПИН-конвертами (далее – ответственное лицо).

4.2. Ответственное лицо осуществляет сбор ключевых носителей в Кемеровской области - Кузбассе, организует закупку недостающего количества ключевых носителей для членов ГЭК и уполномоченных сотрудников ГКУ КЦМКО.

4.3. Ответственное лицо устанавливает отметку о необходимости выдачи ключа шифрования в ПО «Планирование ГИА (ЕГЭ)».

4.4. Ответственное лицо формирует Опись и отправляет её по электронной почте в формате Microsoft Excel в адрес специализированной организации.

4.5. Ответственное лицо отправляет собранные ключевые носители в адрес специализированной организации средствами специальной связи.

4.6. Ключи шифрования выпускаются и записываются

специализированной организацией на направленные ответственным лицом ключевые носители в соответствии с описью.

4.7. Специализированная организация направляет ключевые носители с записанными на них ключами шифрования и ПИН-конверты в адрес ГКУ КЦМКО средствами специальной связи.

5. Выдача ключей шифрования

5.1. Выдача ключевых носителей с записанными на них ключами шифрования членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО организуется ответственным лицом.

5.2. Полученные из специализированной организации ключевые носители с записанными на них ключами шифрования учитываются в ПО «Планирование ГИА» путём проставления отметок о фактически полученных ключах шифрования.

5.3. После учета фактически полученных ключевых носителей и определения списка членов ГЭК и уполномоченных сотрудников ГКУ КЦМКО на региональном уровне средствами ПО «Планирование ГИА» выполняется ручное назначение ключевых носителей членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО.

5.4. По результатам назначения ключевых носителей с записанными на них ключами шифрования средствами ПО «Планирование ГИА» формируется ведомость выдачи ключевых носителей членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО.

5.5. Выдача ключевых носителей членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО производится в ГКУ КЦМКО, по ведомости на основании серийного номера ключевого носителя. Выдача ключей шифрования членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО производится лично по документу, удостоверяющему личность.

5.6. По номеру ключевого носителя и номеру ключа шифрования, указанному в ведомости, ответственное лицо идентифицирует нужный конверт с паролем (с таким же номером ключевого носителя и ключа шифрования). Ключевой носитель наклеен на конверт.

5.7. Если не найден конверт с необходимыми номерами, то члену ГЭК или уполномоченному сотруднику ГКУ КЦМКО выдаётся другой ключевой носитель с записанным на него ключом шифрования и ПИН-конвертом, данные с которого вносятся в ведомость.

5.8. Член ГЭК или уполномоченный сотрудник ГКУ КЦМКО, не вскрывая конверт с паролем, сверяет серийный номер ключевого носителя с указанным на конверте и в ведомости получения. В случае совпадения номеров член ГЭК или уполномоченный сотрудник ГКУ КЦМКО расписывается в ведомости.

5.9. Если номер на ключевом носителе не совпадает с номером на конверте, такой ключевой носитель не выдаётся.

5.10. Член ГЭК или уполномоченный сотрудник ГКУ КЦМКО проверяет работоспособность полученного ключевого носителя. Проверка выполняется подключением ключевого носителя к компьютеру с

установленным КриптоПроРутокен CSP и введением членом ГЭК или уполномоченным сотрудником ГКУ КЦМКО пароля доступа к ключевому носителю (далее – проверка).

5.11. После выдачи ключевых носителей информация (о факте выдачи, времени выдачи и ФИО получившего ключевой носитель) из ведомости вносится в ПО «Планирование ГИА», скан-копия ведомости загружается в ПО «Планирование ГИА».

5.12. Информация о распределении ключевых носителей членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО передается в ФИС ГИА и Приема.

5.13. На основе поступившей информации о распределении ключевых носителей членам ГЭК и назначении членов ГЭК на экзамены в ППЭ, выполняется формирование ключей доступа к КИМ для соответствующих ключей шифрования членов ГЭК.

5.14. В случае, если ключевой носитель был выдан члену ГЭК, но в ПО «Планирование ГИА» отсутствует отметка о получении ключевого носителя, то ключ доступа к КИМ для данного члена ГЭК не формируется.

5.15. Информация о распределении ключевых носителей уполномоченных сотрудников ГКУ КЦМКО используется для передачи ключей шифрования уполномоченных сотрудников ГКУ КЦМКО в ППЭ Кемеровской области - Кузбасса.

5.16. Передача ключей шифрования уполномоченных сотрудников ГКУ КЦМКО в ППЭ выполняется при подключении к порталу на этапе технической подготовки.

5.17. По окончании проведения экзаменов ответственное лицо осуществляет сбор выданных членам ГЭК и уполномоченным сотрудникам ГКУ КЦМКО ключевых носителей с ключами шифрования под подпись о возврате в ведомости выдачи ключевых носителей.

6. Замена, удаление ключей шифрования членов ГЭК

6.1. В случае необходимости замены ключевого носителя (ключа шифрования) члену ГЭК или уполномоченному сотруднику ГКУ КЦМКО соответствующие изменения вносятся в ПО «Планирование ГИА».

6.2. Информация об изменениях в распределении ключевых носителей членов ГЭК или уполномоченных сотрудников ГКУ КЦМКО, внесенная в ПО «Планирование ГИА», передается в ФИС ГИА и Приема. Неактуальные ключи шифрования членов ГЭК не используются при формировании ключей доступа к экзаменационным материалам, неактуальные ключи шифрования уполномоченных сотрудников ГКУ КЦМКО не передаются в ППЭ.

6.3. При необходимости изъятия у члена ГЭК или уполномоченного сотрудника ГКУ КЦМКО ключевого носителя с записанным на него ключом шифрования в ПО «Планирование ГИА» ставится соответствующая отметка.

6.4. Удаленные ключи шифрования членов ГЭК не используются при формировании ключей доступа к экзаменационным материалам. Удаленные ключи шифрования уполномоченных сотрудников ГКУ КЦМКО не передаются в ППЭ.

6.5. В случае потери ключевого носителя или выхода его из строя в ПО «Планирование ГИА» делается соответствующая отметка.

7. Выдача членам ГЭК паролей доступа к ключевым носителям

7.1. В случае потери ключа шифрования и невозможности членом ГЭК или уполномоченным сотрудником ГКУ КЦМКО ввести его правильный пароль, если ключ шифрования еще не заблокирован (не превышено число неудачных попыток ввода пароля), член ГЭК или уполномоченный сотрудник ГКУ КЦМКО обращается на горячую линию ЕГЭ и сообщает:

1) ФИО;

2) номер мобильного телефона, на который будет выслан пароль;

3) код субъекта Российской Федерации;

4) номер ключа шифрования;

5) номер ключевого носителя.

Специалист горячей линии ЕГЭ передает указанные сведения в специализированную организацию, в ответ получает пароль.

Специалист горячей линии ЕГЭ пересылает пароль члену ГЭК или уполномоченному сотруднику ГКУ КЦМКО СМС-сообщением.