

УТВЕРЖДАЮ

Директор
Федерального государственного
бюджетного учреждения
«Федеральный центр тестирования»

 С.В. Водолазков

« ____ » _____ 2016 г.

СОГЛАСОВАНО

Начальник
Управления оценки качества общего
образования Федеральной службы по
надзору в сфере образования и науки

 Ю.С. Егорова

« 30 » декабря 2016 г.

СОГЛАСОВАНО

Начальник
Управления перспективных и
специальных средств и комплексов
обеспечения информационной
безопасности ФГАНУ ЦИТиС

 В.Г. Архангельский

« ____ » _____ 2016 г.

**Порядок работы с электронными ключами шифрования,
электронными носителями и ПИН-конвертами при подготовке и
проведении государственной итоговой аттестации обучающихся,
освоивших образовательные программы среднего общего
образования в 2017 году в рамках обеспечения процессов печати
КИМ в аудиториях пунктов проведения экзаменов, перевода
бланков ответов участников ЕГЭ в электронный вид, подготовки и
проведения ЕГЭ по иностранным языкам с включенным разделом
«Говорение»**

1. Назначение и область действия

Настоящий документ определяет порядок работы членов государственной экзаменационной комиссии (далее – ГЭК) и сотрудников региональных центров обработки информации (далее – РЦОИ), уполномоченных органами исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования (далее – уполномоченные сотрудники РЦОИ), ответственных за расшифровывание бланков ответов участников ЕГЭ, переведенных в электронный вид в пункте проведения экзамена (далее – ППЭ) с электронными ключами шифрования, записанными на ключевые носители, ПИН-конвертами, используемыми при проведении ЕГЭ в рамках обеспечения процессов печати КИМ в аудиториях ППЭ, а так же подготовки и проведения ЕГЭ по иностранным языкам с включенным разделом «Говорение».

2. Основные понятия, используемые в документе

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

Пароль ключа шифрования – код, выдаваемый члену ГЭК и уполномоченному сотруднику РЦОИ в запечатанном ПИН-конверте, использующегося 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 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 РЦОИ 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 ОИВ или организаций, назначенных ОИВ, средствами специальной связи.

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

3.6. Ключи шифрования предназначены для использования на всех экзаменах в течение 2017 года.

3.7. Распределение ключей шифрования членам ГЭК и уполномоченным сотрудникам РЦОИ осуществляется в программном обеспечении «Планирование ГИА» (см. Инструкцию по работе с ключами шифрования членов ГЭК в ПО «Планирование ГИА (ЕГЭ)» - далее - Инструкция).

4. Порядок работы с ключами шифрования

4.1. В процессе подготовки к проведению ЕГЭ ОИВ назначает лицо из числа сотрудников ОИВ или РЦОИ, ответственных за работу с ключами шифрования, ключевыми носителями и ПИН-конвертами (далее – Ответственное лицо).

4.2. Ответственное лицо осуществляет сбор ключевых носителей в субъекте РФ, организует закупку недостающего количества ключевых носителей

для членов ГЭК и (или) уполномоченных сотрудников РЦОИ.

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

4.4. Ответственное лицо формирует Опись и отправляет её по электронной почте в формате Microsoft Excel в адрес специализированной организации (Приложение № 1 к настоящему Порядку).

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

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 ОИВ или организации, назначенной ОИВ, средствами специальной связи согласно Ведомости (Приложение № 2 к настоящему Порядку).

5. Выдача ключей шифрования

5.1. Выдача ключевых носителей с записанными на них ключами шифрования членам ГЭК и уполномоченным сотрудникам РЦОИ 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 РЦОИ на региональном уровне средствами ПО «Планирование ГИА» выполняется ручное или автоматическое (случайное) назначение ключевых носителей членам ГЭК и уполномоченным сотрудникам РЦОИ.

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 РЦОИ (см. Инструкцию).

5.5. Ведомость выдачи ключевых носителей членам ГЭК и уполномоченным сотрудникам РЦОИ может быть сводной или формироваться отдельно.

5.6. Выдача ключевых носителей членам ГЭК и уполномоченным сотрудникам РЦОИ осуществляется по ведомости на основании серийного номера ключевого носителя.

5.7. 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.

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

5.9. Член ГЭК или уполномоченный сотрудник РЦОИ, 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 РЦОИ расписывается в ведомости.

5.10. Если номер на ключевом носителе не совпадает с номером на конверте, такой ключевой носитель не выдаётся. О данном факте необходимо сообщить на горячую линию ЕГЭ по телефону: 8 (495) 989-11-97.

5.11. Член ГЭК или уполномоченный сотрудник РЦОИ проверяет работоспособность полученного ключевого носителя. Проверка выполняется подключением ключевого носителя к компьютеру с установленным ПО КриптоПро Рутокен CSP и введением членом ГЭК или уполномоченным

сотрудником РЦОИ пароля доступа к ключевому носителю (далее – Проверка).

5.12. В случае выдачи ключевых носителей в ППЭ-ТОМ Проверка выполняется в любом ППЭ в рамках технической подготовки к проведению экзаменов.

5.13. В случае выдачи ключевых носителей в ОИВ или РЦОИ проверка выполняется Ответственным лицом только в случае успешной Проверки работоспособности ключевого носителя.

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

5.15. Информация о распределении ключевых носителей членам ГЭК и уполномоченным сотрудникам РЦОИ передается в ФИС ГИА и Приема.

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

5.17. 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.

5.18. Информация о распределении ключевых носителей уполномоченных сотрудников РЦОИ используется для передачи ключей шифрования уполномоченных сотрудников РЦОИ в ППЭ соответствующего субъекта Российской Федерации.

5.19. Передача ключей шифрования уполномоченных сотрудников РЦОИ в ППЭ выполняется при подключении к portalу на этапе технической подготовки.

5.20. По окончании проведения экзаменов Ответственное лицо осуществляет сбор выданных членам ГЭК и уполномоченным сотрудникам

РЦОИ ключевых носителей с ключами шифрования под роспись 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 РЦОИ соответствующие изменения необходимо внести в ПО «Планирование ГИА» (см. Инструкцию).

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

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

6.4. Удаленные ключи шифрования членов ГЭК не используются при формировании ключей доступа к КИМ. Удаленные ключи шифрования уполномоченных сотрудников РЦОИ не передаются в ППЭ.

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

7. Выдача членам ГЭК паролей доступа к ключевым носителям

9.1. В случае утери ключа шифрования и невозможности членом ГЭК или уполномоченным сотрудником РЦОИ ввести его правильный пароль, если ключ шифрования еще не заблокирован (не превышено число неудачных попыток ввода пароля):

Член ГЭК или уполномоченный сотрудник РЦОИ обращается на горячую линию ЕГЭ, по телефону: 8 (495) 989-11-97, и сообщает:

- ФИО;
- номер мобильного телефона, на который будет выслан пароль;
- код субъекта Российской Федерации;
- номер ключа шифрования;
- номер ключевого носителя.

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

Специалист горячей линии ЕГЭ пересылает пароль члену ГЭК или уполномоченному сотруднику РЦОИ SMS-сообщением.

8. Выдача членам ГЭК паролей доступа к КИМ

10.1. В случае если в ППЭ отсутствует подключение к сети Интернет и пароль не может быть получен штатными средствами с портала, член ГЭК обращается на горячую линию ЕГЭ, по телефону 8 (495) 989-11-97, и сообщает:

- ФИО;
- код субъекта Российской Федерации;
- код ППЭ;
- номер мобильного телефона, на который будет выслан пароль;
- номер ключевого носителя;
- номер ключа шифрования;
- код активации пароля (отображается на станции авторизации).

Специалист горячей линии ЕГЭ пересылает пароль члену ГЭК SMS-сообщением.

ОПИСЬ

СКЗИ Рутокен Криптопро CSP, используемых при проведении единого государственного экзамена в _____ (наименование субъекта Российской Федерации)

№ п/п	Серийный номер	Дата отправки	ФИО отправителя	Должность отправителя
1	2	3	4	5
1				
2				
3				

Ответственный за
работу с ключами
шифрования в
субъекте Российской
Федерации

<Должность>

<Фамилия, имя, отчество>

подпись

ВЕДОМОСТЬ

поэкземплярного учета ключевых документов для проведения
единого государственного экзамена в 2017 году,
изготовленных специализированной организацией и
направленных в _____

<наименование субъекта РФ>

№ п/п	Номер ключевого документа	Серийный номер носителя КриптоПРО Рутокен CSP	Номер экземпляра ключевого документа	Примечание
1	2	3	4	5
1			Единственный	
2			Единственный	
3			Единственный	
4			Единственный	
5			Единственный	
6			Единственный	

<Должность>

<Фамилия, имя, отчество>

подпись