

ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ И ПРОГРАММНОМУ
ОБЕСПЕЧЕНИЮ ППЭ ДЛЯ ПРОВЕДЕНИЯ ЕГЭ ПО ВСЕМ
ИНОСТРАННЫМ ЯЗЫКАМ С КОМПОНЕНТОМ В УСТНОЙ ФОРМЕ

Москва 2014

Перечень принятых сокращений и терминов

В настоящем документе используются следующие термины и сокращения:

АРМ	Автоматизированное рабочее место
ЕГЭ	Единый государственный экзамен
КИМ	Контрольные измерительные материалы
ПО	Программное обеспечение
ППЭ	Пункт проведения экзамена
ЭП	Электронная подпись

1. Требования к техническому и программному оснащению ППЭ

В следующей таблице (см. Таблица 1) приведены требования к аппаратному и программному обеспечению, необходимому для проведения экзамена с использованием технологии печати КИМ в аудиториях ППЭ.

Таблица 1

Компонент	Количество	Конфигурация
Рабочая станция в штабе ППЭ	1	Операционная система: WindowsXPservicepack 3/Vista / 7 платформы:ia32 (она же x86), x64. Дополнительное ПО: Microsoft .NET Framework 4.0 и выше. Внешний интерфейс: USB 2.0. Наличие стабильного канала связи с выходом в Интернет. Дополнительных специальных требований к рабочей станции не предъявляется.
Резервный USB модем	1	Резервный USBмодем используется в случае возникновения проблем с доступом в сеть Интернет по стационарному каналу связи.
Токен	по 1 на каждого члена ГЭК	USB-ключ для хранения сертификата члена ГЭК. Детальные требования даны ниже.
Флэш-носитель	1	Флэш-носитель используется техническим специалистом для переноса ключа доступа к электронным КИМ из штаба ППЭ в аудиторию.

Компонент	Количество	Конфигурация
Рабочая станция участника экзамена	до 4 рабочих станций на аудиторию	<p>Операционная система: Windows XP service pack 3 / Vista / 7 платформы: ia32 (она же x86), x64.</p> <p>Дополнительное ПО: Microsoft .NET Framework 4.0 и выше.</p> <p>Оперативная память: минимальная 1 Gb, рекомендуемая 2 Gb.</p> <p>Процессор: минимальная конфигурация: одноядерный 3,0 ГГц; рекомендуемая конфигурация: двухъядерный 2,5 ГГц.</p> <p>Свободное дисковое пространство: от 10 Гбайт.</p> <p>Устройство резервного копирования: ATAPI CD-RW.</p> <p>Внешний интерфейс: USB 2.0</p> <p>Манипулятор «мышь».</p> <p>Клавиатура.</p> <p>Производительность видеоадаптера не менее рекомендуемой для установленной ОС.</p> <p>Звуковая карта.</p> <p>Монитор: разрешение не менее 1280x1024.</p> <p>Специализированное программное обеспечение: Microsoft .Net Framework 4.0.</p>
Аудио оборудование	на каждую рабочую станцию участника экзамена	<p>Тип оборудования: компьютерная гарнитура наушники с микрофоном.</p> <p>Наушники: наушники со встроенным микрофоном, накладные, полуоткрытого типа, тип крепления: оголовье. Рекомендуются закрытого типа (с шумоизоляцией).</p> <p>Микрофон: с подвижным креплением (не на проводе), чувствительность не менее: -60 dB</p> <p>Рекомендуется: наушники со встроенным микрофоном, с шумоподавлением.</p>
Локальный лазерный принтер	1	<p>Формат: не менее А4.</p> <p>Тип печати: черно-белая.</p> <p>Технология печати: лазерная.</p> <p>Скорость черно-белой печати (обычный режим, А4): 20 стр./мин.</p> <p>Качество черно-белой печати (режим наилучшего качества): не менее 600 x 600 точек на дюйм.</p>

Примечание:

Для проведения устной части экзамена по иностранному языку по технологии единого государственного экзамена в пункте проведения экзамена наличие локальной сети не требуется.

Требования к носителям (токенам) сертификата члена ГЭК

Электронный носитель сертификата члена ГЭК (токен) должен соответствовать следующим требованиям:

1. Тип носителя: USB-ключ.
2. Аппаратная реализация алгоритма ГОСТ 28147-89 (зашифрование/расшифрование блоков данных, вычисление имитовставки).
3. Генерация ключа парной связи по алгоритму Диффи-Хеллмана согласно RFC 4357.
4. В комплект поставки должна входить лицензия на КриптоПро CSP версии 3.6 и сертификат ФСБ о соответствии требованиям, предъявляемым к средствам электронной подписи и к средствам криптографической защиты информации по классу не ниже КС2.
5. Должна поддерживаться вся функциональность СКЗИ КриптоПро CSP 3.6.
6. Носитель не должен иметь дополнительной флеш-памяти.
7. Аппаратная реализация российских алгоритмов ЭЦП в аппаратных ключах, криптографические операции на закрытых ключах выполняются внутри носителя, при этом ключи не покидают само устройство.
8. С использованием аппаратных ресурсов носителя должны выполняться следующие криптографические операции:
 - a. генерация ключевых пар ГОСТ Р 34.10-2001,
 - b. формирование электронной подписи по ГОСТ Р 34.10-2001,
 - c. шифрование по ГОСТ 28147-89
9. Носитель должен иметь сертификат ФСБ о соответствии требованиям, предъявляемым к средствам электронной подписи и к средствам криптографической защиты информации по классу не ниже КС2.

ВАЖНО!!! В рамках технологии печати КИМ работы с зашифрованными КИМ все носители ЭП должны выпускаться **одним поставщиком**. Т.е. в случае дополнительной закупки носителей они должны приобретаться у того же поставщика, носители которого уже используются. Это связано с тем, что у разных поставщиков используются разные дистрибутивы CSP КриптоПро (версия криптопровайдера при этом одинаковая). Например, рутокен не будет работать на CSP етокена и наоборот.