

**ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ И ПРОГРАММНОМУ
ОБЕСПЕЧЕНИЮ ППЭ ДЛЯ ПРОВЕДЕНИЯ ЕГЭ С ИСПОЛЬЗОВАНИЕМ
ТЕХНОЛОГИИ ПЕЧАТИ КИМ В АУДИТОРИЯХ ППЭ**

Перечень принятых сокращений и терминов

В настоящем документе используются следующие термины и сокращения:

АРМ	Автоматизированное рабочее место
Станция печати КИМ, АРМ печати КИМ	Компьютер с установленным на нем специализированным ПО для печати КИМ и подключенным к нему печатающим устройством (принтером), предназначенный для печати КИМ в аудитории ППЭ
ЕГЭ	Единый государственный экзамен
КИМ	Контрольные измерительные материалы
ПО	Программное обеспечение
ППЭ	Пункт проведения экзамена
ЭП	Электронная подпись

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: Windows XP service pack 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 USB модем используется в случае возникновения проблем с доступом в сеть Интернет по стационарному каналу связи.
Внешний накопитель резервный	1	Резервное устройство резервного копирования: ATAPI CD-RW (внешний) на ППЭ
Токен	по 1 на каждого члена ГЭК	USB-ключ для хранения сертификата члена ГЭК. Детальные требования даны ниже.
АРМ печати КИМ (Станция печати КИМ)	по 1 на каждую аудиторию	К рабочей станции должен быть подключен локальный лазерный принтер (использование сетевого принтера не допускается). Детальные требования к конфигурации приведены в Таблице 2.

Компонент	Количество	Конфигурация
Локальный лазерный принтер	по 1 на каждое АРМ печати КИМ (Станцию печати КИМ)	Формат: А4. Тип печати: черно-белая. Технология печати: Лазерная. Скорость черно-белой печати (обычный режим, А4): 20 стр./мин. Качество черно-белой печати (режим наилучшего качества): не менее 600 x 600 точек на дюйм.
Флэш-носитель	1	Флэш-носитель используется техническим специалистом для переноса закрытого ключа расшифровки КИМ из штаба ППЭ в аудитории.

В ППЭ должны быть подготовлены резервные картриджи для каждого локального лазерного принтера и необходимое количество бумаги формата А4, определяемое из расчета 16 листов на каждого участника (720 листов на 45 участников).

В следующей таблице (см. Таблица 2) приведены детальные требования к АРМ печати КИМ.

Таблица 2

Компонент	Конфигурация
Операционная система	Windows XP service pack 3 / Vista / 7 платформы: ia32 (она же x86), x64.
Дополнительное ПО	Microsoft .NET Framework 4.0 и выше
Центральный процессор	Рекомендуемая: двухъядерный 2,5 ГГц Минимальная: одноядерный 3,0 ГГц
Оперативная память	Рекомендуемая: 2 Gb Минимальная: 1 Gb
Дисковая подсистема	SATA (IDE), свободного места не менее 200 Mb
Внешние интерфейсы и накопители	Устройство резервного копирования: ATAPI CD-RW и Внешний интерфейс: USB 2.0
Видеоадаптер	встроен в чипсет материнской платы, производительность не менее рекомендуемой для установленной ОС
Клавиатура	присутствует
Мышь	присутствует
Монитор	SVGA разрешение не менее 1024px по горизонтали. Рекомендуемое разрешение: 1280x1024
Система бесперебойного питания (рекомендуется)	Выходная мощность, соответствующая потребляемой мощности подключённой рабочей станции. Время работы при полной нагрузке не менее 15 мин.

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:
 - а. генерация ключевых пар ГОСТ Р 34.10-2001,
 - б. формирование электронной подписи по ГОСТ Р 34.10-2001,
 - с. 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.