Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

ПРИКАЗ

Самара

№ 497-ОВ «04» октября 2021 года
По общим вопросам

1. Утвердить Регламент администратора квалифицированной электронной подписи федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет».

2. Утвердить Регламент владельца квалифицированной электронной подписи федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет».

Ректор С.И. Ашмарина

Разработчик: проректор по административной работе Е.А. Кандрашина

Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГАОУ ВО «СГЭУ»
«04» октября 2021г.
№ 497-ОВ

Регламент владельца квалифицированной электронной подписи
федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет»

Введение. Общие понятия и определения.

Квалифицированная электронная подпись, далее (ЭП), информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Используется для работы с конфиденциальной информацией. ЭП является одним из элементов составляющим систему электронного документооборота (ЭДО), как внутри организации, так и с внешними корреспондентами.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ которой ограничивается в соответствии с законодательством Российской Федерации.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром (УЦ) выдан сертификат ключа подписи, и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Пользователь сертификата ключа подписи — физическое лицо, получившее право от владельца сертификата ключа подписи использовать его ЭП.

Проверка ЭП – процесс, в котором на основе имеющегося электронного документа и соответствующей ЭП, а также заданного алгоритма проверки ЭП, определяются корректность, ошибочность (некорректность) или невозможность проверки корректности ЭП.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники с установленным специальным программным обеспечением, осуществляющее криптографическое преобразование информации для обеспечения её безопасности.

Преобразование электронного документа с помощью ключевой информации – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Требования к применению ЭП

Согласно п.1 ст. 6 Федеральным законом от 06.04.2011г. № 63-ФЗ «Об электронной подписи», ЭП признается равнозначной собственноручной подписи в документе на

бумажном носителе при условии, что сертификат ключа подписи, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания.

Согласно п.1 ст.10 63-ФЗ «Об электронной подписи» владельцы ключей электронных подписей обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

Хранение закрытого ключа ЭП

Владелец/пользователь сертификата ключа обязан хранить в тайне закрытый ключ ЭП. Носитель информации, содержащий закрытый ключ ЭП, должен храниться в условиях, исключающих возможность его компрометации. Пользователю передавать закрытый ключ ЭП другому лицу запрещено.

Обращение с носителем информации (Флэш, e-Token), содержащим закрытый ключ ЭП, должно осуществляться в соответствии с эксплуатационной документацией на средства электронной подписи.

Требования по обеспечению информационной безопасности при обращении с ЭП

Не допускается:

- записывать на носитель ключевой информации постороннюю информацию;
- подключать носитель ключевой информации к техническим средствам обработки информации, не предусмотренным штатным режимом эксплуатации;
- пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей);
- размещать ключевую информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи;
- хранить на носителе ключевой информации иную информацию (в том числе рабочие или личные файлы).

Носители ключевой информации должны использоваться только их владельцем/пользователем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования т.к. размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

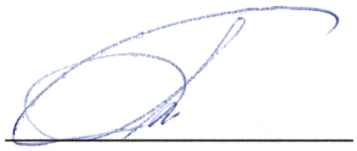
Ответственность за компрометацию или утрату закрытого ключа ЭП возлагается на владельца/пользователя сертификата ключа подписи.

Компрометация ключей

Под компрометацией закрытого ключа электронной подписи (ЭП) понимается его утрата, хищение, разглашение, несанкционированное копирование, увольнение сотрудника, имеющего доступ к закрытому ключу ЭП, любые другие виды разглашения закрытого ключа

ЭП, а также такие случаи, когда нельзя достоверно установить, что произошло с носителем, содержащим закрытый ключ ЭП.

При компрометации (или подозрении на компрометацию) закрытого ключа ЭП владельцу/пользователю необходимо немедленно прекратить использование данного закрытого ключа ЭП, сообщить об инциденте администратору ЭП для передачи сведения в УЦ, выдавший данный закрытый ключ ЭП.

РАЗРАБОТАНО:
Начальник отдела контроля
документационного обеспечения уставной
деятельности университета  С.П. Ткаченко