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 администратора 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 06.04.2011 г. № 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.

Администратор обязан регулярно проверять условия хранения закрытого ключа ЭП.

Требования по обеспечению информационной безопасности при обращении с ЭП

Необходимо:

- ограничить доступ к автоматизированным рабочим местам с АРМ КриптоПРО, которые используются для создания ЭП к электронным документам;
- удалить с рабочих мест где стоит АРМ КриптоПРО программное обеспечение (ПО), не связанное с выполнением служебных обязанностей сотрудников, работающих на этих АРМ КриптоПРО.
- разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании, и т. д.). Использовать фильтры паролей в соответствии со следующими правилами:
    - длина пароля должна быть не менее 6 символов;
    - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
    - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (user, admin, root, и т.д.);
    - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
    - личный пароль владелец/пользователь не имеет права никому сообщать;
    - периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

При использовании ЭП средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

Предусмотреть меры, максимально ограничивающие доступ к:

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

На средствах вычислительной техники необходимо:

- организовать удаление (по окончании сеанса работы средств квалифицированной ЭП) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;
- регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.).
- исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;
- организовать комплекс мероприятий по антивирусной защите и регулярно обновлять антивирусные базы.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной ЭП;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами квалифицированной ЭП без контроля после ввода ключевой информации;
- использовать ключ ЭП и соответствующий сертификат ключа проверки ЭП, на изменение статуса которого, подано заявление в удостоверяющий центр в течение времени, исчисляемого с момента подачи заявления на изменение статуса сертификата

по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса;

- использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки ЭП.

Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной ЭП при их создании должны записываться на предварительно инициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной ЭП согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

Ключи квалифицированной ЭП на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной ЭП.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца/пользователя ключа квалифицированной ЭП.

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