Приложение 5
к Порядку реализации АО «Торговый дом «ПЕРЕКРЕСТОК»
функций аккредитованного удостоверяющего центра
и исполнения его обязанностей, утверждённому
приказом от 26.04.2022 № 3-1-100/000818-22

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.
1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.
1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
1.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено.
1.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
1.10. Обратиться в Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с заявлением о подтверждении подлинности электронной подписи в электронном документе в случае возникновения конфликтной ситуации.

2. Порядок применения средств квалифицированной электронной подписи

2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.
2.2. При эксплуатации средств квалифицированной электронной подписи должны использоваться только квалифицированной сертификаты ключей проверки электронной подписи, выпущенные аккредитованным Удостоверяющим центром.

2.3. Средства квалифицированной электронной подписи должны использоваться с сертифицированными средствами антивирусной защиты.
2.4. Инсталляция средств квалифицированной электронной подписи на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
2.5. При установке и использовании средств квалифицированной электронной подписи должна быть обеспечена защита аппаратного и программного обеспечения от несанкционированного доступа в соответствии с Руководством администратора безопасности из состава эксплуатационной документации на средство квалифицированной электронной подписи.
2.6. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства вычислительной техники с установленным средствами квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, средства вычислительной техники, на которых эксплуатируется средства квалифицированной электронной подписи, и защищаемую информацию.
2.7. На средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, должно использоваться только лицензионное программное обеспечение фирм - изготовителей и не должны устанавливаться средства разработки программного обеспечения и отладчики.
2.8. Программное обеспечение, устанавливаемое на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- не санкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

2.9. Для идентификации пользователя при входе в операционную систему и BIOS на технических средствах, предназначенных для работы со средствами квалифицированной электронной подписи, необходимо использовать 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 и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля не должна превышать 6 месяцев.

2.10. Средствами BIOS должна быть исключена возможность работы на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, если во время начальной загрузки не проходят встроенные тесты.
2.11. ЗАПРЕЩАЕТСЯ:

- оставлять без контроля средства вычислительной техники, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств электронной подписи;
- осуществлять копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- изменять настройки, установленные программой установки средства электронной подписи или администратором;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами квалифицированной электронной подписи.

3. Правила использования ключевых носителей

3.1. Хранить ключ квалифицированной электронной подписи необходимо исключительно на защищенном ключевом носителе.
3.2. На ключевой носитель должен быть установлен индивидуальный PIN-код доступа (отличный от установленного по умолчанию).
3.3. Владелец ключа квалифицированной электронной подписи обязан обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц (хранить и использовать носитель таким образом, чтобы исключался несанкционированный доступ к нему других лиц) и сохранять в конфиденциальности PIN-код доступа. Владелец ключа несет персональную ответственность за хранение личных ключевых носителей.
3.4. В случае утери ключевого носителя или наличия оснований подозревать о получении к нему несанкционированного доступа сторонних лиц владелец ключа электронной подписи обязан обратиться в Удостоверяющий центр с заявлением о прекращении действия сертификатов ключей проверки электронной подписи, ключи электронной подписи которых хранятся на носителе.