ПРАВИЛА

хранения закрытого ключа электронной цифровой подписи и обеспечения его безопасности

Целью данного документа является предоставление Владельцам ЭЦП рекомендаций, при точном и неукоснительном выполнении которых достигается необходимый и достаточный уровень безопасного применения технологии электронной цифровой подписи (ЭЦП).

Сохранение в тайне закрытого ключа ЭЦП – это основа безопасной технологии применения ЭЦП. Без владения закрытым ключом ЭЦП , в том числе без знания пароля закрытого ключа ЭЦП постороннее лицо не сможет сформировать электронную цифровую подпись за владельца закрытого ключа ЭЦП (Владельца ЭЦП).

Вследствие этого, Владелец ЭЦП должен соблюдать следующие основные правила хранения закрытого ключа ЭЦП и обеспечивать его безопасность:

• ни при каких условиях не передавать другим лицам отчуждаемый носитель информации, содержащий закрытый ключ ЭЦП

• принимать все возможные меры к обеспечению конфиденциальности информации о пароле закрытого ключа ЭЦП;

• принимать все возможные меры для предотвращения потери, раскрытия, модифицирования и несанкционированного использования закрытого ключа;

• не использовать закрытый ключ ЭЦП, если известно, что этот ключ используется или использовался ранее другими лицами;

• хранить отчуждаемый носитель информации с ключами ЭЦП в несгораемом сейфе или ином хранилище, обеспечивающем сохранность отчуждаемого носителя данных;

• при транспортировке отчуждаемого носителя данных создавать условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на отчуждаемый носитель данных и записанный закрытый ключ ЭЦП.

Компрометации закрытого ключа ЭЦП – это:

• утрата отчуждаемого носителя данных содержащего закрытый ключ ЭЦП;
• раскрытие третьим лицам, либо несанкционированное получение третьими лицами информации о пароле закрытого ключа ЭЦП;
• утрата отчуждаемого носителя данных содержащего закрытый ключ ЭЦП с последующим обнаружением;
• увольнение сотрудников, имевших доступ к отчуждаемому носителю данных содержащему закрытый ключ ЭЦП и к информации о пароле закрытого ключа ЭЦП;
• нарушение правил хранения отчуждаемого носителя данных содержащего закрытый ключ ЭЦП;
• возникновение подозрений на утечку информации или ее искажение в системе электронного документооборота;

• нарушение печати на сейфе или повреждение иного хранилища, в котором находился отчуждаемый носитель данных содержащий закрытый ключ ЭЦП;
• несанкционированное копирование и другие происшествия, в результате которых закрытый ключ ЭЦП мог стать доступным несанкционированным лицам и (или) процессам.

Действия Владельца ЭЦП в случае компрометации закрытого ключа ЭЦП

• самостоятельное определение факта компрометации закрытого ключа ЭЦП и оценка значения этого события для Владельца ЭЦП;
• организация и осуществление мероприятий по розыску и локализации последствий компрометации закрытого ключа ЭЦП;
• немедленно прекращение использования скомпрометированного закрытого ключа ЭЦП;
• немедленное информирование Центра регистрации о нарушении или возможном нарушении режима доступа к закрытому ключу ЭЦП для временной блокировки сертификата ключа ЭЦП путем направления заявки на блокировку с использованием сервиса сайта Центра регистрации;
• в течение одного рабочего дня направление в Центр регистрации заявления на приостановление действия сертификата ключа ЭЦП или его аннулирование, заверенное собственноручной подписью Владельца ЭЦП. Если Владелец ЭЦП является представителем юридического лица на имя которого выдан сертификат ключа ЭЦП соответствующего скомпрометированного закрытого ключа ЭЦП заявление на приостановление действия сертификата ключа ЭЦП или его аннулирование должно быть подписано руководителем данного юридического лица и скреплено печатью.

Формы заявлений на приостановление действия и аннулирование сертификата ключа ЭЦП устанавливаются Центром регистрации. Все поля заявлений должны быть заполнены достоверной информацией.

Действия Владельца ЭЦП при аннулировании сертификата ключа ЭЦП или нарушении режима конфиденциальности пароля закрытого ключа ЭЦП

• самостоятельное уничтожение, без возможности восстановления, файла с соответствующим закрытым ключом ЭЦП.

Уничтожение файла с закрытым ключом ЭЦП без возможности восстановления выполняется путем полного форматирования отчуждаемого носителя данных.