КРИПТОТЕЛЕКОМ
(4822) 509-509
(4822) 509-000
ЮР. АДРЕС: 170019, Г. ТВЕРЬ, УЛ. 2-Я СЕРОВА, Д.12
ПОЧТ. И ФАКТ. АДРЕС: 170026, Г. ТВЕРЬ, ПР-Т КОМСОМОЛЬСКИЙ, Д. 11, КОРП.1
cryptotelecom.ru

РУКОВОДСТВО

по обеспечению безопасности использования электронной подписи и средств электронной подписи

Использование электронных подписей сопровождается рисками финансовых потерь при несанкционированном получении злоумышленниками ключей электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка электронной подписи. В целях минимизации рисков необходимо принять меры по обеспечению безопасности использования электронных подписей. Настоящее руководство предназначено для обязательного ознакомления владельцу сертификата ЭП и сотруднику организации, ответственному за информационную безопасность.

Порядок действий пользователя

Пользователи Удостоверяющего центра получают средства криптографической защиты информации (далее – СКЗИ), сертифицированные в порядке, установленном законодательством Российской Федерации.

Владелец сертификата ключа проверки электронной подписи обязан:

- Не использовать для электронной подписи и шифрования ключи, если ему известно, что эти ключи уже используются или использовались ранее.
- Хранить в тайне закрытый ключ.
- Немедленно требовать приостановления действия сертификата ключа при наличии оснований полагать, что тайна закрытого ключа нарушена (компрометация ключа).
- Обновлять (перевыпускать) ключ и сертификат ключа проверки подписи в соответствии с установленным регламентом.

Рекомендуется:

- Установка и настройка СКЗИ на рабочем месте должна выполняться в присутствии администратора.
- Перед установкой необходимо проверить целостность программного обеспечения СКЗИ.
- Запрещается устанавливать СКЗИ, целостность которого нарушена.

Компрометация ключа

Компрометация ключа – это утрата доверия к тому, что используемый ключ обеспечивает безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имеющих доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение печати на сейфе с ключевыми носителями.
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Рекомендуемые меры по обеспечению информационной безопасности в организации

- Администрирование компьютера должно осуществляться доверенными лицами.
- ПЭВМ, на которых используется СКЗИ, должны соответствовать требованиям по защите информации в соответствии с эксплуатационной документацией на СКЗИ.
- На рабочих местах, предназначенных для работы с СКЗИ, должно использоваться только лицензионное программное обеспечение, установлены сертифицированные ФСБ России средства антивирусной защиты, внедрена политика назначения и смены паролей.
- Системные блоки ПЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия
- Хранение ключевых носителей осуществляется в запираемых шкафах (хранилищах, сейфах) индивидуального пользования.
- В случае увольнения или перевода в другое подразделение сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей, к которым он имел доступ.
- **НЕ допускается**:
  - ✓ Делать несанкционированные копии с ключевых носителей.
  - ✓ Знакомить с содержанием или передавать ключевые носители лицам, к ним не допущенным.
  - ✓ Выводить секретные ключи на принтер
  - ✓ Устанавливать ключевой носитель в ПЭВМ, не предназначенные для работы с СКЗИ.
  - ✓ Записывать на ключевой носитель постороннюю информацию
  - ✓ Оставлять без контроля ПЭВМ, на которых эксплуатируется СКЗИ, после ввода ключевой информации.
  - ✓ Хранить пароли в виде записей на бумажных носителях, находящихся в общедоступных местах или в незащищенных файлах компьютера.

Нормативные ссылки

1. Федеральный закон РФ от 06.04.2011 №63-ФЗ «Об электронной подписи».
2. Закон РФ "Об информации, информационных технологиях и о защите информации", 27.07.2006 №149-ФЗ.
3. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005), утвержденное приказом ФСБ России от 09.02.2005 № 66.
4. Инструкция об организации и обеспечении безопасности хранения обработки и передачи по каналам связи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом ФАПСИ от 13.06.2001 №152.
5. Эксплуатационная документация на СКЗИ Крипто Про CSP.