

Руководство по обеспечению безопасности при работе с ключами электронной подписи

1. Рекомендации к доверенной среде

- 1.1. На компьютере, с которого производится работа, должно быть установлено только лицензионное программное обеспечение. Установленное программное обеспечение должно регулярно обновляться.
- 1.2. Должна быть установлена система антивирусной защиты с регулярными обновлениями. Все съемные носители, а также все загружаемые из сетей файлы и программы должны проверяться на наличие вирусов.
- 1.3. Запрещается использовать функцию «автоматического выполнения» для съемных носителей и компакт дисков.
- 1.4. По возможности необходимо использовать программные средства фильтрации трафика, ограничение IP-диапазона, блокировки сетевых атак.
- 1.5. Запрещается производить работы в системе с общедоступных компьютеров, например, из интернет-кафе.

2. Рекомендации к идентификации и аутентификации

- 2.1. Для работы с ключами электронной подписи должна быть предусмотрена отдельная учетная запись с правами пользователя.
- 2.2. Идентификация и аутентификация пользователя в системе производится с помощью логина-пароля. Пароли всех пользователей системы должны быть уникальными, также не допускается установка одинаковых паролей на учетную запись и на вход в систему.
- 2.3. Для формирования паролей можно использовать следующие типы знаков:
 - Прописные русские буквы (А.Б.В...);
 - Строчные русские буквы (а, б, в...)
 - Прописные латинские буквы (А, В, С...);
 - Строчные латинские буквы (а, b, с...);
 - Цифры (0, 1, 2...);
 - Знаки, не являющиеся буквами или цифрами (@, &, \$...);
 - Знаки из кодировки Юникод (€, f, ?...).
- 2.4. Пароли, устанавливаемые в системе, должны быть длиной не менее 10 символов и составлять с помощью минимум 3 типов знаков.
- 2.5. В качестве пароля не рекомендуется устанавливать:
 - фамилию (имя или отчество) пользователя, а также его логин;
 - комбинацию символов, которая радикальным образом не отличается от предыдущих паролей, в том числе создается путем приращения;
 - отдельные слова русского или английского языка, жаргонные термины или иные удобные для подбора элементы;
 - отдельные слова русского языка, набираемые в латинском регистре или отдельные слова английского языка, набираемые в русском регистре;
 - общепринятые сокращения или их сочетания (ЭВМ, ЛВС, USSR и т. д.);
 - персональные сведения - номера телефонов, дни рождений, номер документа, удостоверяющего личность и т.п.;
 - только цифровые символы.
- 2.6. Плановая смена паролей должна проводиться не реже, чем раз в 90 дней. Внеплановая смена паролей производится в случае нарушения правил обращения с паролями, при смене ключей электронной подписи, при увольнении ответственного работника.
- 2.7. Пользователю запрещается:
 - несанкционированно сообщать кому-либо (разглашать) свой пароль;

- оставлять свой пароль на бумажном носителе в любом месте, кроме сейфа или шкафа с замком;
- выводить пароль в открытом виде на принтер, дисплей и другие внешние устройства отображения информации;
- записывать куда-либо свой пароль кроме случаев, предусмотренной служебной необходимостью;
- предоставлять доступ в систему другим лицам по своему идентификатору и паролю;
- использовать программную опцию сохранения пароля в памяти системы.

3. Рекомендации при работе с ключевым носителем

- 3.1. Ключи электронной подписи должны, по возможности, храниться на специализированных защищенных носителях (например, eToken - персональное средство аутентификации, обеспечивающее защиту ключа электронной подписи от его компрометации. Обладают следующими характеристиками: включают в себя аппаратную реализацию криптоалгоритмов и защищенную память, невозможность напрямую из операционной системы получить доступ к памяти носителя, копирование ключей электронной подписи возможно только с помощью специального программного обеспечения (AdminPKI), при использовании eToken ГОСТ их вообще невозможно скопировать официальными методами).
- 3.2. Использование обычных flash-накопителей не обеспечивает защиту ключей электронной подписи от копирования, поэтому использование незащищенных flash-накопителей несет в себе увеличение риска компрометации ключа электронной подписи. В случае если необходимость использования незащищенных flash-накопителей возникла, необходимо обеспечить контроль доступа к таким носителям, не оставлять их без присмотра, хранение носителя осуществлять в сейфе или запираемом шкафу.
- 3.3. Необходимо воздерживаться от копирования ключей электронной подписи с ключевого носителя в память компьютера и хранения ключей в реестре, а в случае возникновения такой необходимости использовать компьютер с контролем доступа к нему, с соблюдением рекомендаций к идентификации и аутентификации, а также принятием иных необходимых мер по предотвращению компрометации ключей электронной подписи.
- 3.4. Пользователь системы должен осуществлять вход только с помощью собственной электронной подписи. Во время работы носитель с электронной подписью подключается к компьютеру, после работы в системе необходимо закрыть программу, отключить носитель, убрать его в сейф, если имеется, или в запираемый шкаф. Не разрешается оставлять носители включенными или просто лежащими на рабочем месте во время отсутствия пользователя.
- 3.5. При длительном плановом неиспользовании системы, для организаций при отпуске ответственных работников необходимо произвести приостановление действия ключа электронной подписи.
- 3.6. В случае компрометации ключей электронной подписи, утери или кражи ключевого носителя необходимо незамедлительно сообщить об этом в Удостоверяющий центр электронным письмом по адресу: ca@veles-capital.ru и (или) телефону 8(495)258-19-88 доб.(591) и прекратить действие сертификата ключа проверки электронной подписи.

4. Рекомендации при выборе способа создания ключей электронной подписи

В целях недопустимости компрометации ключей электронной подписи еще на стадии их создания необходимо обратить внимание на соблюдение рекомендаций к доверенной среде, рекомендаций к идентификации и аутентификации и, по возможности, создавать ключи электронной подписи силами Удостоверяющего центра.

Создание ключей электронной подписи в Удостоверяющем центре осуществляется с использованием опечатанной и аттестованной ЭВМ (аттестат выдан 04.02.2011 ООО «ЛИССИ», лицензия ФСТЭК России № 001711 от 29 октября 2009).

У ЭВМ отсутствует доступ к сетям общего пользования, установлено антивирусное программное обеспечение, оснащена программно-аппаратным комплексом (ПАК) «Соболь» 3.0.

ПАК «Соболь 3.0» имеет сертификаты ФСБ России № СФ/027-1450 от 01.04.2010 и ФСТЭК РФ № 1967 от 07.12.2009 и реализует следующие основные функции:

- идентификация и аутентификация пользователей компьютера при их входе в систему с помощью персональных электронных идентификаторов iButton;
- защита от несанкционированной загрузки операционной системы со съемных носителей – дискет, оптических дисков, ZIP-устройств, магнитных дисков, USB-устройств и др.;
- контроль целостности файлов и физических секторов жесткого диска до загрузки операционной системы;
- контроль работоспособности основных компонентов комплекса – датчика случайных чисел, энергонезависимой памяти, персональных электронных идентификаторов;
- регистрация событий, имеющих отношение к безопасности системы;
- позволяет генерировать закрытые ключи с помощью аппаратного датчика случайных чисел, что позволяет в отличие от программного генератора случайных чисел (его еще называют генератор псевдослучайных чисел) создает действительно случайные числа для формирования надежных ключей шифрования и электронной цифровой подписи.