

**Средство криптографической
защиты информации «MS_KEY K» –
«АНГАРА» (вариант исполнения 8.1.1)**

Руководство пользователя

Версия 1.1

Содержание

Предисловие	3
Общие сведения	4
Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе	6
Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1	7
Эксплуатация и хранение	7
Использование USB-токенов при регистрации в системе «iBank 2»	7
Использование USB-токенов при входе в систему	10
Администрирование USB-токенов	11

Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «MS_KEY К» – «АНГАРА» (вариант исполнения 8.1.1) (далее «MS_KEY К» – «АНГАРА» Исп 8.1.1, USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1) в системе «iBank 2».

В разделе [Общие сведения](#) подробно рассмотрено назначение USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1.

В разделе [Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе](#) представлена информация о совместимости изделия с различными операционными системами и действиях, необходимых для обеспечения корректной работы устройства.

В разделе [Эксплуатация и хранение](#) описаны меры по обеспечению сохранности и надежности «MS_KEY К» – «АНГАРА» Исп 8.1.1.

Применение изделия при работе с системой «iBank 2» подробно рассмотрено в разделах:

- [Использование USB-токенов при регистрации в системе «iBank 2»](#)
- [Использование USB-токенов при входе в систему корпоративных клиентов](#)
- [Администрирование USB-токенов](#)

Общие сведения

USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1 представляет собой компактное USB-устройство (см. [рис. 1](#)) с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. Разработчиком устройства является компания ООО «НТЦ Альфа-Проект».



Рис. 1. USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1

USB-токены «MS_KEY К» – «АНГАРА» Исп.8.1.1 генерируют ключи ЭП внутри себя, обеспечивают их защищенное неизвлекаемое хранение и формируют ЭП под электронными документами внутри устройства.

Аппаратная реализация стандарта ЭП, шифрования и хеширования внутри устройства обеспечивает:

- конфиденциальность обрабатываемой информации при передаче и хранении;
- целостность обрабатываемой информации;
- подтверждение авторства посредством электронной подписи.

Формирование ЭП в соответствии с ГОСТ Р34.10-2012 происходит непосредственно внутри устройства: на вход «MS_KEY К» – «АНГАРА» Исп.8.1.1 принимает электронный документ, на выходе выдает ЭП под данным документом.

В «MS_KEY К» – «АНГАРА» Исп.8.1.1 имеется защищенная область памяти, позволяющая хранить до 75 ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка «MS_KEY К» – «АНГАРА» Исп.8.1.1 обеспечена в системе «iBank 2», начиная с версии 2.0.24.492

Использование «MS_KEY К» – «АНГАРА» Исп.8.1.1 возможно в следующих АРМ:

- Internet-Банкинг для корпоративных клиентов (Web);
- ЦФК (Web);
- РС-Банкинг;
- Корпоративный автоклиент;
- Internet-Банкинг для частных клиентов;
- Администратор банка/филиала;
- Операционист корпоративных клиентов;
- Операционист частных клиентов;
- Система управления контентом Internet-Банкинга (CMS);
- Контроль SIM-карт клиентов;
- Оператор сервиса «Чат».

Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

Примечание:

Иллюстрации в документе приведены для стандартных версий Web-АРМов системы «iBank 2».

В «MS_KEY К» – «АНГАРА» Исп 8.1.1 реализованы следующие криптографические функции:

- ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-2012 (функция хеширования);
- ГОСТ 28147-89 (симметричное шифрование);
- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры и режимы работы блочных шифров);
- аппаратный криптографически стойкий генератор случайных чисел.

Средство криптографической защиты информации (СКЗИ) «MS_KEY К» – «АНГАРА» (вариант исполнения 8.1.1) сертифицировано сертификатом ФСБ РФ № СФ/124-3072 от 20.02.2017 – действителен до 20.02.2020.

Примечание:

В системе «iBank 2» поддерживается работа USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов ООО «НТЦ Альфа-Проект», встроила поддержку конфигурации в систему «iBank 2», протестировала систему «iBank 2» на предмет совместимости с USB-токенами «MS_KEY К» – «АНГАРА» Исп 8.1.1 в данной конфигурации и осуществляет их поддержку в системе «iBank 2» только в специальной конфигурации.

В настоящее время в системе «iBank 2» реализована поддержка USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрети» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank 2».

Использование USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank 2».

Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе

Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1 возможна на следующих платформах:

- Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
- Apple Mac OS X: 10.7.3 (Lion) и выше;
- Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.

«MS_KEY К» – «АНГАРА» Исп 8.1.1 поддерживает CCID-драйвер, который входит в состав современных ОС Microsoft Windows, Linux, Mac OS X, и не требует установки дополнительного программного обеспечения.

Для работы «MS_KEY К» – «АНГАРА» Исп 8.1.1 в WEB-версиях АРМ системы «iBank 2» необходим плагин **BIFIT Signer** версии 5.0 и выше.

Для работы «MS_KEY К» – «АНГАРА» Исп 8.1.1 в java-апплетах системы «iBank 2» необходимо дополнительно установить библиотеку **pkcs11-angara**.

Для получения библиотеки для используемой ОС обратитесь в ваш банк.

Разрядность используемой Java и библиотеки **pkcs11-angara** должны совпадать.

Разместите файл библиотеки в среде пользовательской ОС:

Для ОС Windows:

Файл библиотеки соответствующей разрядности (**pkcs11-angara.dll**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: **C:\Windows\System32**.

Для ос Linux:

Файл библиотеки соответствующей разрядности (**libpkcs11-angara.so**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: **/usr/lib**.

Для MAC OS X:

Файл библиотеки соответствующей разрядности (**libpkcs11-angara.dylib**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек подключенного устройства, например: **/Users/имя_пользователя/Library/Java/Extensions/** (если его нет, необходимо создать каталог **/Java/Extensions/**).

Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1

Эксплуатация и хранение

USB-токены являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов, а также сохранность конфиденциальной информации пользователя.

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- USB-токены необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать устройства от попадания на них прямых солнечных лучей.
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении USB-токена компьютеру не прилагайте излишних усилий.
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи, влаги и т.п. При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.
- Не допускается непрерывное функционирование USB-токена более суток (24 часов).
- Не разбирайте USB-токены, так как это ведет к потере гарантии!
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать USB-токен из USB-порта во время записи и считывания.
- В случае неисправности или неправильного функционирования USB-токенов обращайтесь в ваш банк.

Внимание!

1. Не передавайте USB-токены третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
2. Подключайте USB-токен к компьютеру только на время работы с системой «iBank 2».
3. В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с вашим банком.

Использование USB-токенов при регистрации в системе «iBank 2»

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «**Регистратор для корпоративных клиентов**», банковских сотрудников — в АРМ «**Регистратор для банковских сотрудников**»:

1. Подключитесь к Интернету, запустите Web-браузер и перейдите на страницу входа для клиентов или для сотрудников банка системы «iBank 2» вашего банка.
2. На странице входа клиентов выберите пункт: **Новый клиент**, на странице входа сотрудников банка — **Регистрация** или **Новый сотрудник**.

В результате загрузится соответствующий АРМ.

3. Подключите USB-токен «MS_KEY К» – «АНГАРА» Исп 8.1.1 к USB-порту компьютера.

4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на третьем шаге (банковский сотрудник) в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. [рис. 2](#), [рис. 3](#)).

The screenshot shows the iBank 2 registration interface for a corporate client. The title is "Регистрация нового клиента" and the step is "Шаг 8 из 12". The text explains that a new EP key must be added to a key storage, and that one storage can contain multiple keys. It asks for the full path to the file or the serial number of the hardware device used for key generation. A note states that if the storage does not exist, it will be created. There is a dropdown menu labeled "Аппаратное устройство" with a selected option: "MS_Key К" - "АНГАРА" Исп.8.1.1 (001524). A blue "Выбрать..." button is next to it. At the bottom, there are "Назад" and "Вперед" buttons.

Рис. 2. АРМ «Регистратор для корпоративных клиентов (Web)». Предварительная регистрация. Шаг 8 из 12

The screenshot shows the iBank 2 registration interface for a bank employee. The title is "Регистрация нового сотрудника" and the step is "Шаг 3 из 7". The text explains that a new EP key must be added to a key storage, and that one storage can contain multiple keys. It asks for the full path to the file or the serial number of the hardware device used for key generation. A note states that if the storage does not exist, it will be created. There is a dropdown menu labeled "Аппаратное устройство" with a selected option: "MS_Key К" - "АНГАРА" Исп.8.1.1 (001524). A blue "Выбрать..." button is next to it. At the bottom, there are "Назад" and "Вперед" buttons.

Рис. 3. АРМ «Регистратор для банковских сотрудников (Web)». Предварительная регистрация. Шаг 3 из 7

5. Если к «MS_KEY К» – «АНГАРА» Исп 8.1.1 задан PIN-код, то появится окно для ввода PIN-кода (см. [рис. 4](#)). Укажите значение PIN-кода пользователя.

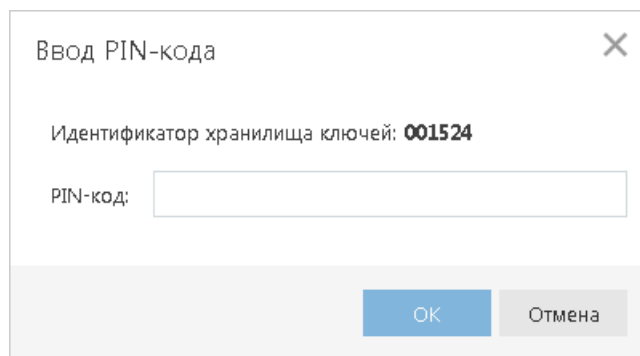


Рис. 4. Ввод Pin-кода пользователя

Внимание!

После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется.

На следующих шагах регистрации вам необходимо ввести наименование и пароль к создаваемому ключу ЭП. Для повышения уровня безопасности пароля воспользуйтесь следующими рекомендациями:

- пароль не должен состоять из одних цифр;
- пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
- пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
- пароль не должен быть значимым словом (ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Если при вводе наименования ключа в хранилище ключей уже существует ключ с таким наименованием, то в этом случае перезаписи ключа не произойдет, о чем будет выдано соответствующее предупреждение (см. рис. 5). В этом случае необходимо либо присвоить другое наименование ключу, либо предварительно удалить ненужный ключ из хранилища (см. раздел [Администрирование USB-токенов](#)).

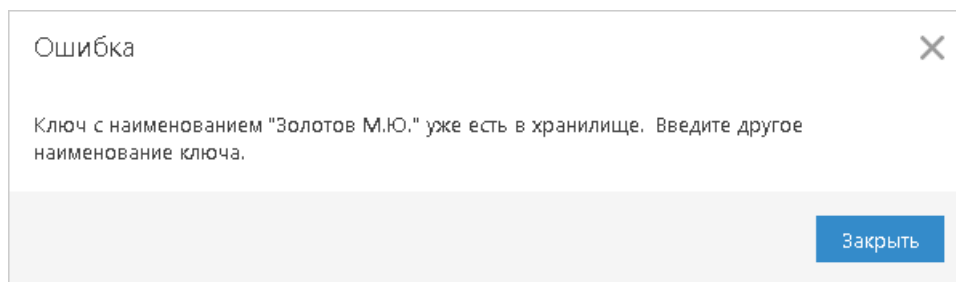


Рис. 5. Сообщение об ошибке

Примечание:

В памяти USB-токена «MS_KEY К» – «АНГАРА» Исп 8.1.1 может храниться не более 75 ключей ЭП, включая удаленные. Предупреждение о переполнении памяти токена выдается при создании последнего возможного ключа. При исчерпании памяти токена необходимо обратиться в банк для повторной инициализации токена. При этом все существующие на токене ключи ЭП будут удалены.

Внимание!

Неправильно ввести пароль к ключу ЭП, который находится на USB-токене «MS_KEY К» – «АНГАРА» Исп 8.1.1, можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Использование USB-токенов при входе в систему

Для загрузки поддерживаемых АРМ (список поддерживаемых АРМ см. в разделе [Общие сведения](#)) подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank 2» вашего банка.

Подключите USB-токен «MS_KEY К» – «АНГАРА» Исп 8.1.1 к USB-порту компьютера.

На странице входа корпоративных клиентов банка выберите необходимый пункт:

- Интернет-Банкинг;
- Центр финансового контроля;
- Запустите приложение РС-Банкинг и выполните синхронизацию.

Или на странице входа банковских сотрудников выберите необходимый пункт:

- Операционист;
- Администратор;
- Система управления контентом;
- Контроль SIM-карт клиентов.

Первое окно АРМ **Вход в систему**, предназначенное для аутентификации пользователя, представлено на [рис. 6](#).

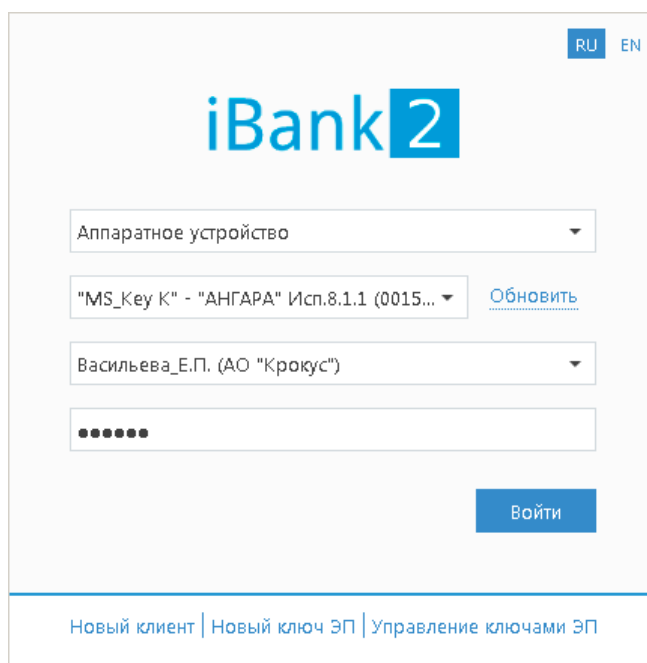


Рис. 6. Окно «Вход в систему. Аутентификация в iBank 2»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена.
- При использовании USB-токена, к которому задан PIN-код, после выбора устройства на предыдущем шаге появляется окно для ввода PIN-кода (см. [рис. 7](#)).

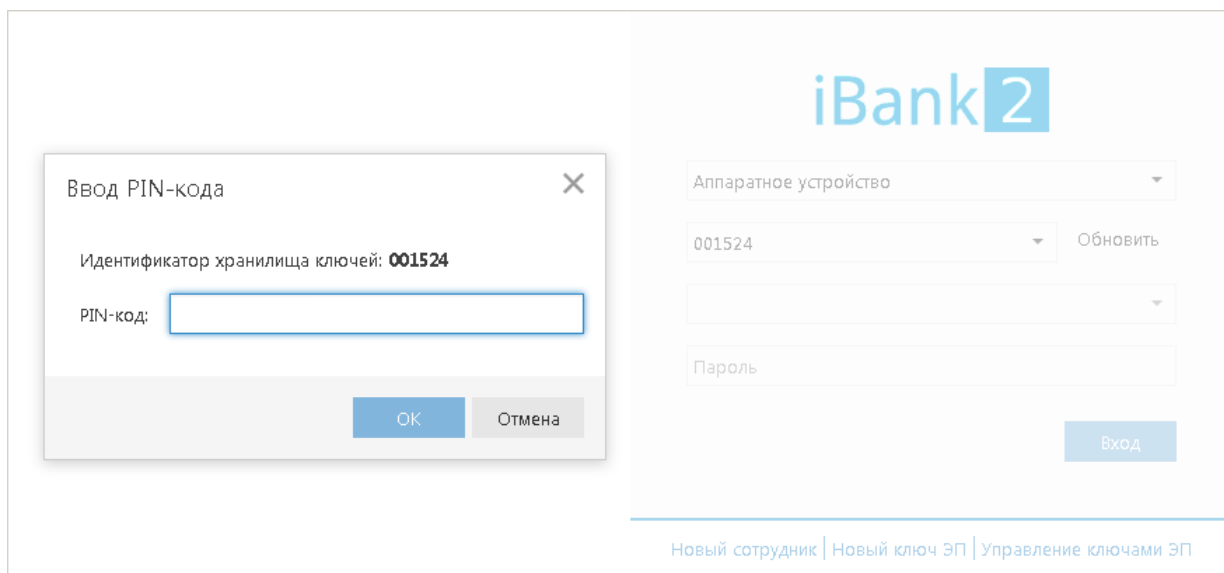


Рис. 7. Окно «Вход в систему. Ввод PIN-кода»

- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Для входа в систему нажмите кнопку **Вход**.

Администрирование USB-токенов

Возможны следующие действия с «MS_KEY К» – «АНГАРА» Исп 8.1.1 и ключами ЭП:

1. [Задание PIN-кода доступа](#)
2. [Печать сертификата ключа проверки ЭП](#)
3. [Смена пароля для доступа к ключу ЭП](#)
4. [Смена наименования ключа ЭП](#)
5. [Удаление ключа ЭП](#)

Корпоративные клиенты выполняют администрирование ключей в следующих разделах:

- Регистратор для корпоративных клиентов (Web) — пункт **Управление ключами ЭП**. Регистратор доступен на странице входа (см. [рис. 6](#)).
- РС-Банкинг — в разделе **Ключи ЭП/Администрирование ключей ЭП**.

Банковские сотрудники выполняют администрирование ключей в разделе **Управление ключами ЭП**.

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле ниже отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. [рис. 8](#)).

iBank 2

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

"MS_Key К" - "АНГАРА" Исп.8.1.1 (001524) Выбрать

Наименование ключа
Admin_1
Васильева_Е.П. (АО "Крокус")
Test_java_applet
Супер_опер
Семенов_тестовый_ключ
Admin

Количество ключей на аппаратном устройстве: 6

Сменить PIN Печать Сменить пароль Переименовать Удалить

Рис. 8. Администрирование ключей ЭП

- Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку.

Задание PIN-кода доступа

Примечание:

Задание и смена PIN-кода доступа осуществляется только в WEB-АРМах системы «iBank 2».

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти «MS_KEY К» – «АНГАРА» Исп 8.1.1, реализована возможность задавать PIN-код доступа к устройству.

При обращении к «MS_KEY К» – «АНГАРА» Исп 8.1.1 с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «MS_KEY К» – «АНГАРА» Исп 8.1.1, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в клиентском АРМ;
- обращение к «MS_KEY К» – «АНГАРА» Исп 8.1.1 в случае его отключения и последующего подключения;
- обращение к «MS_KEY К» – «АНГАРА» Исп 8.1.1 в ходе администрирования ключей ЭП;
- подпись документов и синхронизация данных с банком во время работы в РС-Банкинге.

Для назначения PIN-кода нажмите кнопку **Сменить PIN**, дважды введите новое значение PIN-кода и нажмите кнопку **Принять**.

Назначенный PIN-код к «MS_KEY К» – «АНГАРА» Исп 8.1.1 удалить нельзя, его можно лишь сменить.

Внимание!

После 10 последовательных попыток ввода неверного PIN-кода устройство блокируется.

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять**.

Смена пароля для доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль ключа ЭП и дважды — новый пароль. Нажмите кнопку **Принять**. Новый пароль к ключу ЭП будет установлен.

Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать**. Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП в хранилище ключей. Нажмите кнопку **Принять**. Новое наименование ключа ЭП в хранилище будет установлено.

Удаление ключа ЭП

Внимание!

Если ключ ЭП удалить из хранилища ключей, восстановить его будет невозможно. Поэтому удалять можно ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т.д.).

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Удалить**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.