ЧФ «Энигма-Софт»
61072, Украина, г. Харьков, ул. 23 Августа 38, к. 23.
http://enigmasoft.com.ua, office@enigmasoft.com.ua
+380-577-177-977, (+380-577- 590-723,+380-577-590-724)

Комплекс «СТИЛЬ» - Клиент-Банк

Защищенные носители ключевой информации

Система защиты x.509

Харьков

Содержание

1 Введение

Общие положения

Данный документ предназначен для пользователей «Стиль» Клиент-Банк, работающего под системой защиты x.509 ИИТ.

Документ служит для клиентов вспомогательным материалом, при выборе оптимального носителя ключевой информации.

Описание соответствует версии Клиент-Банка «Стиль» v.4.41.004 или выше, работающего под управлением ОС Windows XP sp3 или выше.

1.1 Особенности работы под Windows XP

Работа с Windows XP ведется аналогично работе на Windows 7, и других ОС, для (см. Раздел 2).

Примечание: при возникновении проблем с работой носителей электронных ключей, необходимо убедится, что в системе присутствует драйвер **«Устройство чтения смарт-карт» (Usbccid.sys)**. В случае его отсутствия, необходимо установить компонент, с помощью сервера обновлений Microsoft (windowsupdate.microsoft.com).

Работа на Windows XP под виртуальной машиной (VMware)

Подтверждена работа всех ключей, кроме Aladdin JaCarta (могут возникнуть проблемы при инсталляции сопутствующих библиотек и утилит).

2 Защищенные носители ключевой информации

2.1 Работа с электронным ключом «Автор»

Внешний вид ключа представлен на Рис.1

Рисунок 1.Ключ Avtor secure token 337.

Предварительная настройка

ОС при подключении устройства в USB-порт определяет устройство и устанавливает необходимые драйвера автоматически.

PIN-код устройства

Для любых операций с устройством, необходимо знать его PIN-код.

Предустановленный: *«12345678»*.

В системе «Стиль»-Клиент Банк пароль доступа к личному ключу должностного лица и PIN-код совпадают.

При генерации ключа на устройство обязательно вводится пароль ключа, равный значению PIN-кода устройства.

Следующим шагом пароль ключа и PIN-код устройства изменяются, функцией смены пароля в системе защиты комплекса «Стиль» - Клиент Банк.

В случае утери PIN-кода устройства, начальные настройки устройства восстанавливаются с помощью специальных утилит, предоставляемых производителем по запросу.

Работа с устройством

Для указания устройства в комплексе «Стиль» - Клиент банк необходимо:

- Подключить устройство к USB-порту;
- Выбрать тип носителя - **«smart-карта»**;
- Выбрать в списке устройство, отображаемое как «**е.ключ чи смарт-карта Автор (PKCS#11) - «Код носителя»»** (См. Рис.2)

Внимание! Работа с устройством, отображаемым как **«smart карта Техноконс. TEllipse - Avtor Secure Token 0»** запрещена.

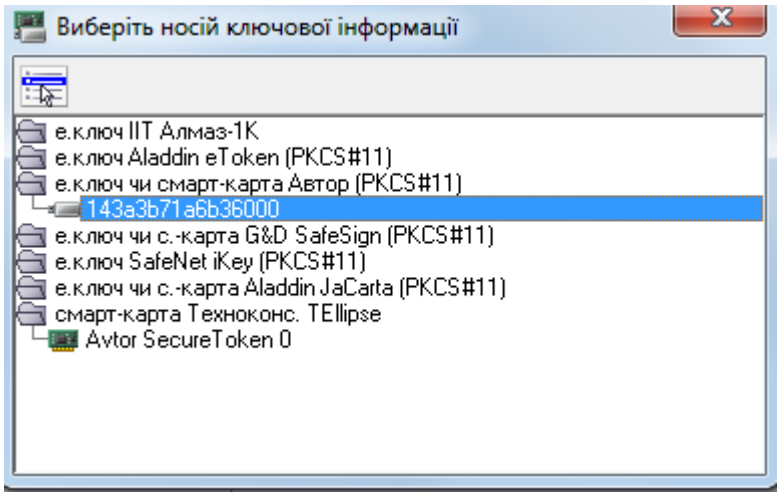

Рисунок 2.Выбор носителя ключевой информации.

Функции управления ключами

Доступны следующие функции управления ключом на устройстве:

- просмотр контекста ключа;
- смена пароля ключа;
- удаление ключа с носителя;

Запрещены следующие функции управления ключом на устройстве:

- Резервное копирование ключа с носителя;
- Резервное копирование ключа на носитель;

2.2 Работа с электронным ключом «Алмаз 1К»

Внешний вид ключа представлен на Рис.3

Рисунок 3. Электронный ключ «Алмаз -1К».

Предварительная настройка

ОС при подключении устройства в USB-порт определяет устройство и устанавливает необходимые драйвера автоматически.

PIN-код устройства

Для работы с финансовыми документами необходимо знать PIN-код устройства.

В системе «Стиль» - Клиент-Банк пароль доступа к личному ключу должностного лица и PIN-код совпадают.

Предустановленный PIN-код устройства отсутствует. Пароль ключа, введенный при генерации, устанавливается PIN-кодом устройства и в дальнейшем работа ведется с ним.

При генерации нового ключа с новым паролем, старые ключ и пароль удаляются.

Работа с устройством

Для указания устройства в комплексе «Стиль» - Клиент-банк необходимо:

- Подключить устройство к USB-порту;
- Выбрать тип носителя - **«smart-карта»**;
- Выбрать в списке устройство отображаемое как « **е.ключ ІІТ Алмаз – 1К - «Код носителя»»** (См. Рис.4)

Внимание! Работа с устройством, отображаемым как **«smart карта Техноконс. TEllipse - «IIT E.Key Almaz-1C 0»»** запрещена.

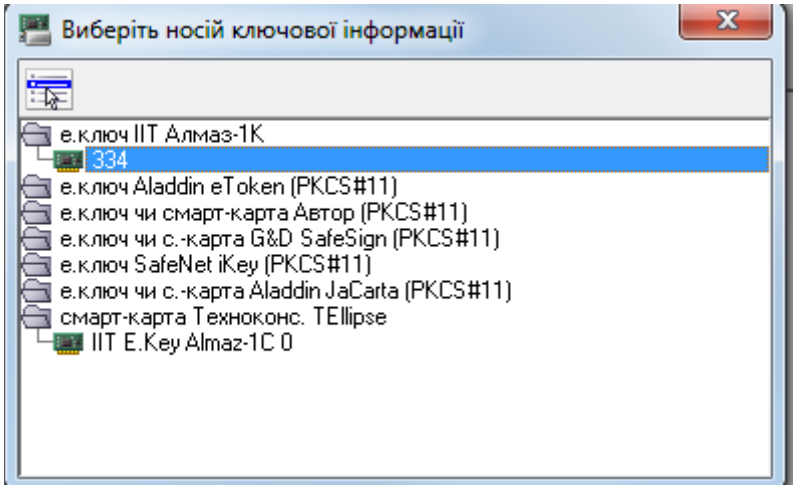

Рисунок 4.Выбор носителя ключевой информации.

Функции управления ключами

Доступны следующие функции управления ключом на устройстве:

- просмотр контекста ключа;
- смена пароля ключа;
- удаление ключа с носителя;

Запрещены следующие функции управления ключом на устройстве:

- Резервное копирование ключа с носителя;
- Резервное копирование ключа на носитель;

2.3 Работа с электронным ключом «Кристал-1»

Внешний вид ключа представлен на Рис.5

Рисунок 5.Электронный ключ Кристал-1.

Предварительная настройка

Перед началом использования устройства, на ПК клиента необходимо

- установить пользовательское ПО устройства «IIT E.ключ Кристал-1», доступное по следующему адресу: (http://iit.com.ua/download/productfiles/EKeyCrystal1Install.exe);
- Подключить устройство к USB-порту;
- Выполнить инициализацию (форматирование) устройства и установить PIN-код устройства с помощью, установленного ПО (См. Рис 6);

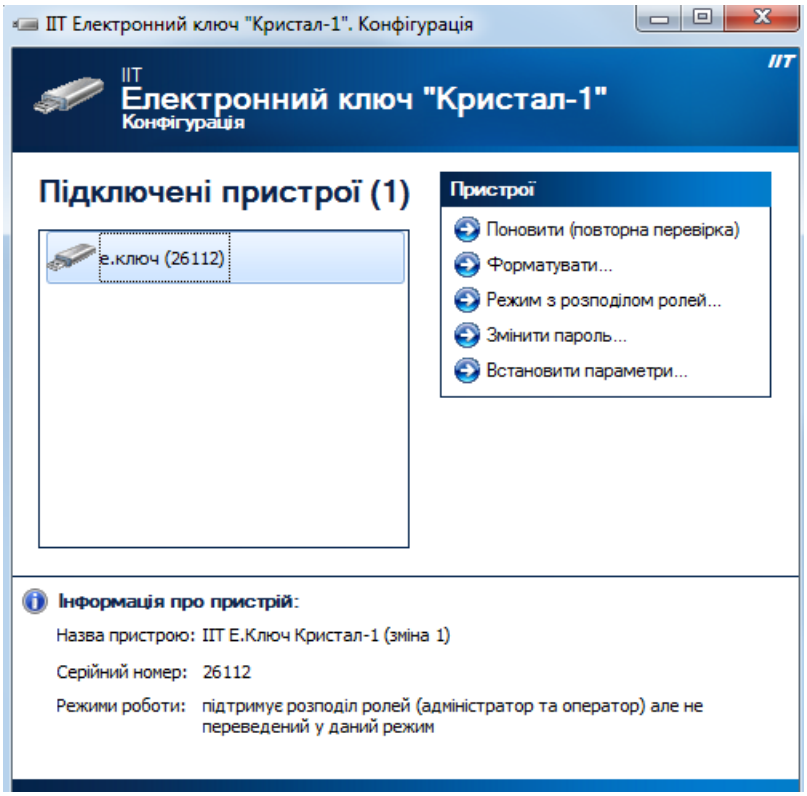

Рисунок 6. Программа «IIT E.ключ Кристал-1».

PIN-код устройства

Для любых операций с устройством, необходимо знать его PIN-код.

Начальный PIN-код устройства задается при инициализации устройства.

В системе «Стиль»-Клиент Банк пароль доступа к личному ключу должностного лица и PIN-код совпадают.

При генерации ключа на устройство обязательно вводится пароль ключа, равный значению PIN-кода устройства.

Следующим шагом пароль ключа и PIN-код устройства изменяются, функцией смены пароля в системе защиты комплекса «Стиль» - Клиент Банк.

В случае утери PIN-кода устройства, выполнить инициализацию и установить PIN-код устройства с помощью, установленного ПО (См. Рис 6).

Работа с устройством

Для указания устройства в комплексе «Стиль» - Клиент Банк необходимо:

- Подключить устройство к USB-порту;
- Выбрать тип носителя - **«smart-карта»**;
- Выбрать в списке устройство отображаемое как

  « **е.ключ Кристал - 1 - «Код носителя»»** (См. Рис.7) или

  « **е.ключ Кристал - 1 (носій) - «Код носителя»»**;

Внимание! Оба элемента списка адресуют одно и то же устройство и операции с любым из элементов тождественны.

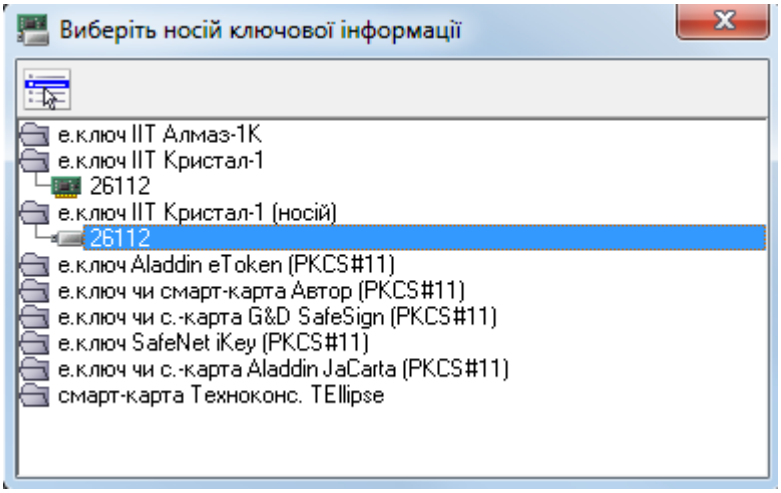

Рисунок 7.Выбор носителя ключевой информации.

Функции управления ключами

Доступны следующие функции управления ключом на устройстве:

- просмотр контекста ключа;
- смена пароля ключа;
- удаление ключа с носителя;

Запрещены следующие функции управления ключом на устройстве:

- Резервное копирование ключа с носителя;
- Резервное копирование ключа на носитель;

2.4 Работа с электронным ключом «SafeNet 5100»

Внешний вид ключа представлен на Рис.8

Рисунок 8. Электронный ключ «SafeNet 5100».

Предварительная настройка

Устройство поставляется с платным ПО (Security authentication Client) от производителя с ежегодно возобновляемой лицензией. Лицензии от производителя на данное ПО за время тестирования устройства мы так и не получили, несмотря на своевременную оплату.

- установлено альтернативное, бесплатное ПО **«eToken PKI client 5.1»,** предоставленное поставщиком электронных ключей;
- Выполнить инициализацию (форматирование) устройства с помощью, установленного ПО (См. Рис 9,10);
- установить PIN-коды администратора и пользователя, без настройки изменения пароля при первом запуске и нажать «Запуск»;

Подробная документация предоставляется продавцом и производителем устройства.

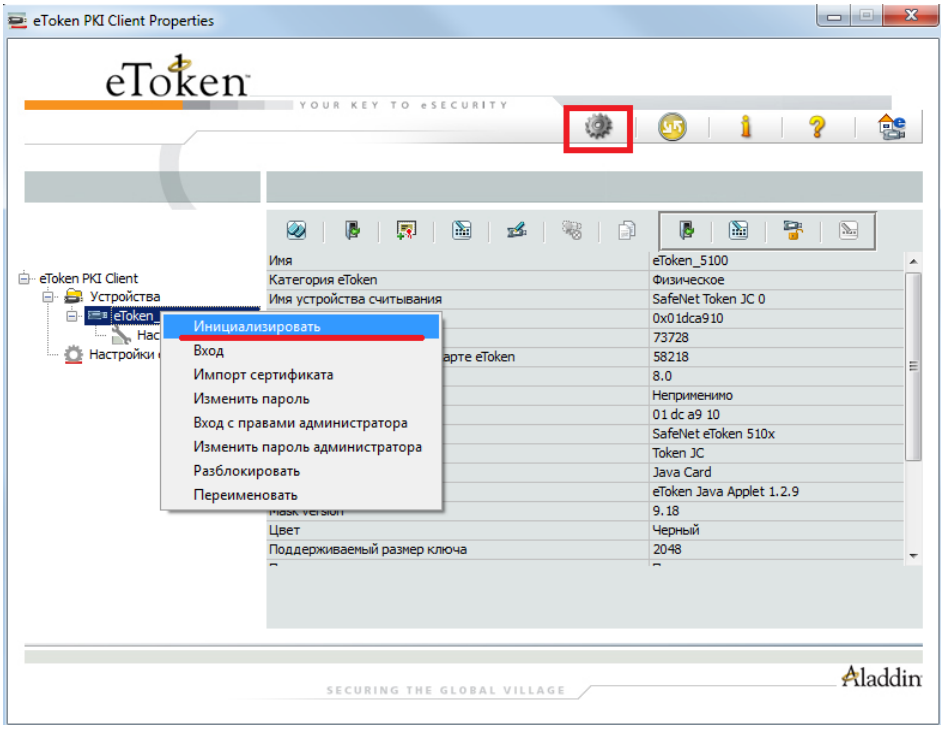

Рисунок 9. Инициализация «SafeNet 5100» с помощью «eToken PKI client 5.1».

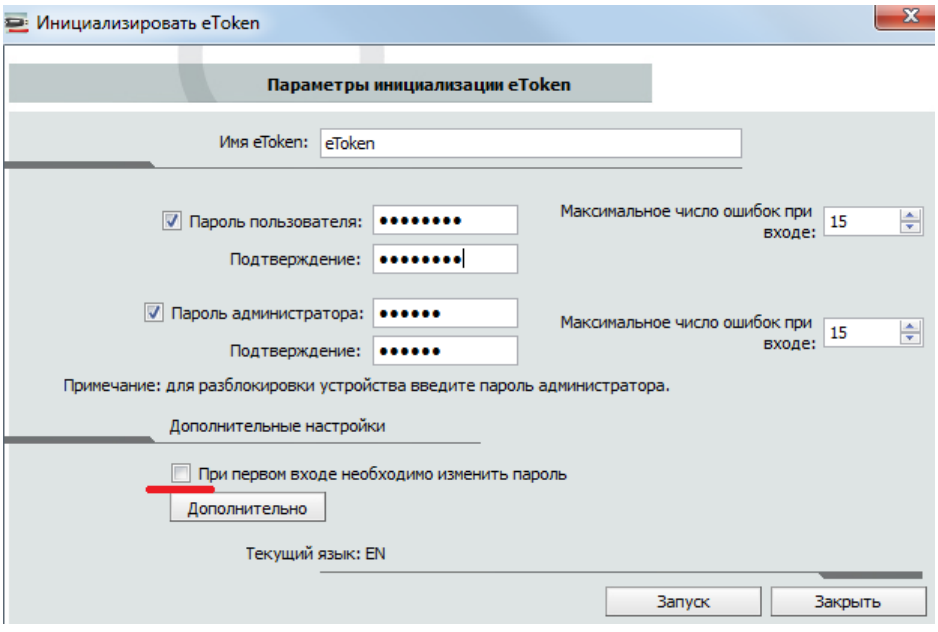

Рисунок 10.Выбор параметров инициализации «SafeNet 5100» с помощью «eToken PKI client 5.1».

PIN-код устройства

Для любых операций с устройством, необходимо знать его PIN-код.

PIN-код пользователя и администратора задаются при инициализации устройства. (Рис.9,10)

В системе «Стиль» - Клиент Банк пароль доступа к личному ключу должностного лица и PIN-код пользователя совпадают.

В случае утери PIN-кода пользователя, доступ к ключу должностного лица будет утерян.

После 15 неверных попыток ввода пароля (настраиваемый при инициализации параметр) доступ к ключу должностного лица по PIN-коду пользователя будет заблокирован.

Чтобы продолжить работу с устройством, необходимо повторно проинициализировать устройство.

При утере обоих PIN-кодов, устройство необходимо переинициализировать, при этом все данные на устройстве будут утеряны.

Работа с устройством

Для указания устройства в комплексе «Стиль» - Клиент Банк необходимо:

- Подключить устройство к USB-порту;
- Выбрать тип носителя - **«smart-карта»**;
- Выбрать в списке устройство отображаемое как « **е.ключ Aladdin eToken (PKCS#11) - «Код носителя»»** (См. Рис.11)

Внимание! Работа со всеми устройствами кроме « **е.ключ Aladdin eToken (PKCS#11) - «Код носителя»»** запрещена.

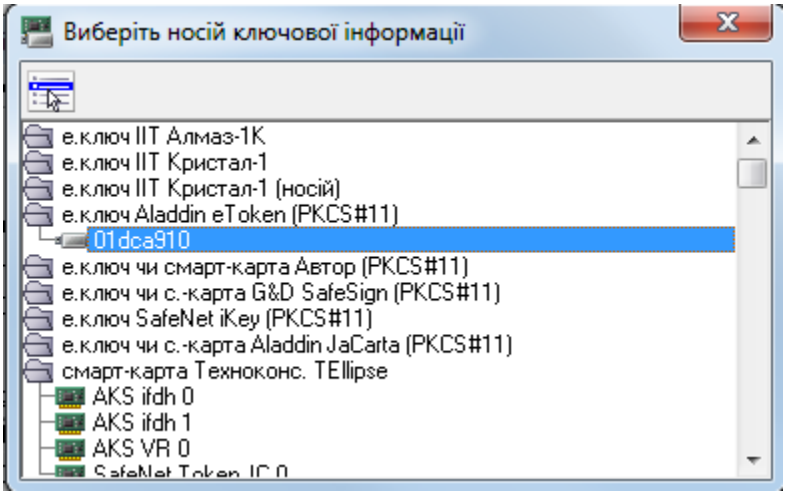

Рисунок 11.Выбор носителя ключевой информации.

Функции управления ключами

Доступны следующие функции управления ключом на устройстве:

- просмотр контекста ключа;
- смена пароля ключа (По умолчанию только «сильный» буквенно-цифровой пароль в разных регистрах. Требования к стойкости ключа, могут быть настроены в утилите конфигурации устройства («eToken PKI client 5.1»). В случае несовпадения нового пароля, сконфигурированным критериям, возникает ошибка - 17 (0x0011));
- удаление ключа с носителя;

Запрещены следующие функции управления ключом на устройстве:

- Резервное копирование ключа с носителя;
- Резервное копирование ключа на носитель;

2.5 Работа с электронным ключом «JaCarta»

Внешний вид ключа представлен на Рис.12

Рисунок 12. Электронный ключ «Aladdin JaCarta».

Предварительная настройка

Перед началом использования устройства, на ПК клиента необходимо

- установить пользовательское ПО устройства «JaCarta DSTU», предоставляется производителем;
- Подключить устройство к USB-порту;
- Выполнить инициализацию (форматирование) устройства с помощью, установленного ПО (См. Рис 13);
- установить PIN-код администратора на 3-й вкладке «Инициализация» (предустановленный код «1234567890»);
- инициализировать PIN-код пользователя, не менее 6 символов (вкладка 2, операции с «ПИН-кодом»);

Подробная документация предоставляется продавцом и производителем устройства.

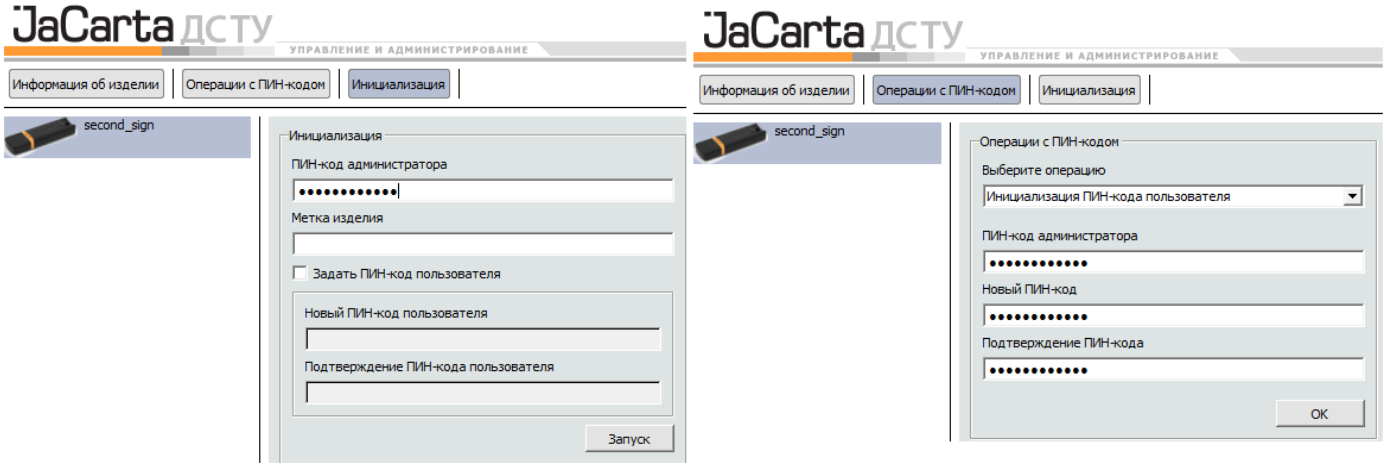

Рисунок 13.Инициализация PIN-кода администратора и пользователя.

PIN-код устройства

Для любых операций с устройством в комплексе «Стиль» - Клиент-Банк, необходимо знать его PIN-код пользователя.

PIN-код пользователя и администратора задаются при инициализации устройства. (Рис.13)

В системе «Стиль» - Клиент-Банк пароль доступа к личному ключу должностного лица и PIN-код пользователя совпадают.

При утере PIN-кода пользователя, доступ к ключу должностного лица будет утерян. Для дальнейшей работы с устройством, необходимо будет снова провести инициализацию устройства.

После 10 неверных попыток ввода пароля пользователя, устройство блокируется. Для работы со старым PIN-кодом, необходимо разблокировать устройство с помощью пароля администратора.

После 10 неверных попыток ввода пароля администратора, устройство, и все операции с правами администратора, блокируются и не могут быть восстановлены.

Работа с устройством

Для указания устройства в комплексе «Стиль» - Клиент-Банк необходимо:

- Подключить устройство к USB-порту;
- Выбрать тип носителя **- «smart-карта»**;
- Выбрать в списке устройство, отображаемое как « **е.ключ чи с.-карта Aladdin JaCarta (PKCS#11) - «Код носителя»»** (См. Рис.14) ;

Внимание! Работа со всеми устройствами, кроме « **е.ключ чи с.-карта Aladdin JaCarta (PKCS#11)- - «Код носителя»»** запрещена.

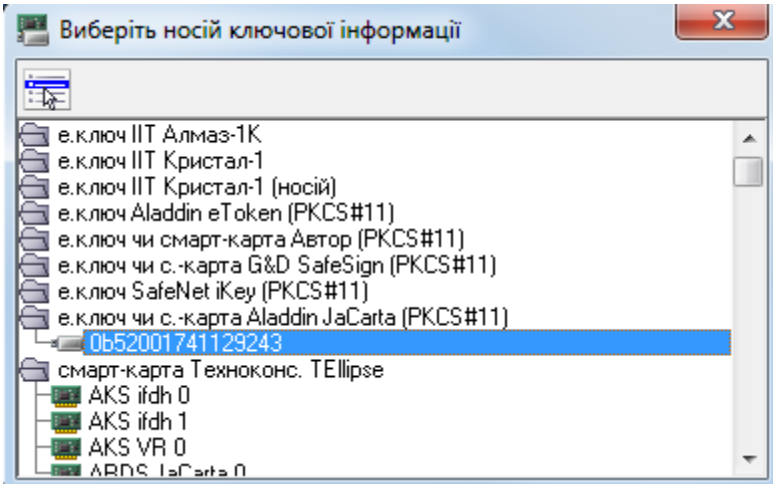

Рисунок 14.Выбор носителя ключевой информации.

Функции управления ключами

Доступны следующие функции управления ключом на устройстве:

- просмотр контекста ключа;
- смена пароля ключа;
- удаление ключа с носителя;

Запрещены следующие функции управления ключом на устройстве:

- Резервное копирование ключа с носителя;
- Резервное копирование ключа на носитель;

Специалисты ЧФ «Энигма-Софт» желают Вам

ПРИЯТНОЙ РАБОТЫ