



**Инструкция пользователя  
системы электронного банкинга StarAccess**

---

**Особенности использования  
USB-токена "Кристалл-1" для хранения  
электронных ключей**

**(версия 1)**

**2012 г.**

## Содержание

1. Общие положения. ....	2
1.1. Используемые сокращения и термины.....	2
1.2. Назначение и возможности. ....	2
2. Порядок создания ключей ЭЦП на USB-токене "Кристалл-1" для клиентов.....	3
2.1. Регистрация новых клиентов в АРМ "Интернет банкинг" с ключом на USB-токене ".....	3
2.2. Генерация нового/дополнительного ключа на USB-токене зарегистрированным клиентом. ....	4
2.3. Администрирование ключей, хранящихся в USB-токене. ....	5
2.4. Особенности регистрации новых клиентов в АРМ "РС-Банкинг".....	6
2.5. Особенности генерации в АРМ "РС-Банкинг" нового/дополнительного ключа. ....	6
2.6. Администрирование ключей на USB-токене в АРМ "РС-Банкинг".....	7
3. Особенности работы с ключом, хранящимся в USB-токене "Кристалл-1". ....	7
3.1. Общая информация. ....	7
3.2. Вход в АРМ "Интернет банкинг" с использованием ключа на USB-токене. ....	7
3.3. Синхронизация АРМ "РС-Банкинг" с использованием ключа на USB-токене.....	7
Приложение 1. Характеристики USB-токена "Кристалл-1". Подготовка рабочей станции пользователя для работы с USB-токеном. ....	9
Общее описание.....	9
Установка драйверов и программного комплекса конфигурации.....	9
Работа с USB-токеном: запуск программы, параметры, форматирование, смена пароля доступа. ....	12
Техническое обслуживание, ремонт и хранение.....	13

### 1. Общие положения.

**Внимание!** В настоящей инструкции описаны особенности работы с USB-токеном "Кристалл-1". Подробное описание регистрации, генерации электронного ключа, работы в системе приведено в соответствующих инструкциях. Описание подготовки рабочей станции к работе с USB-токеном "Кристалл-1" и его характеристики приведены в Приложении 1.

#### 1.1. Используемые сокращения и термины.

**Банк** – АО "УкрСиббанк".

**StarAccess (Система)** - система электронного банкинга StarAccess.

**Клиент** – юридическое или физическое лицо - клиент банка, который эксплуатирует Систему.

**АРМ** – автоматизированное рабочее место клиента системы электронного банкинга StarAccess.

**Электронно-цифровая подпись (ЭЦП)** - вид электронной подписи, полученной по результатам криптографического преобразования набора электронных данных, который дает возможность подтвердить его целостность и идентифицировать личность лица, его наложившего. Электронно-цифровая подпись накладывается с помощью секретного ключа и проверяется с помощью открытого ключа.

**Секретный ключ** – параметр криптографического алгоритма формирования электронно-цифровой подписи, доступный только его владельцу.

**Открытый ключ** - параметр криптографического алгоритма проверки электронно-цифровой подписи, доступный всем субъектам отношений в сфере использования электронно-цифровой подписи.

**USB-токен "Кристалл-1" (USB-токен)** - сертифицированный ГСССЗЗИ Украины криптографический модуль гарантированного хранения ключей, выполненный в виде USB-устройства, предназначенного для безопасного хранения и использования секретных ключей пользователя. В процессе использования USB-токена секретный ключ никогда не покидает защищенную область памяти устройства. Все процессы по формированию ЭЦП и шифрованию данных происходит внутри USB-токена.

#### 1.2. Назначение и возможности.

Внешний вид USB-токена "Кристалл-1" приведен на рис. 1.

USB-токен "Кристалл-1" предназначен для аппаратного выполнения криптографических преобразований. Аппаратная реализация делает невозможным доступ к секретным ключам.

Возможность работы с USB-токеном "Кристалл-1" реализована в АРМ "Регистратор", АРМ "Интернет-Банкинг" и АРМ "РС-Банкинг" для юридических и физических лиц.



**Рис.1. Внешний вид USB-токена "Кристалл-1".**

USB-токен "Кристалл-1" может хранить и использовать два 257-битных секретных ключа национального стандарта "ДСТУ 4145-2002". Инициализация системы криптозащиты происходит после ввода правильного пароля доступа пользователя к USB-токену и секретному ключу. В случае превышения числа попыток неправильного ввода пароля (16 попыток) USB-токен полностью блокируется и дальнейшая работа с ключом, который хранится в USB-токене, невозможна. Код разблокировки не поддерживается.

В случае если USB-токен пользователя был полностью заблокирован, необходимо провести форматирование USB-токена "Кристалл-1", при этом вся хранящаяся в нем информация будет уничтожена. После форматирования можно сгенерировать новую пару ключей (секретный и открытый ключи).

## 2. Порядок создания ключей ЭЦП на USB-токене "Кристалл-1" для клиентов.

### 2.1. Регистрация новых клиентов в АРМ "Интернет банкинг" с ключом на USB-токене "

Для предварительной регистрации необходимо выбрать на сайте системы в меню пункт "Регистрация новых клиентов с ключом на USB-токене".

После загрузки апплета АРМ "Регистратор" необходимо выполнить действия, подробно описанные в инструкции пользователя по регистрации (настройка подключения, ввод реквизитов пользователя и счетов, информации о контактном лице, блокировочного слова и количества подписей при необходимости, проверка введенных реквизитов, информации о владельце ключа).

На Рис.2 показано окно выбора USB-токена "Кристалл-1", на котором будет сгенерирован секретный ключ. После выбора ключа необходимо нажать кнопку "Вперед".

**Внимание!** Перед первым использованием ключ необходимо отформатировать с использованием специального программного обеспечения, доступного на сайте системы (<https://my.ukrsibbank.com/ua/sme/operations/staraccess/files/>), при этом вся хранящаяся на нем информация будет уничтожена.

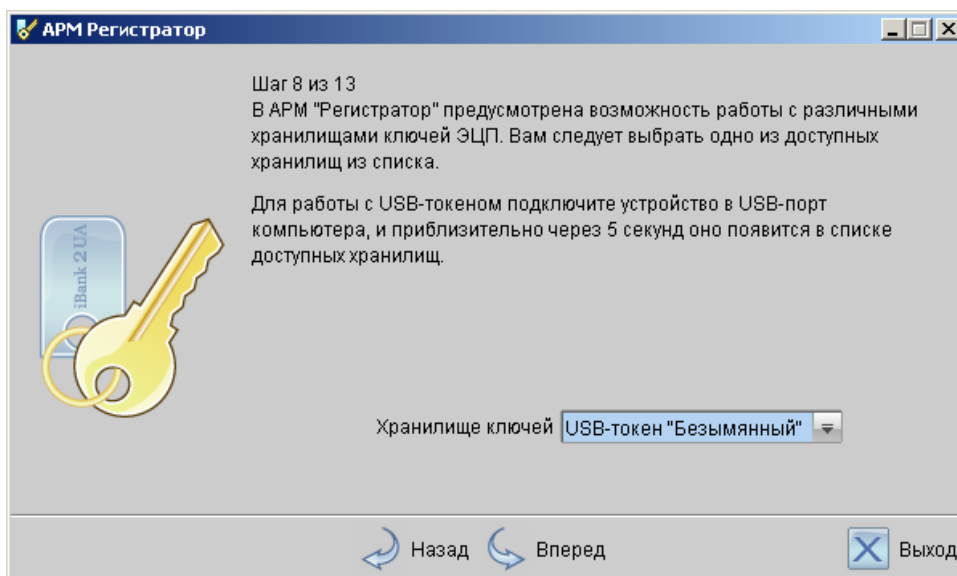


Рис. 2. Выбор USB-токена для генерации ключа.

На следующем шаге необходимо ввести пароль для доступа к USB-токену "Кристалл-1" (Рис.3). Требования к паролям приведены "Инструкции пользователя системы электронного банкинга "StarAccess". Рекомендации по информационной безопасности при работе с системой "StarAccess".

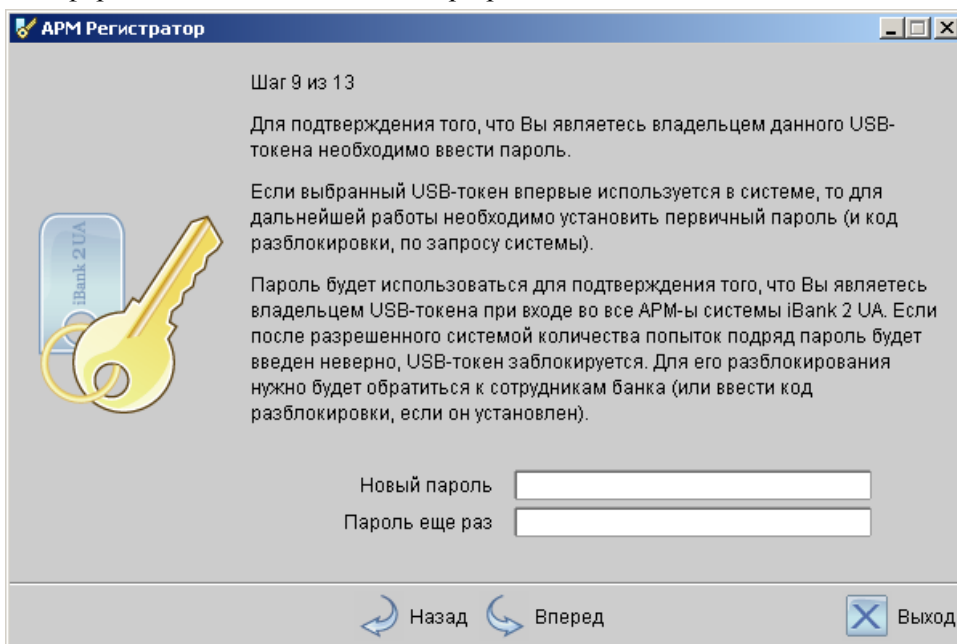
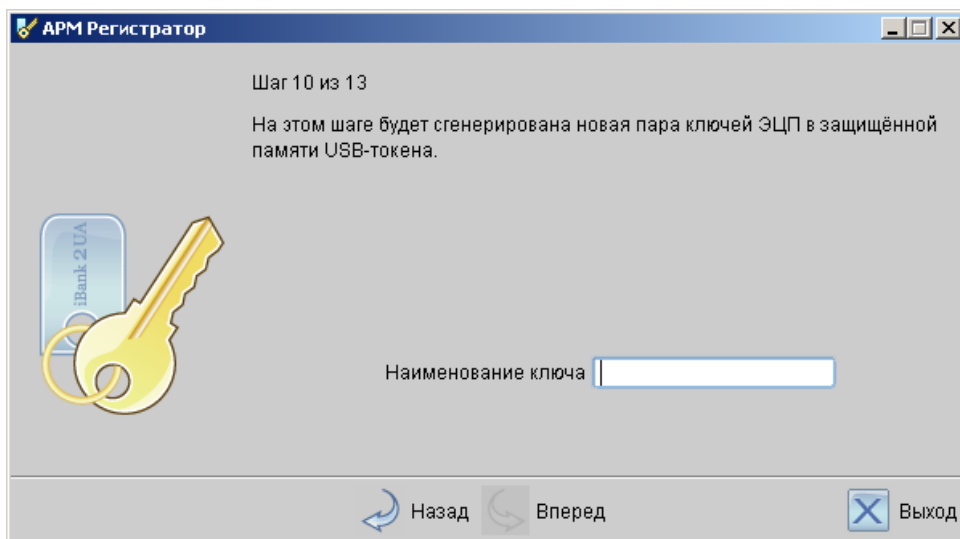


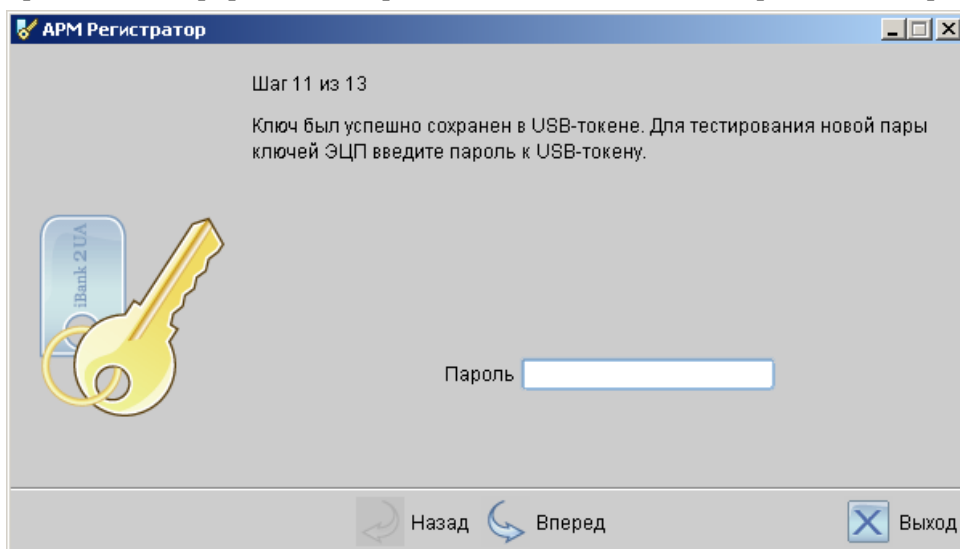
Рис. 3. Задание пароля для доступа к USB-токену.

После задания пароля для доступа к USB-токену предлагается ввести его название (Рис.4).



**Рис. 4. Установка имени USB-токена.**

Для тестирования сгенерированной пары ключей необходимо повторно ввести пароль (Рис.5).



**Рис. 5. Тестирование сгенерированных ключей.**

**Внимание!** В случае превышения числа попыток неправильного ввода пароля (16 попыток), USB-токен полностью блокируется и работа с ключом в USB-токене невозможна. Для дальнейшей работы с USB-токеном необходимо провести его полное форматирование.

После тестирования ключа система предлагает распечатать сертификат открытого ключа и указывает его идентификатор (Рис.6). Необходимо установить флаг "Распечатать сертификат" (на принтер) для печати двух экземпляров или флаг "в RTF файл" для сохранения сертификата в файле, далее нажать кнопку "Вперед".

Последним шагом программы предварительной регистрации является окно "Предварительная регистрация успешно завершена" (Рис.7). Для выхода необходимо нажать кнопку "Выход".

**Примечание:**

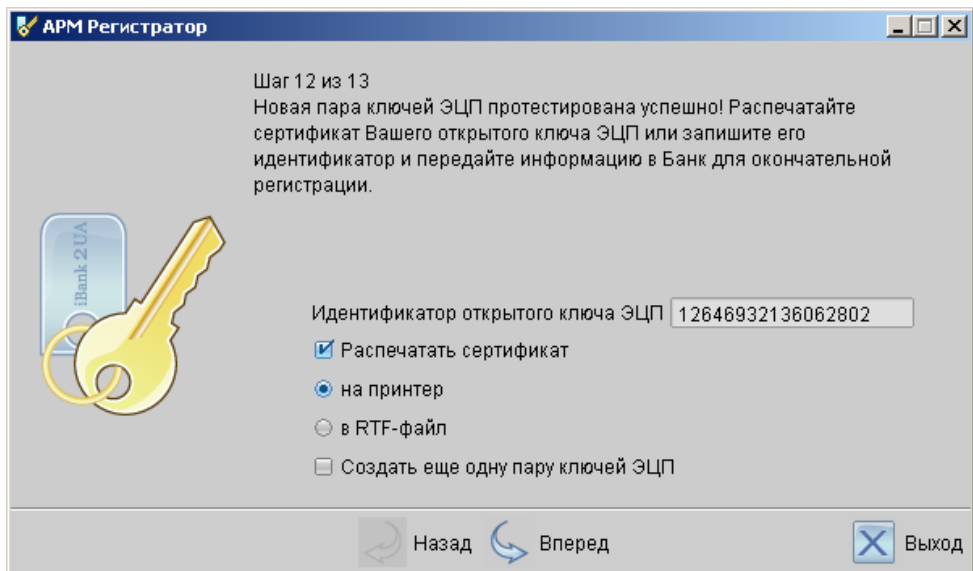
1. В распечатанный сертификат следует от руки вписать информацию о владельце счета, поставить личную подпись и заполнить пол "Достоверность приведенных данных подтверждаю" с подписью руководителя и печатью организации.

2. Информация про вновь зарегистрированного клиента в системе хранится на протяжении 30 дней. Если до момента истечения данного срока клиент не прошел полную регистрацию в отделении банка, информация о предварительной регистрации удаляется.

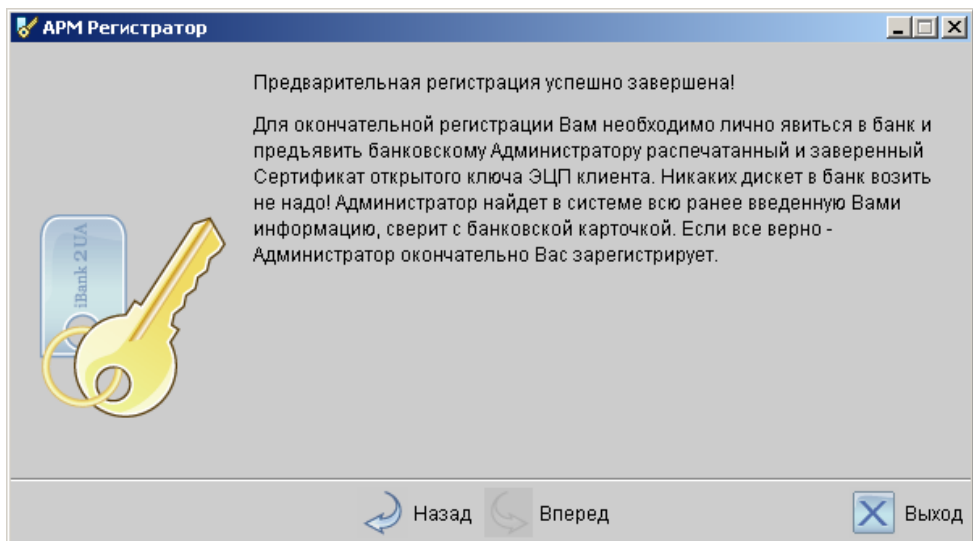
**2.2. Генерация нового/дополнительного ключа на USB-токене зарегистрированным клиентом.**

Перегенерация (генерация нового ключа) может понадобиться в связи с утерей, компрометацией, окончанием срока действия или других причин. Срок действия ключей, которые хранятся на USB-токене "Кристалл-1" составляет 1095 дней (3 года).

После выбора на сайте системы в выпадающем меню пункта "Регистрация новых ключей на USB-токене" необходимо последовательно исполнить действия, как указано на рисунках 2-7.



**Рис. 6. Печать сертификата открытого ключа.**

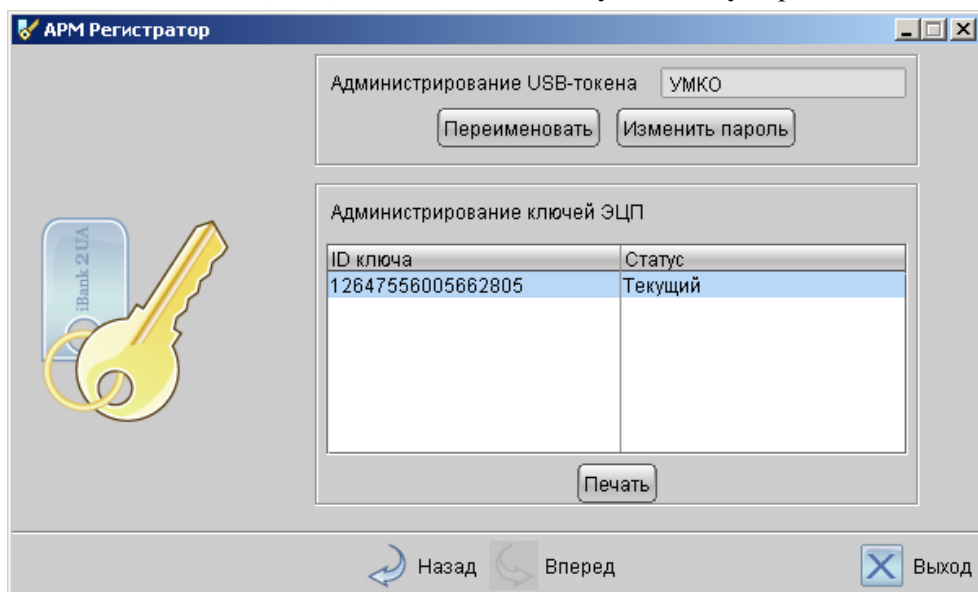


**Рис. 7. Успешное завершение предварительной регистрации.**

### 2.3. Администрирование ключей, хранящихся в USB-токене.

На Рис.8 представлено окно администрирования ключей, которое появляется после выполнения следующих действий:

- на сайте системы в выпадающем меню выбрать пункт "Администрирование ключей на USB-токене";
- выбрать носитель - USB-токена (Рис.2) и ввести соответствующий ему пароль.



**Рис. 8. Администрирование ключей.**

Для любой операции необходимо выбрать ключ, после чего активируются кнопки. В окне администрирования можно повторно распечатать сертификат ключа, изменить пароль USB-токена, переименовать USB-токен. Для завершения работы необходимо нажать кнопку "Выход".

В USB-токене может одновременно храниться до 2-х ключей ЭЦП. При этом действующим всегда является один (имеет статус "Текущий"), который сгенерирован первым, второй ключ всегда имеет статус "Новый" (например, в случае генерации нового ключа после завершения срока действия текущего).

#### 2.4. Особенности регистрации новых клиентов в АРМ "РС-Банкинг".

Для выполнения предварительной регистрации в АРМ "РС-Банкинг" с ключом на USB-токене "Кристалл-1" необходимо установить и выполнить предварительную настройку АРМ "РС-Банкинг" согласно инструкции пользователя (особенности регистрации и работы в АРМ "РС-Банкинг").

После запуска АРМ "РС-Банкинг" появится окно выбора клиента (Рис.9). Необходимо выбрать нового клиента, нажать кнопку "Вход", в появившемся окне нажать кнопку "Предварительная регистрация" (Рис.10). Выбрав USB-токен в качестве места хранения ключей (Рис.11), необходимо последовательно исполнить действия, как указано на рисунках 2-7.

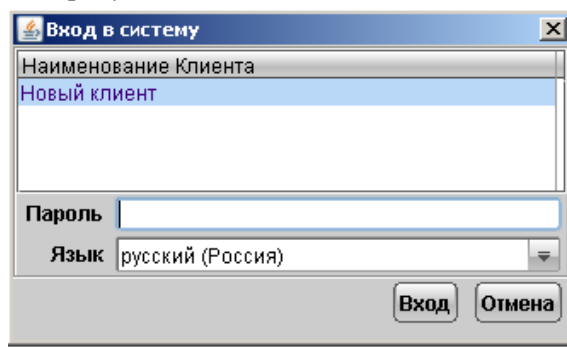


Рис. 9. Окно выбора клиента.

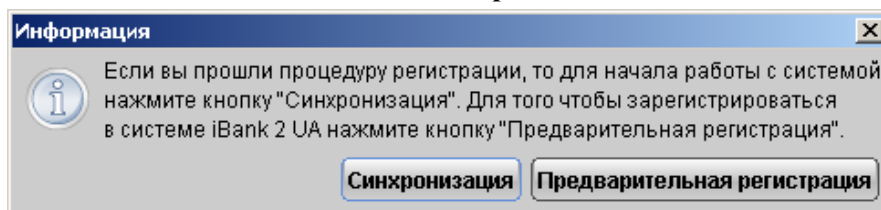


Рис. 10. Окно выбора предварительной регистрации в АРМ "РС-банкинг".

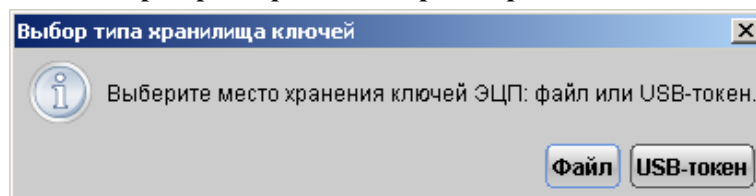


Рис. 11. Окно выбора места хранения ключей ЭЦП.

#### 2.5. Особенности генерации в АРМ "РС-Банкинг" нового/дополнительного ключа.

Для создания нового/дополнительного ключа на USB-токене "Кристалл-1" необходимо запустить АРМ "РС-Банкинг", в появившемся окне выбрать пункт меню "Сервис" / "Новые ключи ЭЦП" (Рис.12).

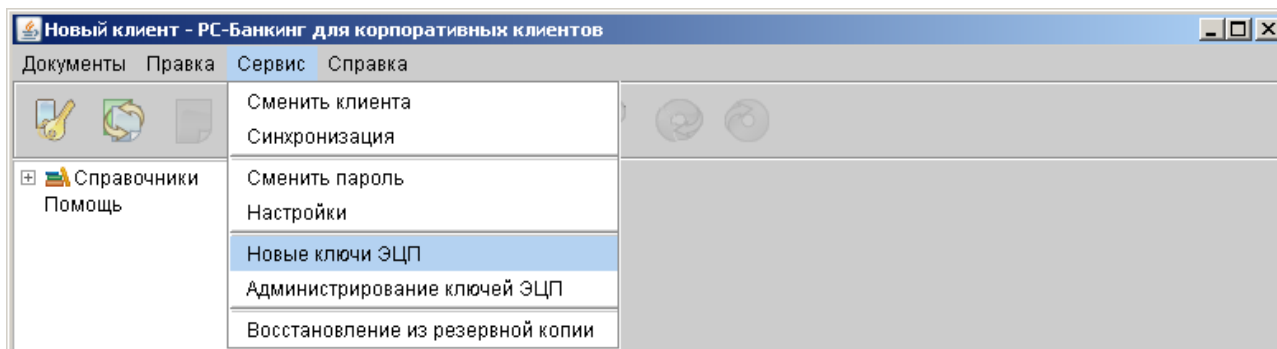


Рис. 12. Окно выбора создания нового ключа в АРМ "РС-Банкинг".

В открывшемся окне (Рис.11) необходимо нажать кнопку "USB-токен", для создания ключа последовательно исполнить действия, как указано на рисунках 2-7.

**Внимание!** В распечатанный сертификат следует от руки вписать информацию о владельце счета, поставить личную подпись и заполнить пол "Достовірність наведених даних підтверджую" с подписью руководителя и печатью организации.

## 2.6. Администрирование ключей на USB-токене в АРМ "РС-Банкинг".

На Рис.13 представлено окно администрирования ключей, которое появляется после выполнения следующих действий:

- Выбрать соответствующий пункт меню;
- Выбрать USB-токен (Рис.11) и ввести соответствующий ему пароль.

Для любой операции необходимо выбрать ключ, после чего активируются кнопки. В окне администрирования можно повторно распечатать сертификат ключа, изменить пароль USB-токена, переименовать USB-токен. Для завершения работы необходимо нажать кнопку "Выход".

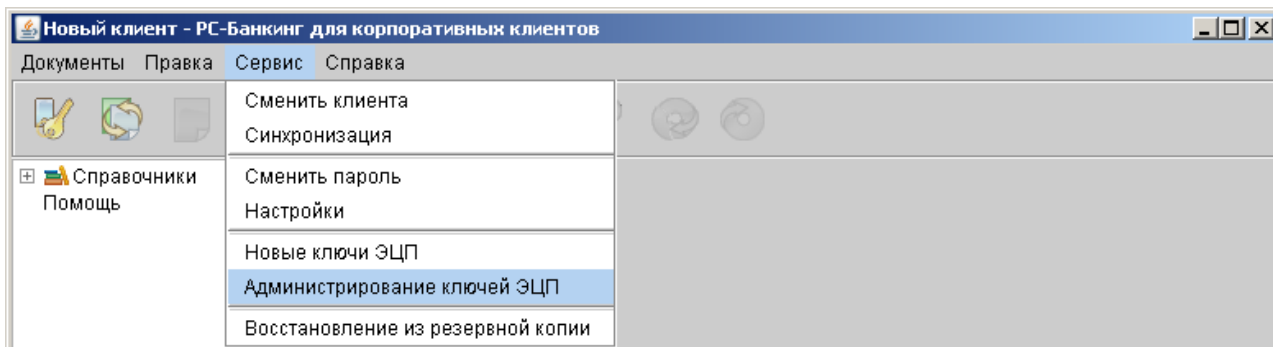


Рис. 13. Окно выбора администрирования ключей ЭЦП в АРМ "РС-Банкинг".

## 3. Особенности работы с ключом, хранящимся в USB-токене "Кристалл-1".

### 3.1. Общая информация.

На USB-токене "Кристалл-1" могут одновременно находиться до 2-х ключей. Актуальным всегда будет только один – активированный первым (в интерфейсе "Администрирование ключей" имеет статус "Текущий"), второй ключ имеет статус "Новый". При генерации на USB-токен нового ключа заменяется ключ, находящийся в статусе "Новый". По истечению срока действия или в случае блокировки ключа в статусе "Текущий", во время входа в систему блокированный ключ удаляется, второй ключ автоматически переходит в статус "Текущий". Для дальнейшей работы необходима активация ключа банком.

Для удаления ключей в USB-токене необходимо отформатировать с помощью специального программного обеспечения, доступного на сайте системы (<https://ibank.ukrsibbank.com>, раздел "Файлы").

### 3.2. Вход в АРМ "Интернет банкинг" с использованием ключа на USB-токене.

При входе в АРМ "Интернет банкинг" необходимо выбрать в поле "Хранилище ключей" название ключа, в поле "Пароль" ввести пароль доступа к USB-токену (Рис.14).

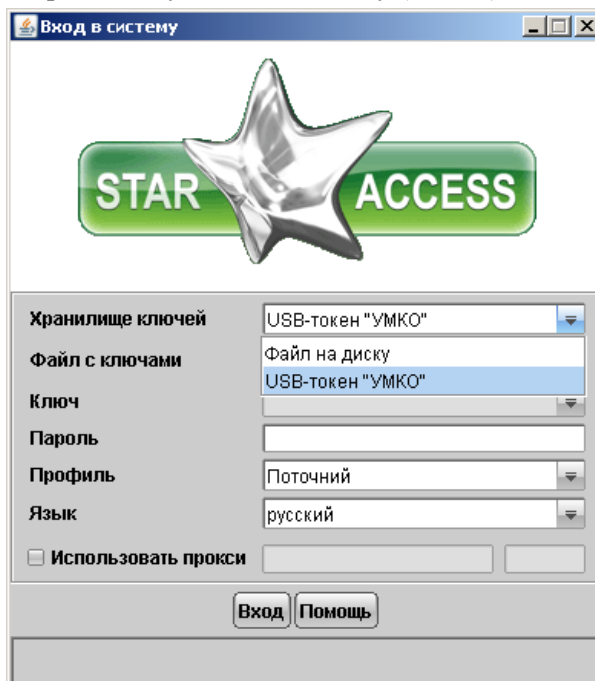


Рис. 14. Окно входа в АРМ "Интернет банкинг".

### 3.3. Синхронизация АРМ "РС-Банкинг" с использованием ключа на USB-токене.

Для синхронизации АРМ "РС-Банкинг" с использованием ключа на USB-токене необходимо запустить АРМ "РС-Банкинг", выбрать в меню "Сервис" пункт "Синхронизация" (Рис.15), в открывшемся

окне выбрать в поле "Хранилище ключей" название ключа и ввести пароль доступа к USB-токену в поле "Пароль" (Рис.16).

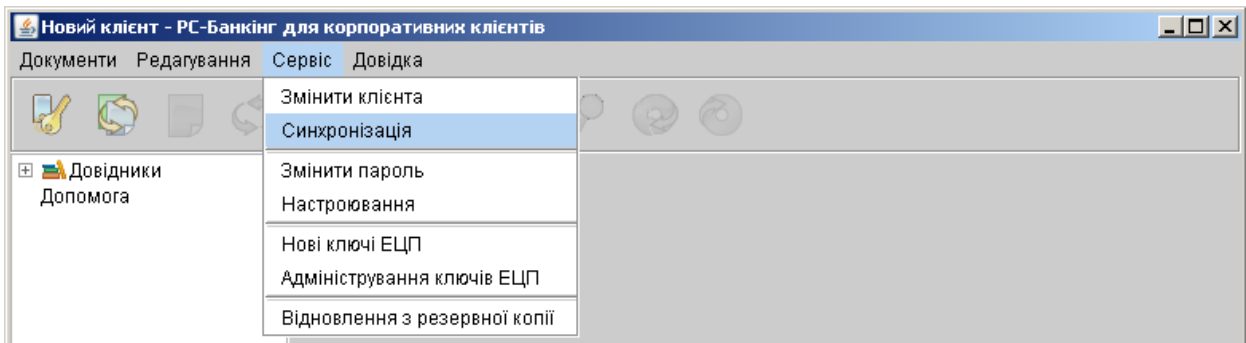


Рис. 15. Вхід в настройки синхронизации АРМ "РС-Банкінг".

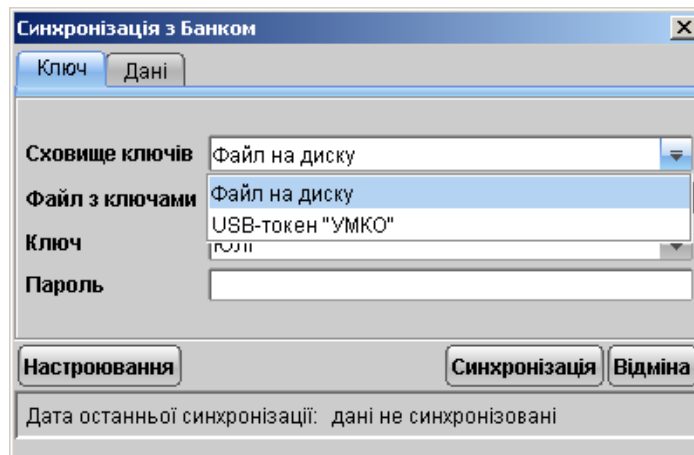


Рис. 16. Окно синхронизации в АРМ "РС-Банкінг".



## **Приложение 1. Характеристики USB-токена "Кристалл-1". Подготовка рабочей станции пользователя для работы с USB-токеном.**

### **Общее описание.**

Электронный ключ "Кристалл-1" (шифр изделия "ИТ Электронный ключ Кристалл-1" - USB-токен "Кристалл-1") предназначен для использования в аппаратно-программных средствах и комплексах криптографической защиты информации (КЗИ) от несанкционированного доступа (НСД).

Область использования устройства – аппаратно-программные средства и комплексы крипто защиты информации, которые предназначены для защиты конфиденциальной информации, которая не является собственностью государства (носитель может быть использован в других программных продуктах, поддерживающих работу с ним).

Драйверы та программный комплекс конфигурации функционируют в ОС Microsoft Windows 98, Microsoft Windows ME, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows XP або Microsoft Windows 2003 Server и выше.

USB-токен "Кристалл-1" реализует следующие **функции**:

- аутентификацию пользователя во время доступа к ключу;
- генерация секретных и открытых ключей для алгоритма ЭЦП;
- генерация ключей для алгоритма шифрования и генерацию случайных последовательностей на основании аппаратного генератора;
- хранение секретных ключей во внутренней памяти и защита их от не санкционированного доступа;
- шифрование данных;
- формирование и проверка ЭЦП;
- вычисление HASH-функции;
- контроль целостности и работоспособности встроенного программного и аппаратного обеспечения и др.

Электронный ключ реализует следующие **криптографические алгоритмы и протоколы**:

- шифрование по ГОСТ 28147-89 (режим простой замены и режим производства имитовставок);
- ЭЦП по ДСТУ 4145-2002 (для ключей любой длины, предусмотренной стандартами стандартом);
- хеширование по ГОСТ 34.311-95;
- протокол распределения ключевых данных Диффи-Хелмана в группе точек эллиптической кривой (длина ключа до 571 бит).

Аппаратная часть и программное обеспечение USB-токена "Кристалл-1" поддерживает следующие **форматы данных**:

- технические спецификации Национальной системы ЭЦП. Форматы базовых объектов (усиленный сертификат, CBC, ЭЦП).
- RFC 3280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 2511. Internet X.509 Certificate Request Message Format.
- RFC 3630. Cryptographic Message Syntax.
- PKCS#8: Private-Key Information Syntax Standard.

USB-токен "Кристалл-1" может быть подключен или отключен от USB-порта рабочей станции пользователя без выключения питания и перезагрузки операционной системы. Системный блок рабочей станции должен быть заземлен.

Запрещается нарушение целостности корпуса изделия и USB-порта при его эксплуатации.

### **Установка драйверов и программного комплекса конфигурации.**

#### **1) Установка драйверов устройства.**

Драйверы устройства предназначены для:

- Обеспечения корректного распознавания устройства операционной системой рабочей станции;
- Передачи кодов команд и входящих данных для выполнения внутренних программ устройства, которые выполняют преобразование входящих данных в исходящие;
- Получение из устройства результатов выполнения команд и исходящих данных.

Необходимые драйверы и другое ПО размещены на сайте системы (<https://ibank.ukrsibbank.com>, раздел "Файлы").

При первом подключении диспетчер устройств ОС найдет новое устройство и откроет окно мастера инсталляции драйвера устройства (рис.1.1). В окне необходимо выбрать опцию "Установка из указанного места" и нажать кнопку "Далее".

На следующей странице (рис.1.2) необходимо выбрать опцию "Включить следующее место поиска" и нажать кнопку "Обзор". В появившемся окне (рис.1.3) указать путь к папке, где размещен файл EKeyCr1.inf, который входит в инсталляционный пакет программ устройства, и нажать кнопку "ОК", для продолжения нажать кнопку "Далее".

В появившемся окне (рис.1.4) нажать кнопку "Все равно продолжить".

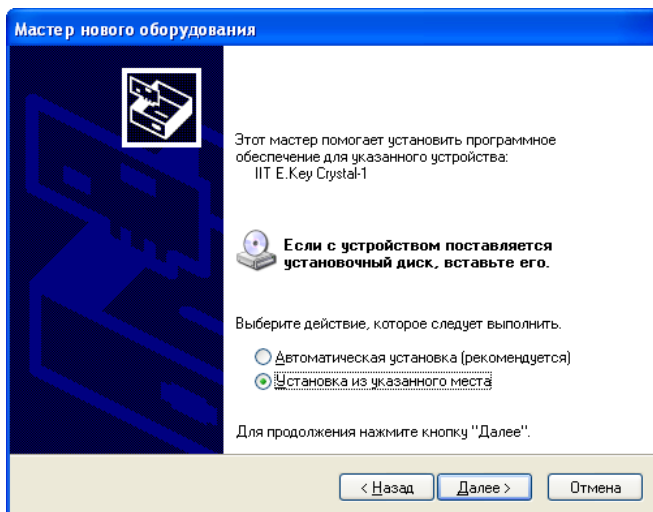


Рис.1.1.

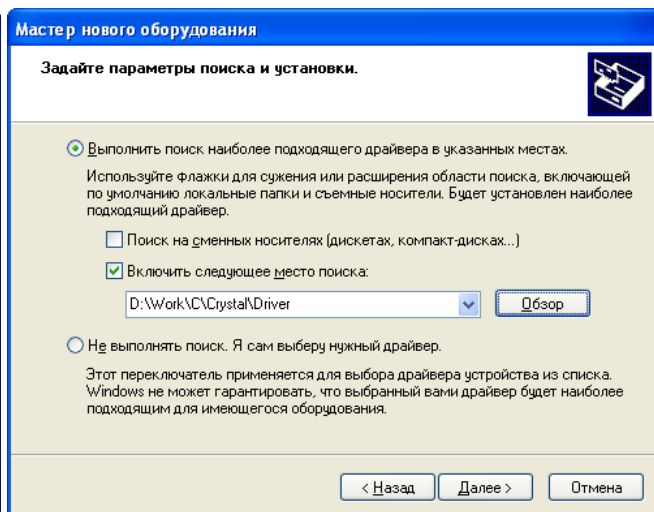


Рис.1.2.

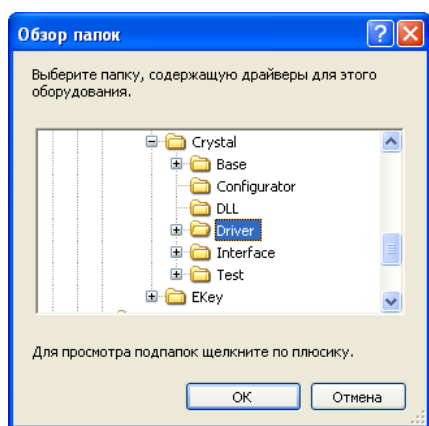


Рис.1.3.

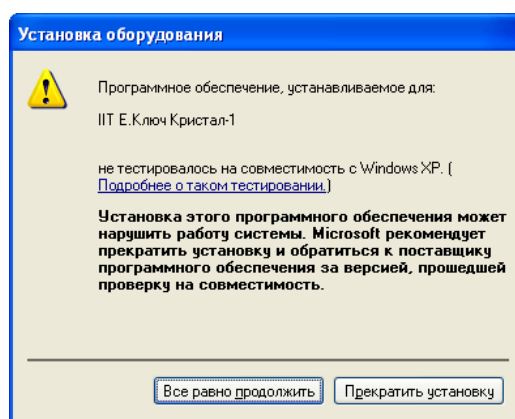


Рис.1.4.

После завершения инсталляции драйвера (рис.1.5) будет выведена последняя страница мастера нового оборудования (рис. 2.6), на которой необходимо нажать кнопку "Готово".

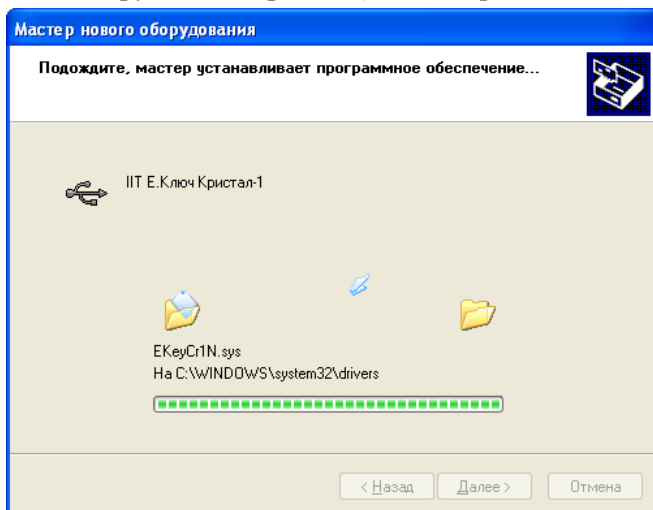


Рис.1.5.

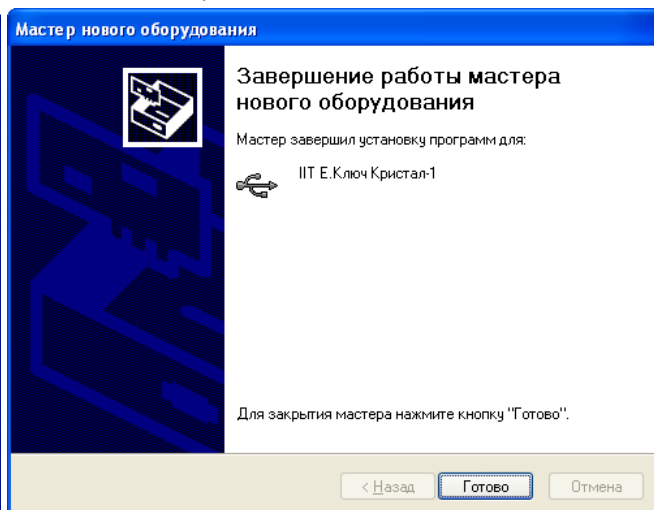


Рис.1.6.

После завершения инсталляции драйвера необходимо проверить установку, запустив диспетчер устройств операционной системы (рис.1.7) – развернуть пункт "Контроллеры универсальной последовательной шины USB" и в списке устройств найти "ИТ Е.Ключ Кристал-1".

### Установка программного комплекса конфигурации.

Программный комплекс конфигурации (Программа) предназначен для форматирования и установки параметров электронного ключа (выполняет технологическое тестирование электронного ключа для проверки работоспособности при проведении технического обслуживания).

Для инсталляции программы необходимо запустить мастер инсталляции (EKeyCrystal1Install.exe).

На первой странице (рис.1.8) выводится информация о начале установки.

Для продолжения работы необходимо нажать кнопку "Далее", для завершения – "Отмена".

На следующей странице (рис.1.9) при необходимости можно указать каталог установки.

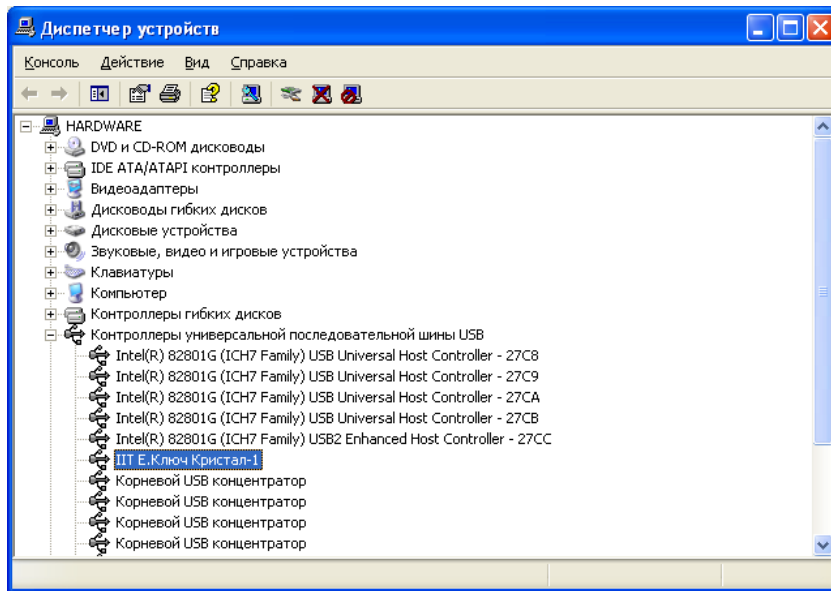


Рис.1.7.

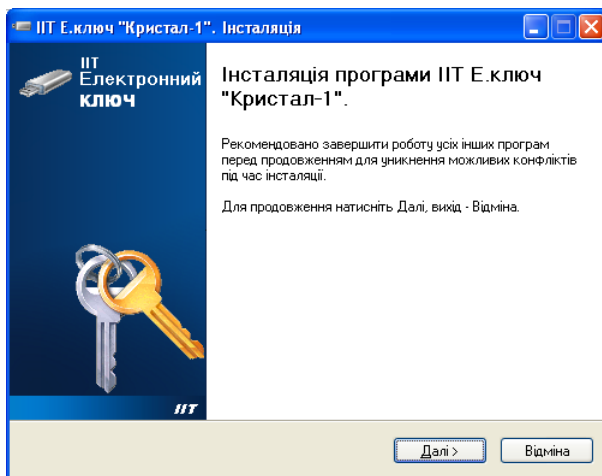


Рис.1.8.

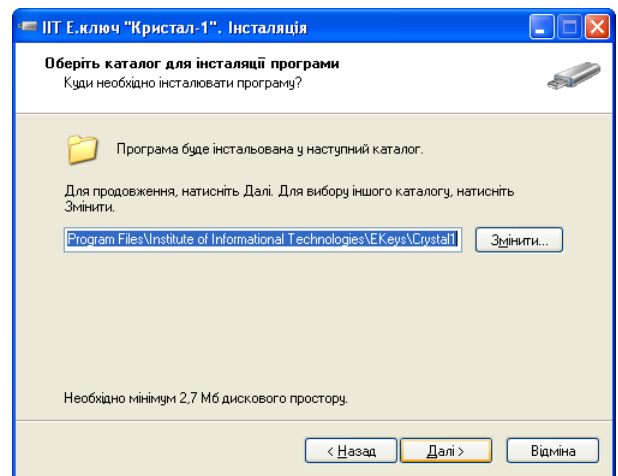


Рис.1.9.

На следующих страницах (рис.1.10-1.11) при необходимости можно указать раздел меню "Пуск", в котором будут установлены ярлыки запуска и удаления программы, задать создание ярлыка запуска на рабочем столе.

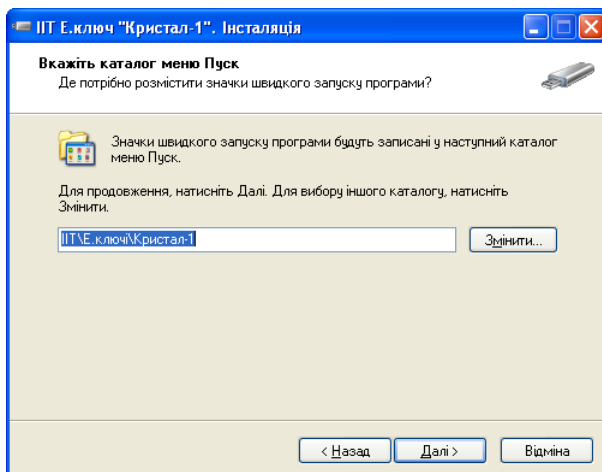


Рис.1.10.

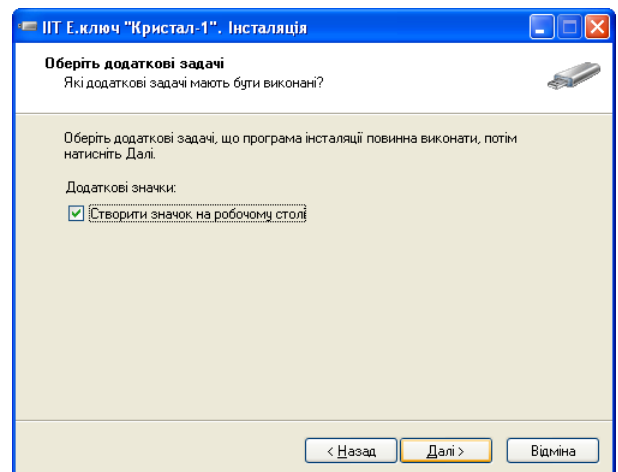


Рис.1.11.

На следующей странице (рис.1.12) будет выведена информация об операциях, которые будут выполнены в ходе установки. Нажмите кнопку "Установить".

Во время установки также может автоматически устанавливаться драйвер электронного ключа (драйверы не являются подписанными Microsoft, поэтому в окне, приведенном на рис.1.13, необходимо нажать кнопку "Все равно продолжить"). После установки мастер завершит свою работу (рис.1.14).

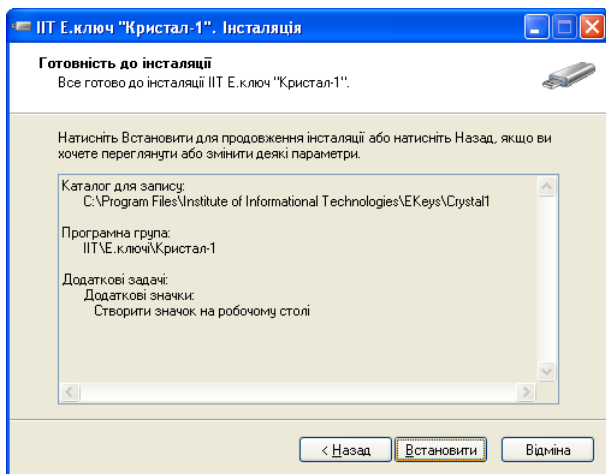


Рис.1.12.

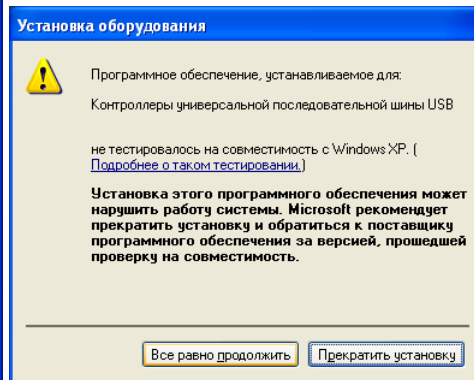


Рис.1.13.

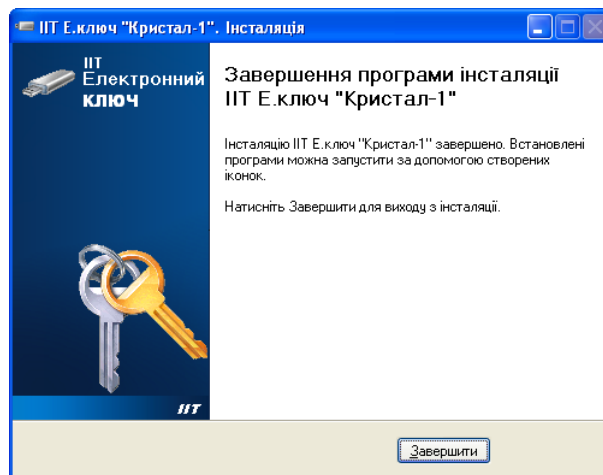


Рис.1.14.

**Работа с USB-токеном: запуск программы, параметры, форматирование, смена пароля доступа.**

Для запуска программы необходимо запустить исполняемый модуль EKeyCrystal1Cfg.exe (рис.1.15).

В левой панели появившегося окна отображается перечень подключенных электронных ключей (устройств). Для работы необходимо выбрать соответствующий электронный ключ (рис.1.16). В нижней части окна выводится информация о параметрах электронного ключа.

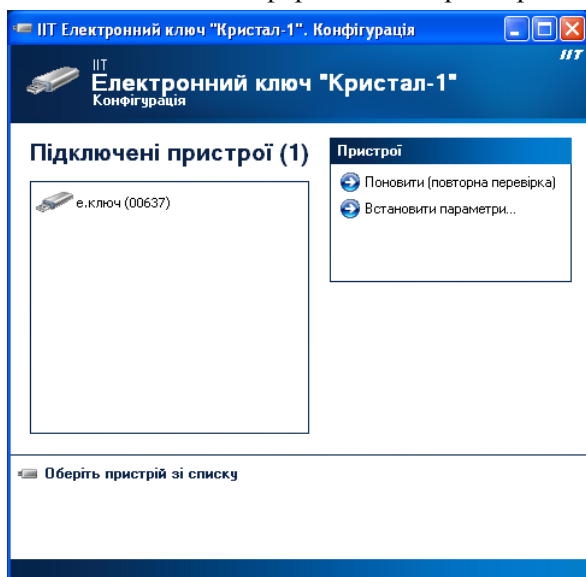


Рис.1.15.

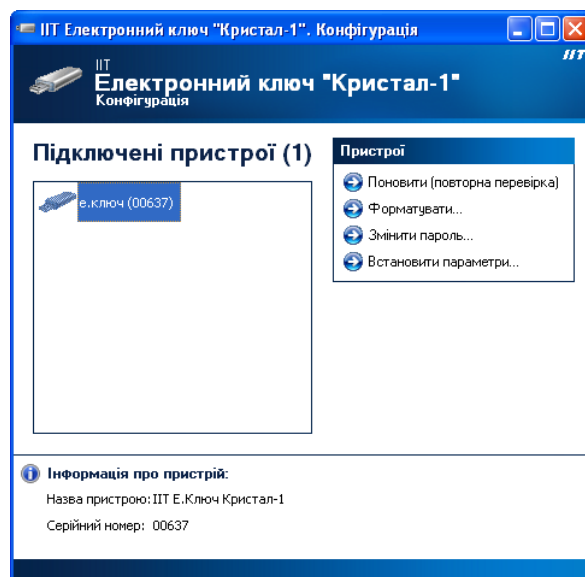
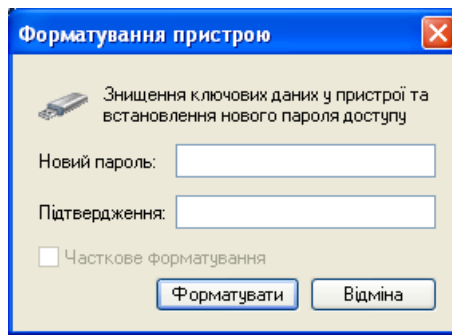


Рис.1.16.

Для форматирования электронного ключа необходимо нажать кнопку "Форматировать" в верхней панели окна (рис.1.16), при этом вся информация на электронном ключе будет уничтожена.

После форматирования необходимо задать новый пароль доступа к электронному ключу (рис.1.17).



**Рис.1.17.**

**Внимание!** Для смены пароля доступа к электронному ключу необходимо использовать АРМ "Регистратор" (для АРМ "Интернет-Банкинг") или АРМ "РС-Банкинг" (см. Раздел 2). Изменить пароль доступа к электронному ключу в USB-токене с помощью установленного ПО невозможно.

#### **Техническое обслуживание, ремонт и хранение.**

Техническое обслуживание устройства выполняется разработчиком (поставщиком). Устройство не имеет индивидуальных особенностей технического обслуживания, ремонту не подлежит (подлежит замене).

Проверка работоспособности осуществляется с помощью программного комплекса тестирования и конфигурации.

Климатические требования к эксплуатации USB-токена "Кристалл-1":

- температура окружающего воздуха – (15...25) 0С;
- относительная влажность окружающего воздуха – (45...75) %;
- атмосферное давление – 84-107 кПа (630-800 мм. рт. ст.);
- в воздухе не допускается наличие паров кислот, щелочей и прочих агрессивных примесей, которые вызывают коррозию.

Устройство в упакованном для транспортирования виде сохраняет внешний вид и работоспособность после влияния следующих климатических факторов с последующей шестичасовой выдержкой в нормальных климатических условия:

- температура воздуха от 40<sup>0</sup>С до плюс 60 °С;
- относительная влажность воздуха до 98% при плюс 25°С;
- атмосферное давление от 60 до 107 кПа (от 450 до 800 мм.рт.ст.).

Гарантийный срок хранения - 1 год.