

СОДЕРЖАНИЕ

1. Введение.....	2
2. Подготовка «Astroma SecretKey» к работе.....	3
2.1 Установка программного обеспечения «Astroma SecretKey»	3
2.2 Установка драйвера для USB-ключа «LOCK»	7
2.3 Задание/изменение пароля доступа к USB-ключу	9
2.4 Генерация ключа шифрования	10
3. Работа с «Astroma SecretKey».....	11
3.1 Создание зашифрованных файлов	12
3.2 Работа с зашифрованными файлами.....	14
3.3 Создание дубликата USB-ключа	15
3.4 Перешифровка файлов	16
3.5 Расшифровка файлов.....	18

1. Введение

На современной стадии развития науки и техники все большую ценность приобретает информация разных видов (государственная, научно-техническая, коммерческая и т. д.). Как правило, она хранится на компьютерных носителях, что значительно упрощает процесс ее обработки. Эти факторы обуславливают важность защиты информации от несанкционированного использования. «**Astroma SecretKey**» является одним из средств защиты информации, хранимой на компьютерных носителях.

Применение «**Astroma SecretKey**» позволяет хранить защищаемую информацию на носителях в зашифрованном виде. В процессе работы с защищенной информацией при чтении с носителя происходит автоматическая ее расшифровка, а при записи – шифрование. Процессы шифрования и расшифровки происходят исключительно внутри USB-ключа «LOCK» посредством ключа шифрования, который хранится в памяти устройства. Доступ к USB-ключу осуществляется посредством пароля, что предотвращает возможность несанкционированного доступа к информации в случае завладения USB-ключом посторонними лицами. После трех подряд попыток ввода неверного пароля производится стирание ключа шифрования из памяти USB-ключа, после чего доступ к информации становится невозможным без наличия дубликата USB-ключа.

По сравнению с другими системами «**Astroma SecretKey**» обладает рядом преимуществ:

- При использовании «**Astroma SecretKey**» вся защищаемая информация хранится на любых доступных носителях в зашифрованном виде, поэтому использовать ее нелегально невозможно, даже имея копию.
- Расшифрованная защищаемая информация располагается только в оперативной памяти компьютера, где обрабатывается приложениями Windows (MS Office, Adobe Reader, Блокнот и т.д.).
- Доступ к информации осуществляется с помощью компактного электронного устройства - USB-ключа.
- Электронный USB-ключ полностью выполняет функции криптографического устройства, производя внутри себя шифрование и расшифровывание информации «на лету».
- Ключ шифрования всегда хранится в энергонезависимой памяти микрочипа USB-ключа и никогда ее не покидает, следовательно, ключ шифрования не попадает в компьютер и никому не может быть доступен ни в каком виде, тем более открытым.
- В любой момент пользователь может произвести смену ключа шифрования с перешифровкой информации.
- Помимо наличия самого USB-ключа требуется знание пароля доступа для его разблокировки, поэтому нелегальное завладение данным устройством не предоставляет возможности доступа к зашифрованной информации.
- После третьей подряд попытки ввода неверного пароля в USB-ключе производится уничтожение ключа шифрования, и доступ к информации с использованием данного устройства в дальнейшем становится невозможным.
- При необходимости предоставления доступа к информации нескольким лицам, либо на случай утраты USB-ключа имеется возможность создания ключей-дубликатов, если при генерации ключа шифрования была сохранена его копия.

2. Подготовка «Astroma SecretKey» к работе

В базовый комплект поставки «Astroma SecretKey» входят:

- USB-ключ «LOCK» с необходимым программным обеспечением в памяти, предназначенным для работы в системе «Astroma SecretKey»;
- Диск для установки на компьютер пользователя программного обеспечения «Astroma SecretKey» и драйвера USB-ключа «LOCK».

Перед использованием «Astroma SecretKey» для защиты информации предварительно необходимо произвести ряд подготовительных действий, таких как инсталляция программного обеспечения «Astroma SecretKey», установка драйвера USB-ключа «LOCK», задание пароля для USB-ключа и генерацию ключа шифрования. Порядок выполнения этих действий описан ниже.

2.1 Установка программного обеспечения «Astroma SecretKey»

Для установки программного обеспечения «Astroma SecretKey» вставьте установочный диск в CD-привод вашего компьютера. После этого должен автоматически запуститься процесс инсталляции. Если этого не произошло, то вручную произведите запуск файла с именем **SetupSEC.exe**. На экране появится окно, изображенное на рис. 2.1.А, где будет предложено выбрать язык для установки.

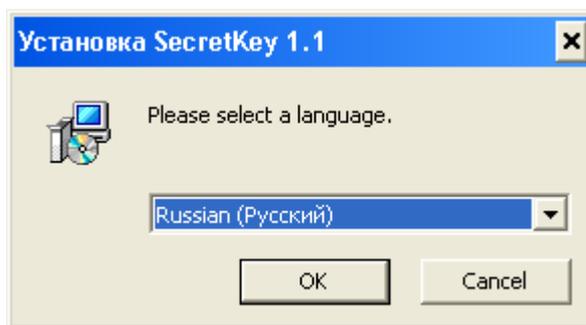


Рис. 2.1.А. Окно выбора языка интерфейса программы установки

После выбора из списка языка для установки нажмите кнопку «OK», или если хотите отменить установку, нажмите кнопку «Cancel». После нажатия кнопки «OK» на экране появится окно запуска мастера установки «Astroma SecretKey» (рис. 2.1.Б).

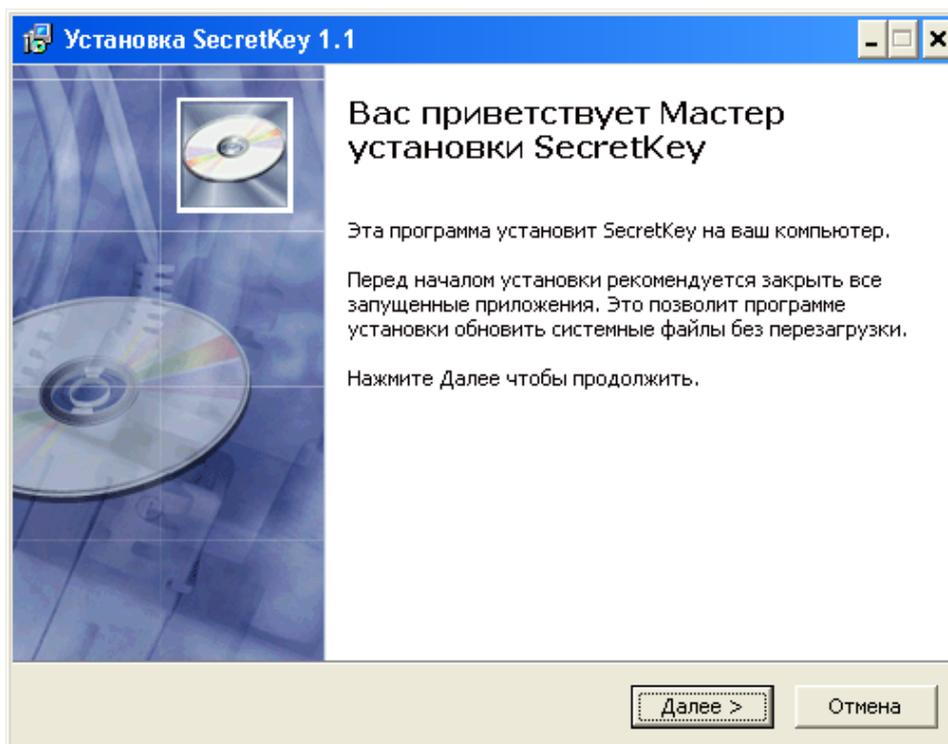


Рис. 2.1.Б. Окно запуска мастера установки «Astroma SecretKey»

Мастер установки сообщит о предстоящих действиях и предложит либо прервать установку нажатием кнопки «Отмена» либо продолжить нажатием кнопки «Далее». После нажатия кнопки «Далее» мастер предложит выбрать папку для установки (рис. 2.1.В).

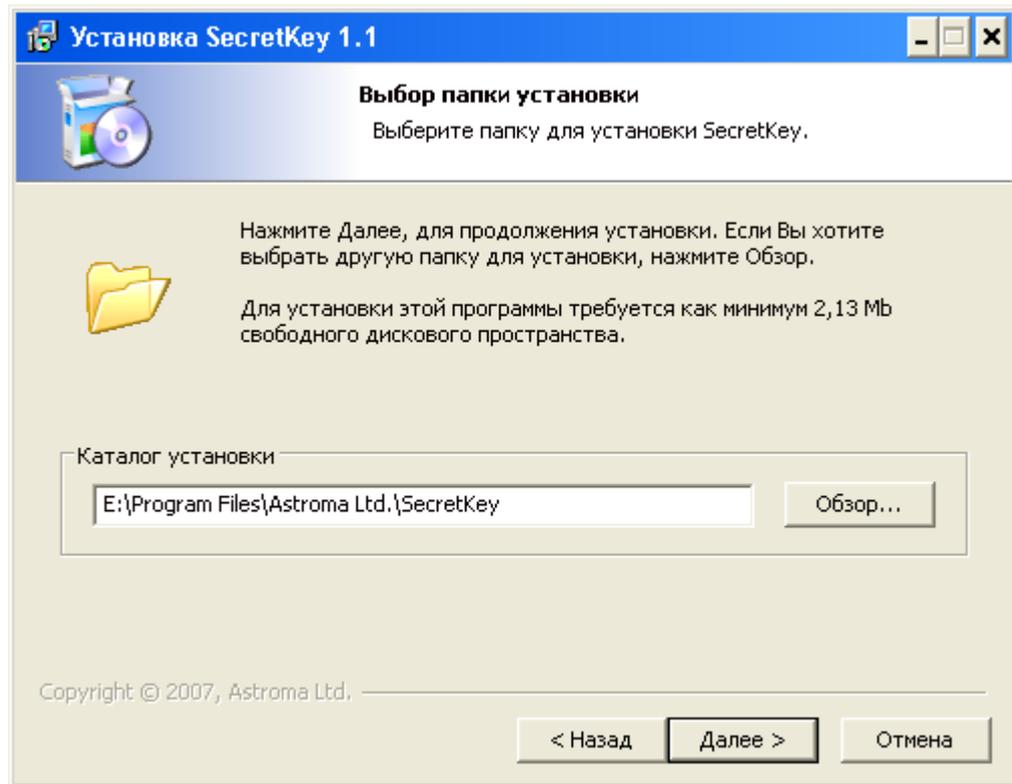


Рис. 2.1.В. Окно выбора места установки «Astroma SecretKey»

В строке «Каталог установки» будут отображаться путь и имя папки для установки «Astroma SecretKey» по умолчанию. Если это устраивает, нажмите кнопку «Далее». Если же Вы хотите изменить место установки, произведите выбор нового места, нажав кнопку «Обзор» или напрямую впишите путь непосредственно в строку «Каталог установки», после чего нажмите кнопку «Далее». Затем на экране появится окно выбора программной группы в меню «Пуск» (рис. 2.1.Г).

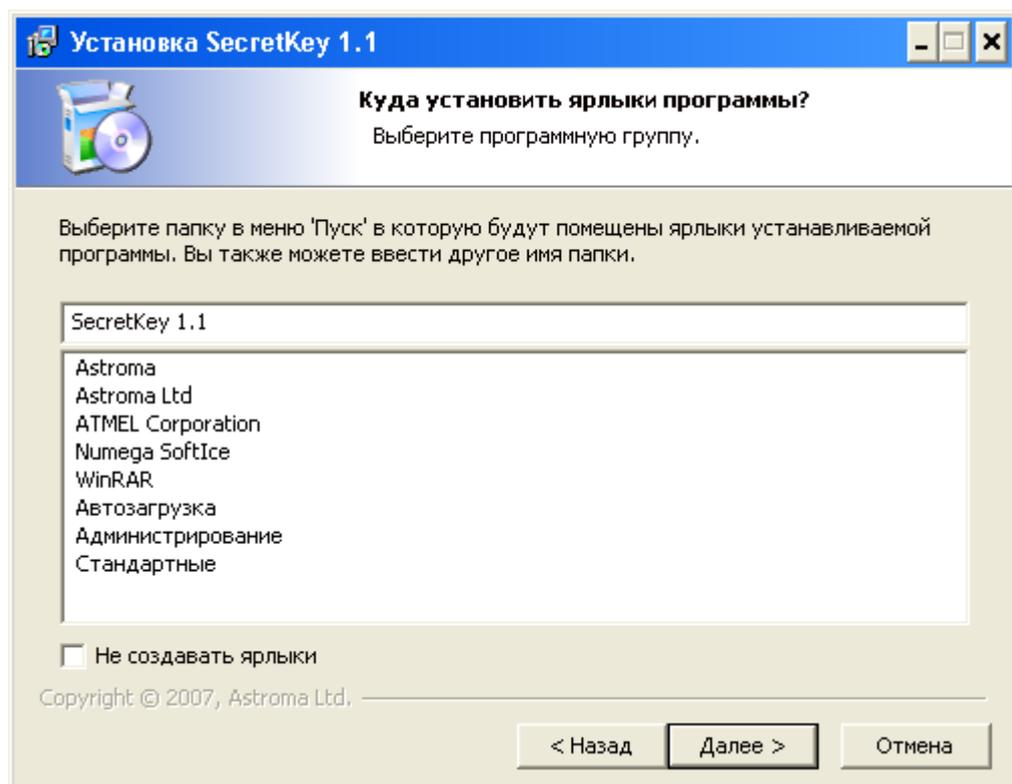


Рис. 2.1.Г. Окно выбора программной группы в меню «Пуск»

В строке, расположенной над предоставленным списком возможных программных групп, следует указать название программной группы, где будут располагаться ярлыки для запуска программного обеспечения «Astroma SecretKey» через меню «Пуск». По умолчанию программная группа будет называться «SecretKey 1.1». После задания названия группы необходимо нажать кнопку «Далее». При этом Вам будет предложено создать ярлык «Astroma SecretKey» на рабочем столе (рис. 2.1.Д).

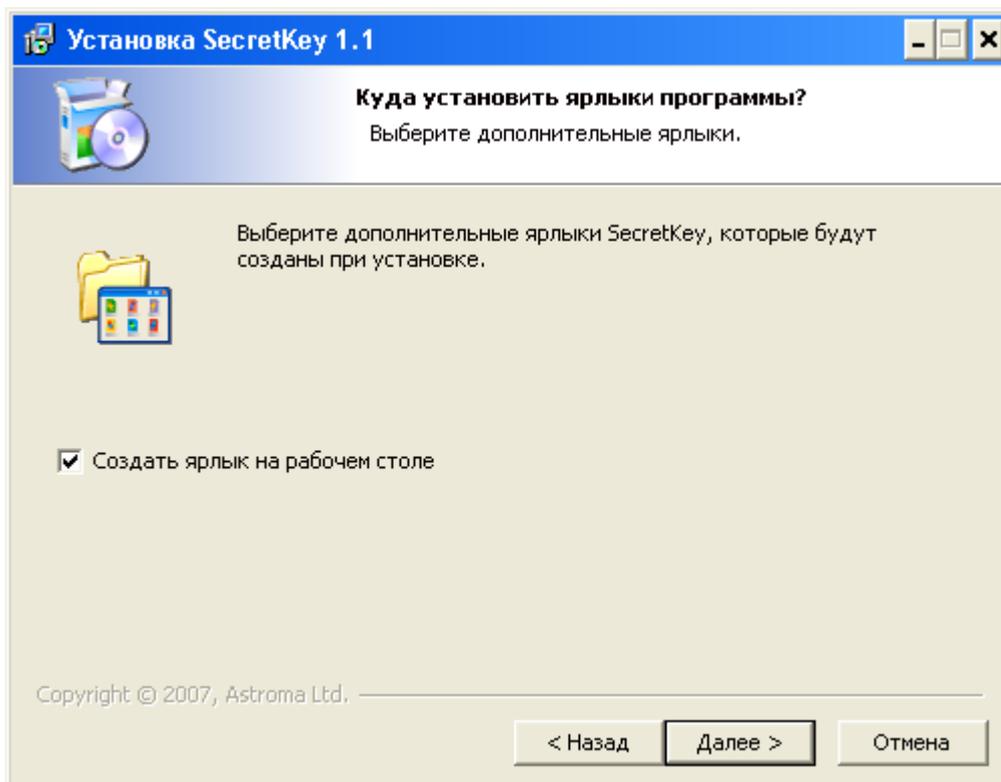


Рис. 2.1.Д. Окно с предложением создать ярлык «Astroma SecretKey» на рабочем столе

После ответа на предложение для продолжения установки нажмите кнопку «Далее». На экране появится окно, выбранных параметров установки «Astroma SecretKey» (рис. 2.1.Е).

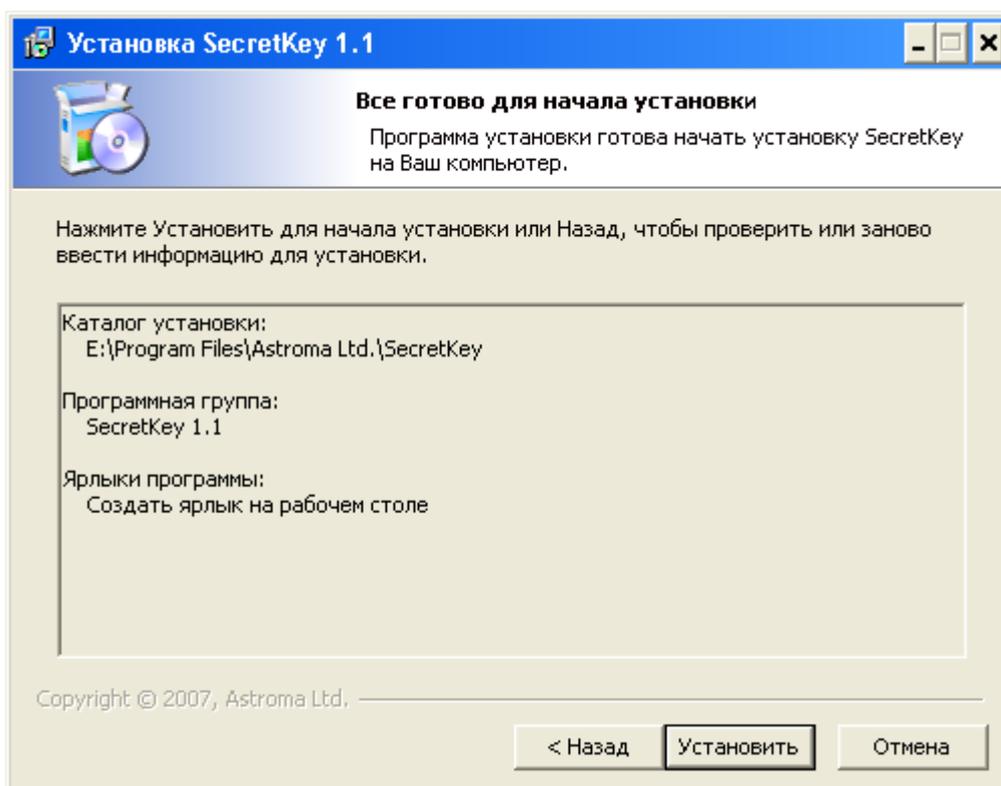


Рис. 2.1.Е. Окно параметров установки «Astroma SecretKey»

После проверки параметров установки, если Вы обнаружили ошибки, вернитесь для ее исправления к соответствующему окну, нажимая кнопку «Назад». Если все верно, нажмите

кнопку «Установить» для начала инсталляции. Выполнение этой операции Вы можете контролировать в окне процесса установки «**Astroma SecretKey**» (рис. 2.1.Ж).

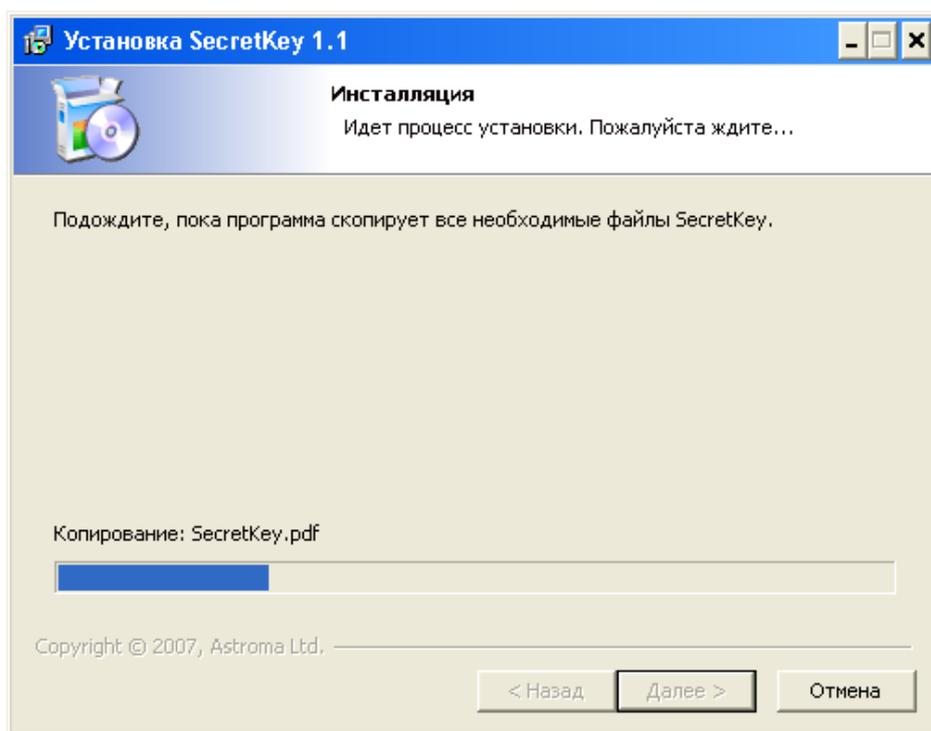


Рис. 2.1.Ж. Окно хода выполнения процесса установки «**Astroma SecretKey**»

Если Вы хотите прервать процесс установки, следует нажать кнопку «Отмена». По завершении установки на экране появится окно, показанное ниже (рис. 2.1.И).

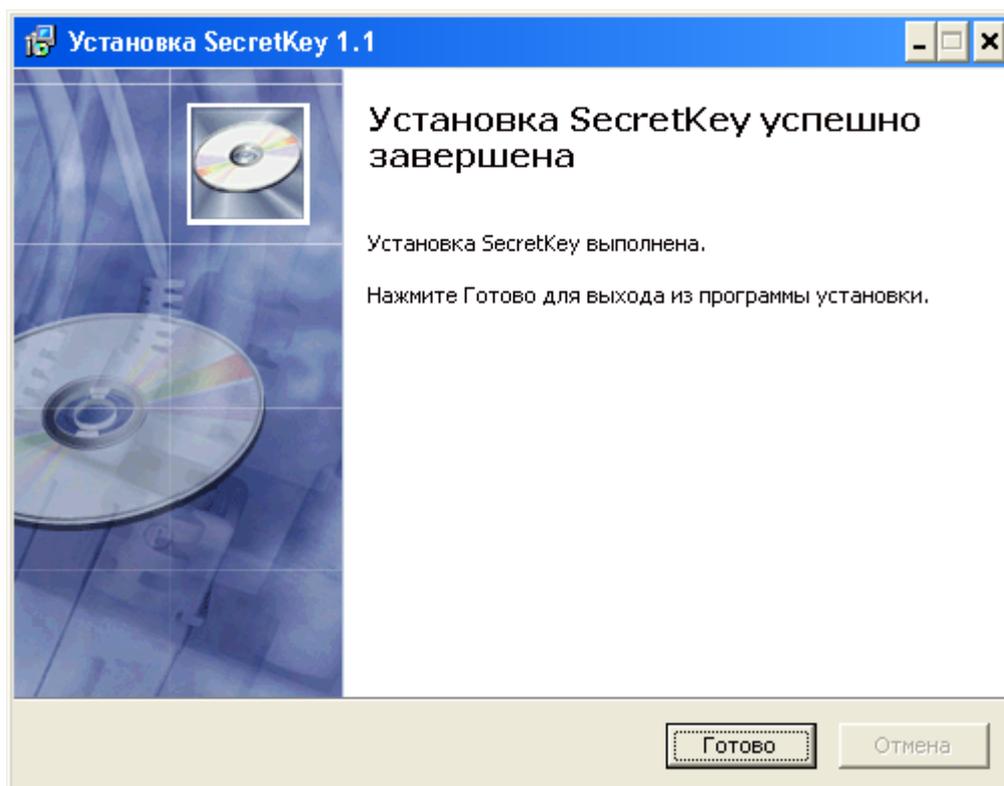


Рис. 2.1.И. Окно завершения установки «**Astroma SecretKey**»

Данное окно сообщает об удачной установке программного обеспечения «**Astroma SecretKey**». Здесь следует нажать кнопку «Готово», тем самым, завершая установку.

Перед использованием «**Astroma SecretKey**» необходимо так же установить драйвер USB-ключей «LOCK», процесс установки которого описан ниже.

2.2 Установка драйвера для USB-ключа «LOCK»

По завершении установки «Astroma SecretKey» необходимо произвести установку драйвера USB-ключа «LOCK». Подключите USB-ключ к компьютеру, система автоматически запустит мастер установки нового оборудования, и на экране появится окно, изображенное ниже (рис. 2.2.К).

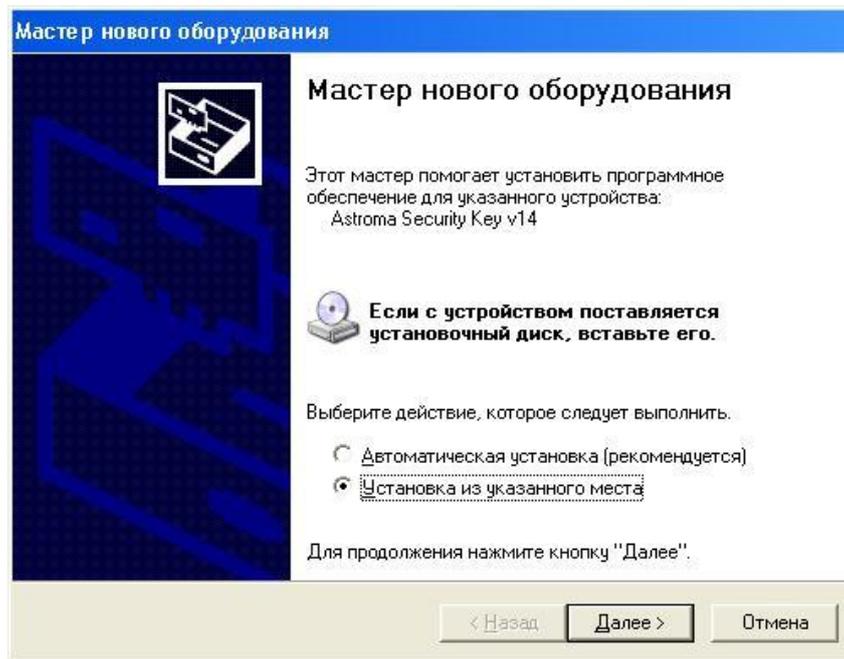


Рис. 2.2.К. Окно мастер установки нового оборудования

В данном окне нужно выбрать опцию «Установка из указанного места» и нажать кнопку «Далее», после чего появится следующее окно (рис. 2.2.Л), где мастер установки нового оборудования попросит задать параметры поиска.

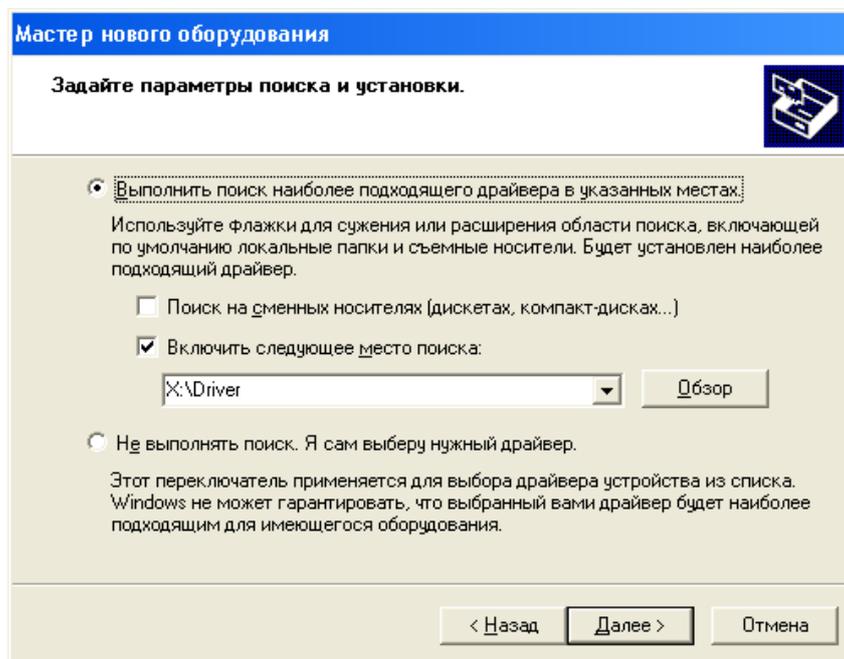


Рис. 2.2.Л. Окно задания параметров поиска драйвера

Здесь следует выбрать параметры «Выполнить поиск наиболее подходящего драйвера в указанных местах» и «Включить следующее место поиска:», а в строке ввести: **X:\Driver**, где X – буквенное обозначение вашего привода компакт-дисков в котором находится установочный диск с «Astroma SecretKey». При установке «Astroma SecretKey» копия драйвера создается в месте, куда Вы установили программу, поэтому в строке так же можно ввести: **x:\Program Files\Astroma Ltd.\SecretKey\Driver**, где x – диск Вашего компьютера, на который Вы установили «Astroma SecretKey». После этого нажмите кнопку «Далее». Мастер установки

нового оборудования произведет копирование необходимых файлов в системные папки, процесс которого будет отображаться в окне, показанном на рис. 2.2.М.

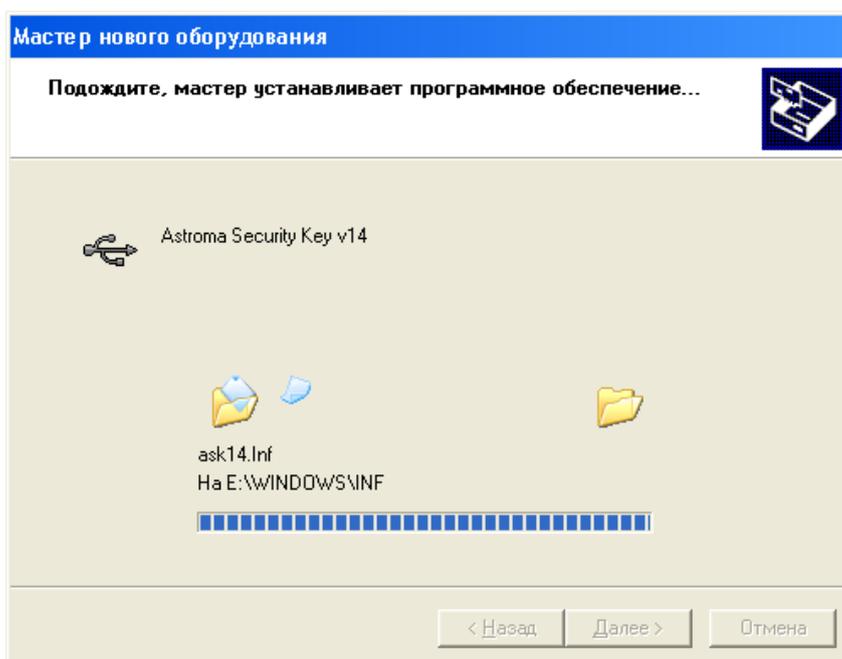


Рис. 2.2.М. Окно хода выполнения процесса установки драйвера

После завершения процесса копирования на экране появится окно, изображенное на рис. 2.2.Н.

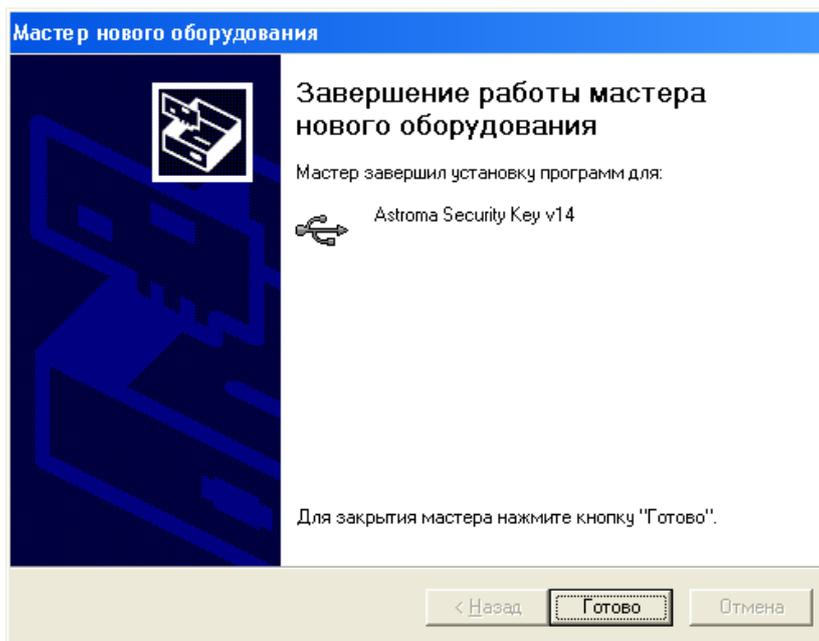


Рис. 2.2.Н. Окно завершения процесса установки драйвера

В форме, представленной на рис. 2.2.Н, следует нажать кнопку «Готово». На этом установка драйвера завершается. После установки драйвера программа «**Astroma SecretKey**» полностью готова к работе. Для проверки правильности установки драйвера и корректности работы USB-ключа можно воспользоваться утилитой «Диспетчер устройств» (рис. 2.2.О).

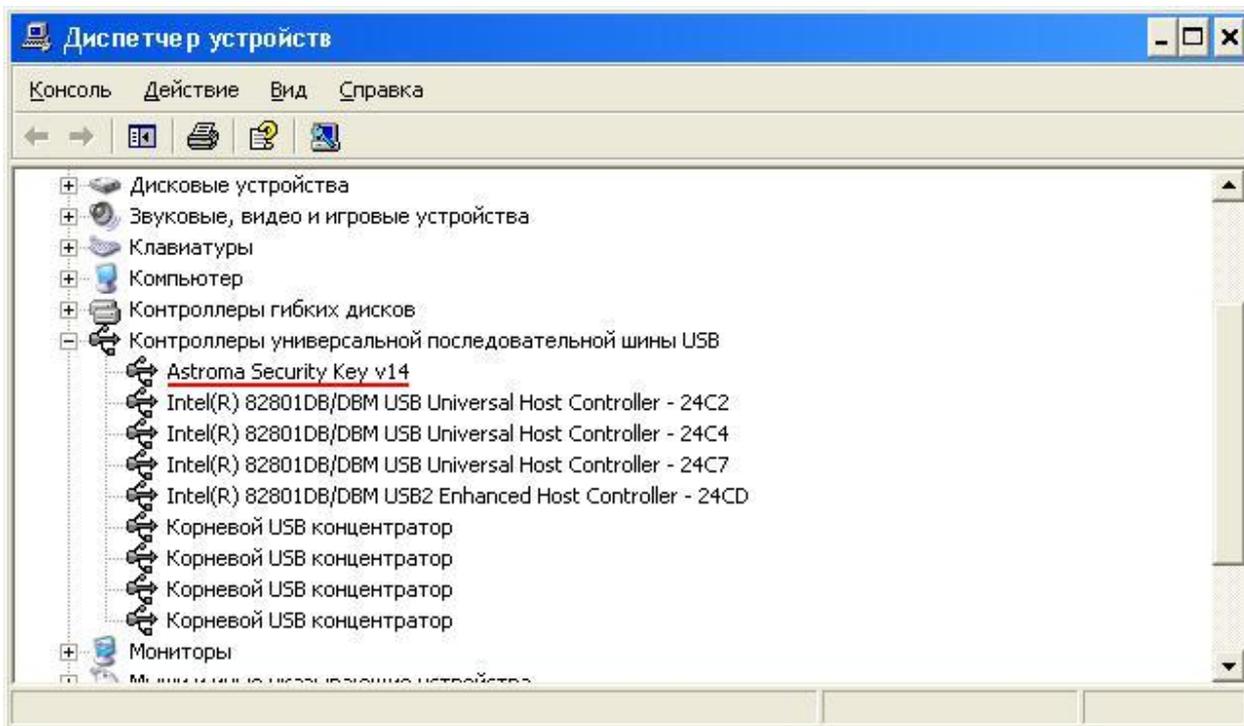


Рис. 2.2.О. Окно утилиты «Диспетчер устройств»

В списке входящих в систему устройств должно появиться устройство «**Astroma Security Key**» подчеркнутое на рис. 2.2.О красным цветом.

2.3 Задание/изменение пароля доступа к USB-ключу

Пароль необходим для предотвращения несанкционированного доступа к информации, в случае, если USB-ключ окажется в руках человека, не имеющего прав доступа. Пароль представляет собой строку длиной до 8-ми произвольных символов (цифр, букв и других символов), причем строчные и прописные буквы считаются разными символами.

Запустите программу «**Astroma SecretKey**». На экране появится главное окно программы (рис. 2.3.А), с просьбой ввести пароль для разблокировки USB-ключа. Если USB-ключ ранее не использовался и пароль в нем не задан, то в окне запроса пароля следует просто нажать кнопку «Ввести».

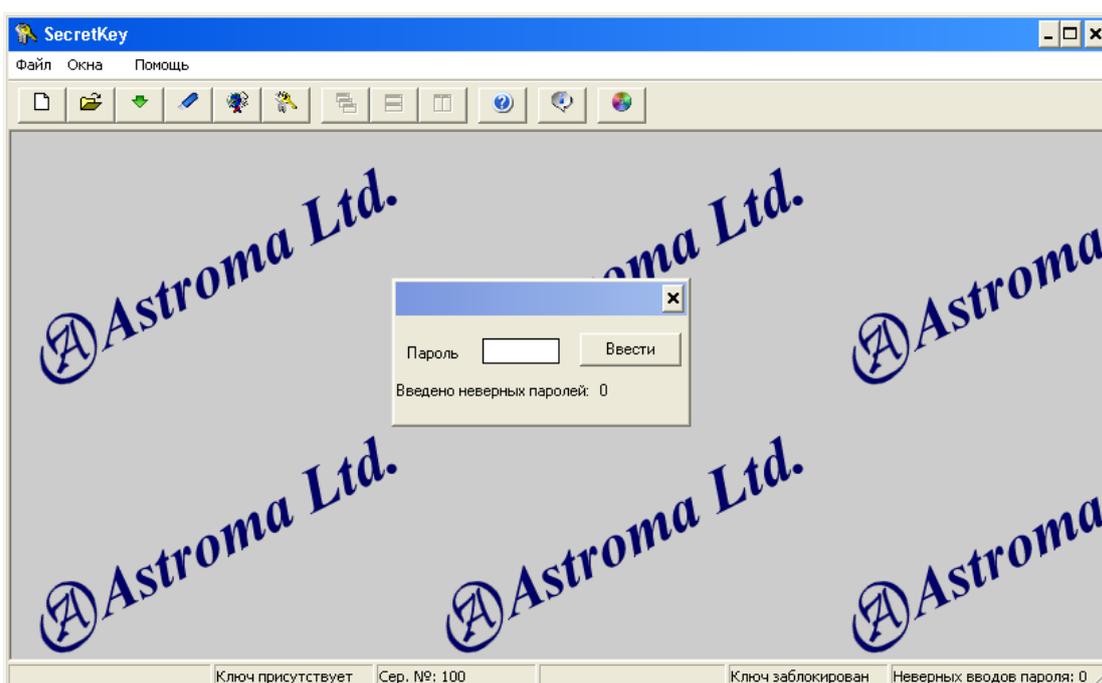


Рис. 2.3.А. Окно утилиты «Диспетчер устройств»

Окно запроса пароля исчезнет. Для задания пароля нажмите на панели инструментов главного окна «Astroma SecretKey» кнопку  (см. рис. 2.3.А). На экране появится окно изменения пароля доступа к ключу, изображенное ниже (рис. 2.3.Б). В поле «Текущий пароль» ничего вводить не следует, если ранее пароль не задавался, иначе необходимо ввести текущий пароль доступа. В поле «Новый пароль» введите пароль, который Вы желаете установить, а в поле «Подтверждение пароля» повторите этот же пароль еще раз, после чего нажмите кнопку «Обновить».

Если все значения были заданы верно, то по нажатию кнопки «Обновить» произойдет запись нового пароля в память USB-ключа, и доступ к ключу будет возможен уже только с использованием нового пароля. Если же при вводе была допущена ошибка, программа выдаст сообщение о ней. После исправления ошибки снова следует нажать кнопку «Обновить» для задания нового значения пароля.

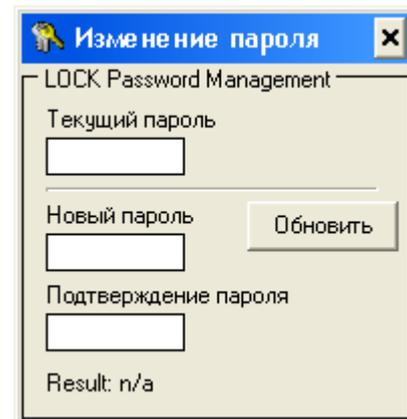


Рис.2.3.Б. Окно изменения пароля

2.4 Генерация ключа шифрования

Ключ шифрования представляет собой уникальную последовательность случайных значений, посредством которой производится шифрование и дешифрование информации. Доступ к зашифрованной информации возможен лишь в том случае, если имеется корректный ключ шифрования, следовательно, он должен всегда держаться в секрете, что и обеспечивает USB-ключ. Хранящийся в его памяти ключ шифрования не может быть оттуда прочитан.

Для генерации ключа шифрования следует на панели инструментов (см. рис. 2.3.А) нажать на кнопку . После этого на экране появится окно «Генерация ключа шифрования», представленное на рис. 2.4.В.

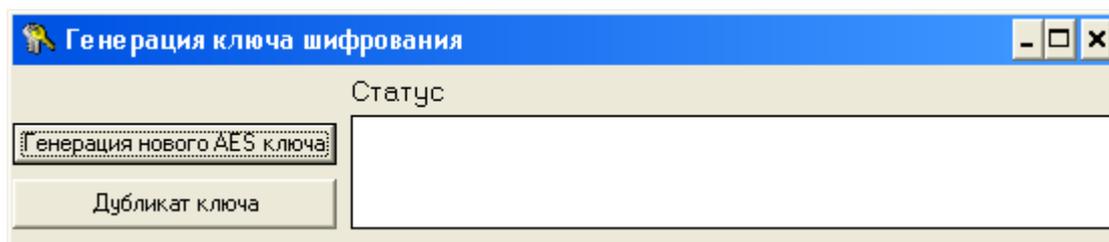


Рис. 2.4.В. Окно формирования ключа шифрования «Astroma SecretKey»

Данное окно предназначено для:

- генерации нового ключа шифрования (кнопка «Генерация нового AES ключа»;
- создания дубликатов USB-ключей (кнопка «Дубликат ключа»).

Чтобы произвести генерацию ключа шифрования следует нажать кнопку «Генерация нового AES ключа». Если USB-ключ ранее не использовался, и в его памяти нет ключа шифрования, то на экране появится окно, изображенное на рис. 2.4.Д. В случае же, если какой либо ключ шифрования присутствует в памяти USB-ключа, на экране отобразится предупреждение, что имеющийся ключ шифрования будет уничтожен. Это означает, что вся информация, ранее зашифрованная при помощи данного ключа шифрования, после генерации нового ключа станет в дальнейшем недоступной. Для отмены генерации нового ключа шифрования следует нажать кнопку «Нет». Если же действительно нужно произвести генерацию нового ключа, нажмите кнопку «Да».

Новый ключ шифрования будет записан в USB-ключ, откуда его в дальнейшем невозможно извлечь. Поэтому Вам будет предложено сохранить копию ключа шифрования (рис. 2.4.Д).

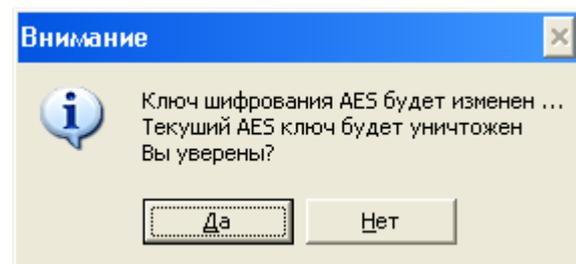


Рис. 2.4.Г. Предупреждение при генерации нового ключа шифрования.

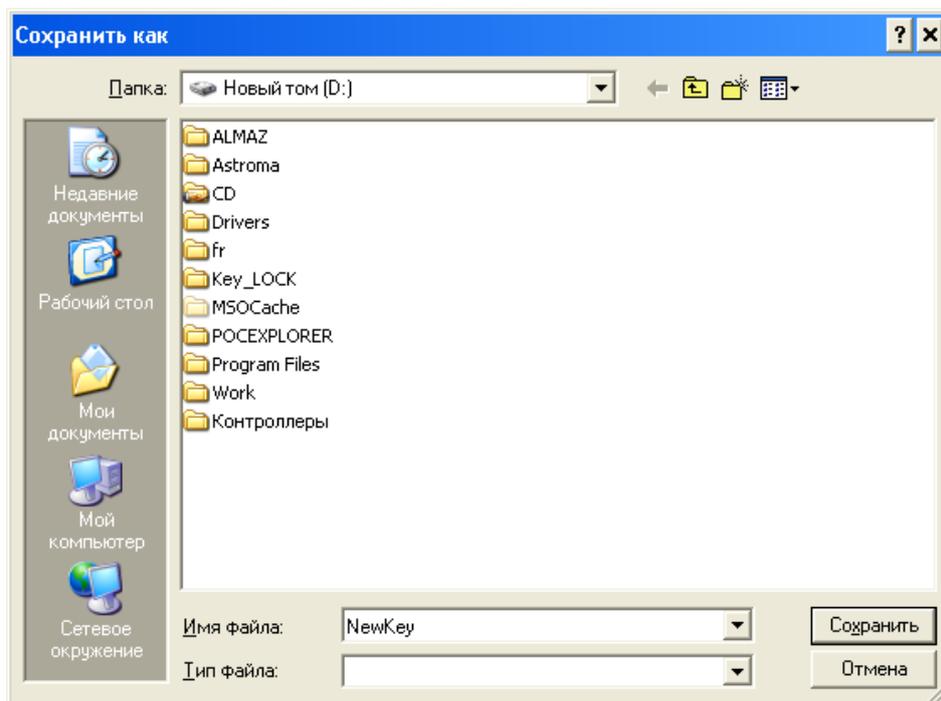


Рис. 2.4.Д. Окно выбора файла для сохранения копии ключа шифрования

Копия ключа шифрования может понадобиться в дальнейшем для создания дубликатов USB-ключа. Потребность в дубликатах может возникнуть при утрате оригинала USB-ключа, либо в случае необходимости доступа к информации нескольких лиц.

Если Вы решили сохранить копию ключа шифрования, выберите носитель и папку, затем задайте имя файла без расширения и нажмите кнопку «Сохранить» (см. рис. 2.4.Д). Копия ключа шифрования будет сохранена на указанном Вами носителе в указанной папке с заданным Вами именем файла и расширением «.aes».

ВНИМАНИЕ!!! Избегайте сохранения копий ключей шифрования на жестких дисках компьютера! Используйте для этих целей съемные носители, которые после извлечения следует хранить в недоступном для посторонних месте!

При нажатии кнопки «Отмена» (см. рис. 2.4.Д) копия ключа шифрования сохранена не будет, а его оригинал будет сохранен только в памяти USB-ключа, откуда его прочитать невозможно. В этом случае при утрате USB-ключа доступ к зашифрованной с его помощью информации будет в дальнейшем невозможен.

По завершении генерации нового ключа шифрования в окне «Генерация ключа шифрования» появится сообщение об удачном завершении процесса (Рис. 2.4.Е).

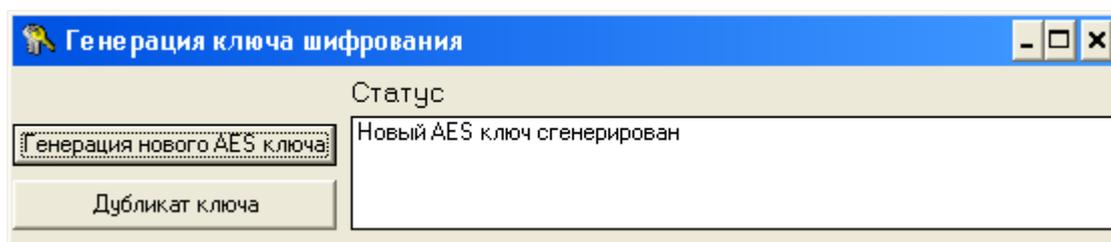


Рис. 2.4.Е. Сообщение об удачном завершении генерации нового ключа шифрования

3. Работа с «Astroma SecretKey»

Подключите USB-ключ к компьютеру и запустите программу «Astroma SecretKey». На экране появится главное окно приложения, с просьбой ввести пароль для разблокировки USB-ключа (см. рис. 2.3.А). Введите пароль и нажмите кнопку «Ввести».

ВАЖНО!!! После трех подряд сделанных попыток ввода неверного пароля ключ шифрования, находящийся в памяти USB-ключа, будет уничтожен, что обеспечит невозможность дальнейшего доступа к зашифрованной информации с использованием

данного USB-ключа, пока дубликат уничтоженного ключа шифрования не будет загружен в устройство заново.

Если пароль введен правильно, то USB-ключ будет разблокирован для дальнейшей работы с ним, о чем будет свидетельствовать надпись «Ключ разблокирован» в правом нижнем углу окна (рис. 3.A).

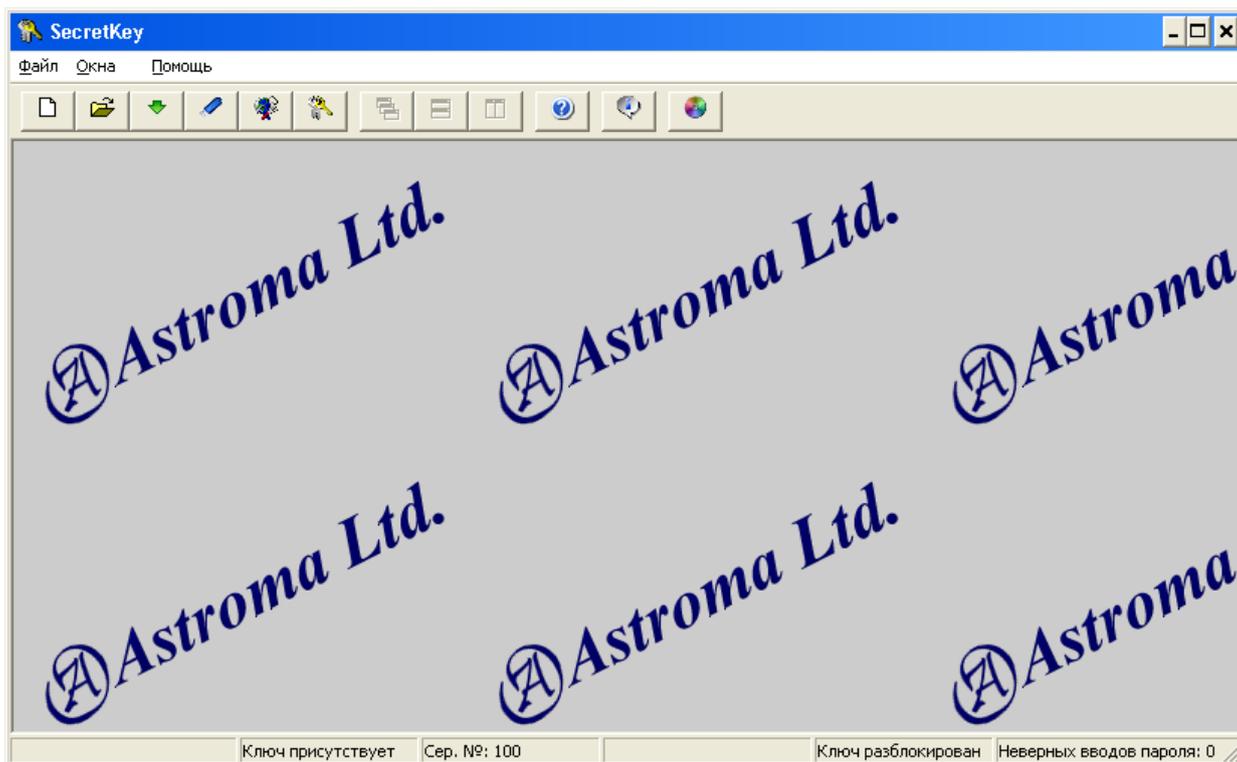


Рис. 3.A. Главное окно «Astroma SecretKey» после снятия блокировки с USB-ключа

3.1 Создание зашифрованных файлов

Для создания зашифрованного файла на панели инструментов «Astroma SecretKey» (см. рис. 2.3.A) нажмите кнопку . На экране появится окно выбора файла, подлежащего шифрованию (рис. 3.1.A).

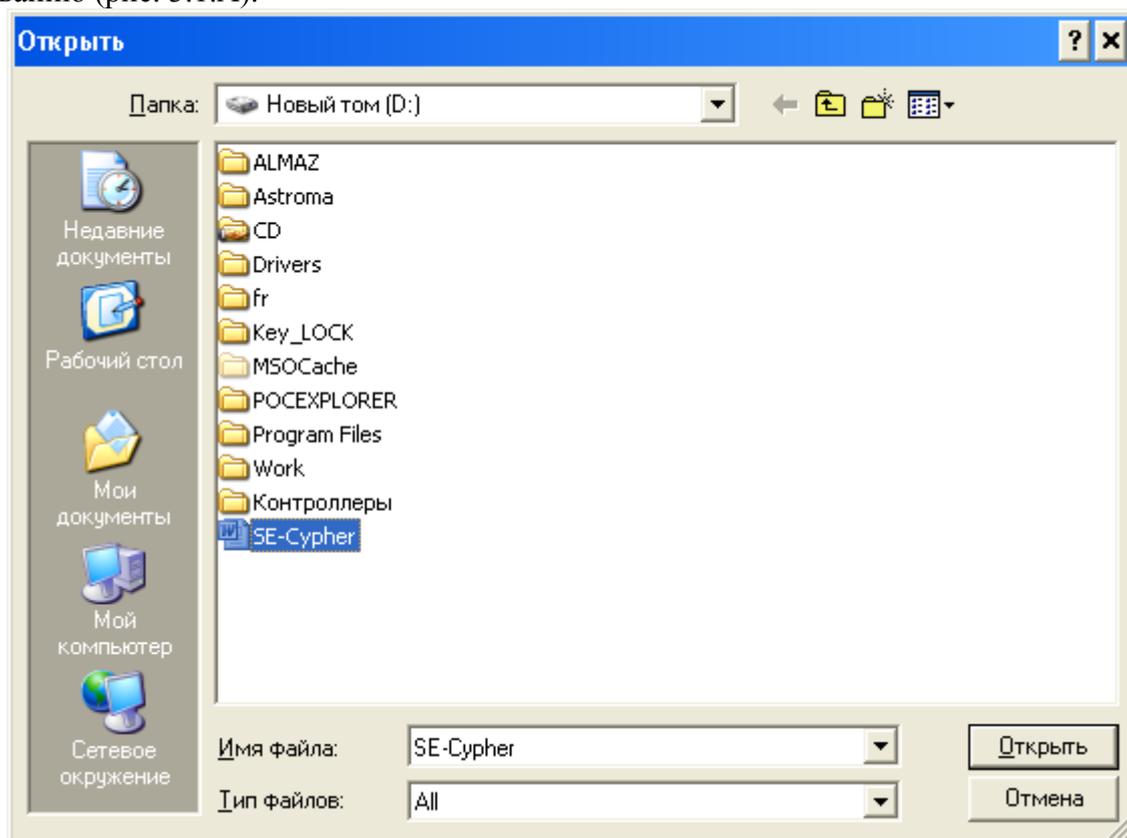


Рис. 3.1.А. Окно выбора незашифрованного файла

Выберите из списка необходимый файл и нажмите кнопку «Открыть». После этого на экране появится окно, показанное ниже, где Вам будет предложено указать, куда необходимо сохранить выбранный файл, но уже в зашифрованном виде (см. рис. 3.1.Б).

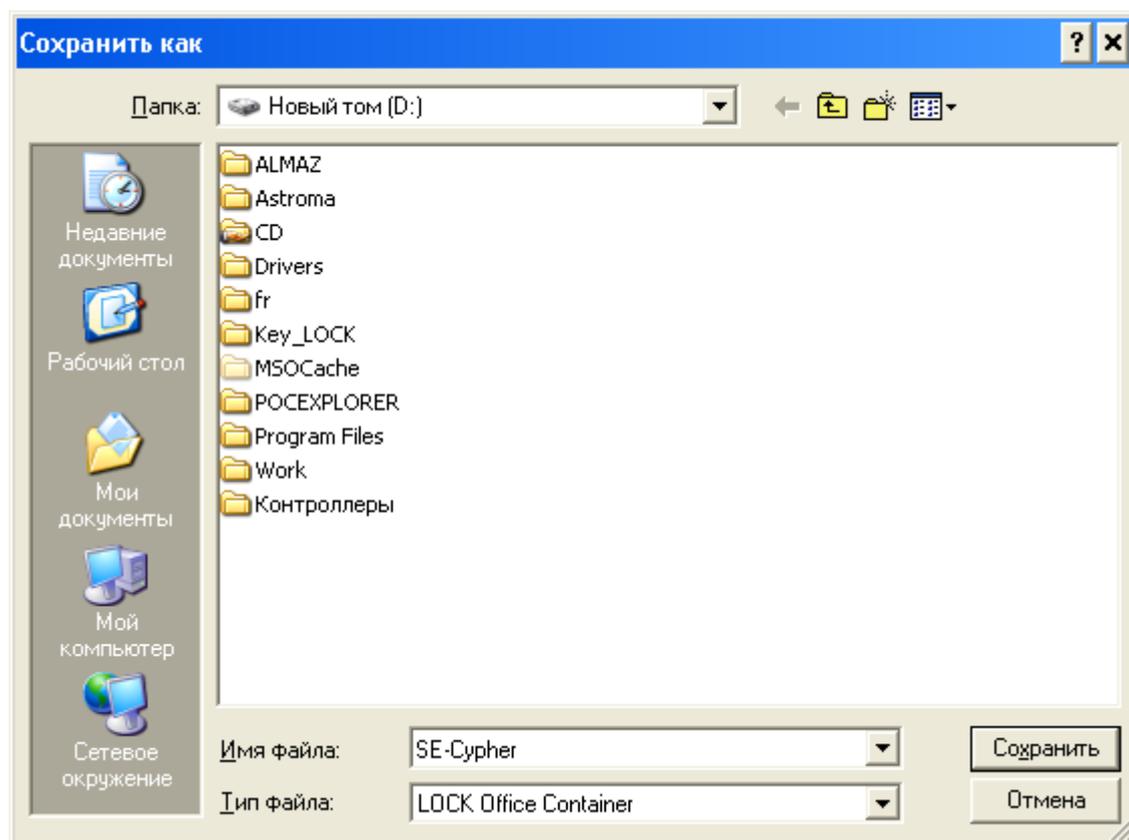


Рис. 3.1.Б. Окно выбора каталога для сохранения зашифрованного файла

Выберите папку и укажите имя файла, под которым Вы хотите его сохранить. Тип файла указывать не следует, так как «Astroma SecretKey» автоматически присвоит файлу тип «office_lock». Далее нажмите кнопку «Сохранить». Если Вы хотите отменить процедуру создания зашифрованного файла, это можно сделать путем нажатия кнопки «Отмена». После сохранения зашифрованного файла Вам будет предложено удалить исходный незашифрованный файл (рис. 3.1.В).

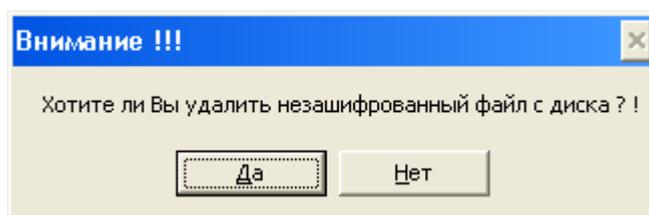


Рис. 3.1.В. Предложение об удалении исходного незашифрованного файла

Если Вы не хотите его удалять, например, исходный файл хранится на съемном носителе, нажмите кнопку «Нет». Для удаления следует нажать кнопку «Да». Процедура удаления не просто делает пометку, что файл удален, а производит запись бессмысленных данных поверх файла, разрушая информацию, и затем уже удаляет файл.

ВАЖНО!!! Рекомендуется удаление исходных файлов с жёсткого диска ПК, иначе шифрование становится бессмысленным.

3.2 Работа с зашифрованными файлами

Для открытия зашифрованного файла на панели инструментов «Astroma SecretKey» (см. рис. 2.3.А) следует нажать на кнопку . На экране появится окно выбора файла, показанное ниже (рис. 3.2.А).

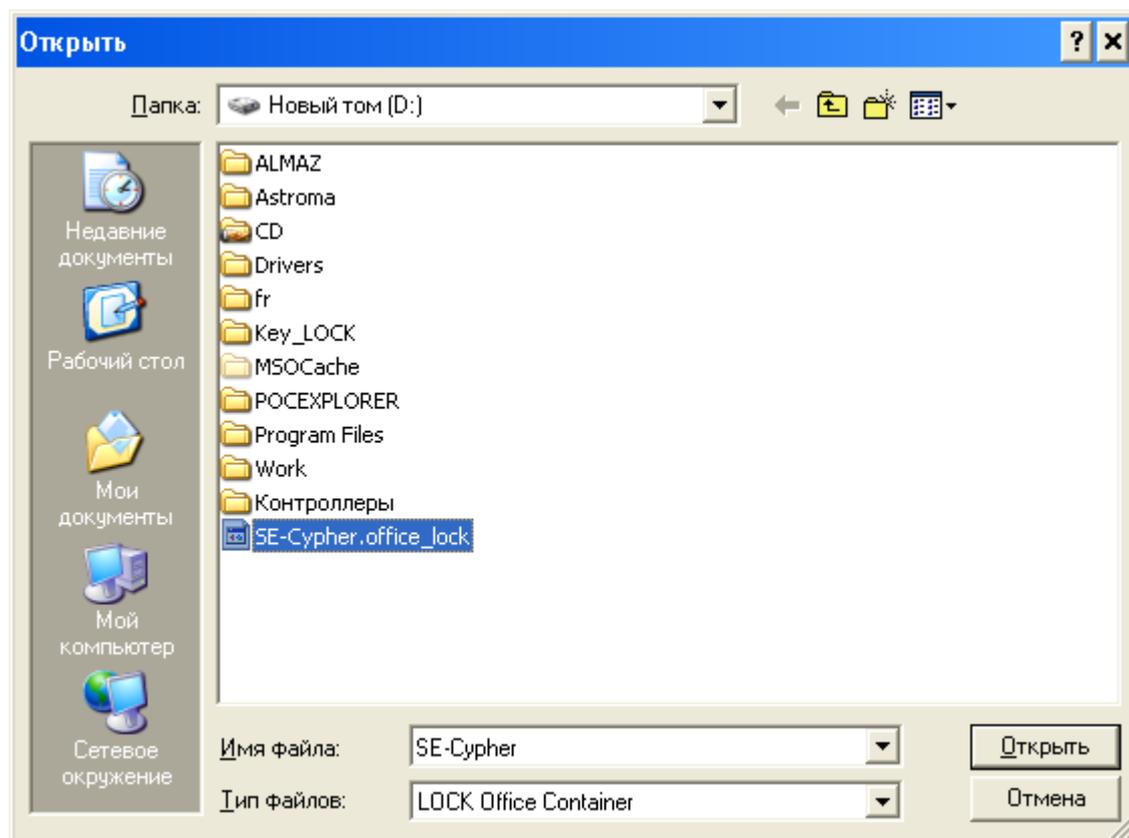


Рис. 3.2.А. Окно выбора зашифрованного файла

Выберите требуемый файл и нажмите кнопку «Открыть». В зависимости от типа исходного зашифрованного файла, автоматически произойдет запуск приложения, обрабатывающего файлы данного типа. Например, для файлов с расширением «.doc» будет запущен Microsoft Word, а с расширением «.xls» - Microsoft Excel и т.д.

На рис. 3.2.Б показано окно с открытым документом Microsoft Word, который был ранее зашифрован, а затем открыт посредством «Astroma SecretKey». Дальнейшая работа с документом производится обычным образом.

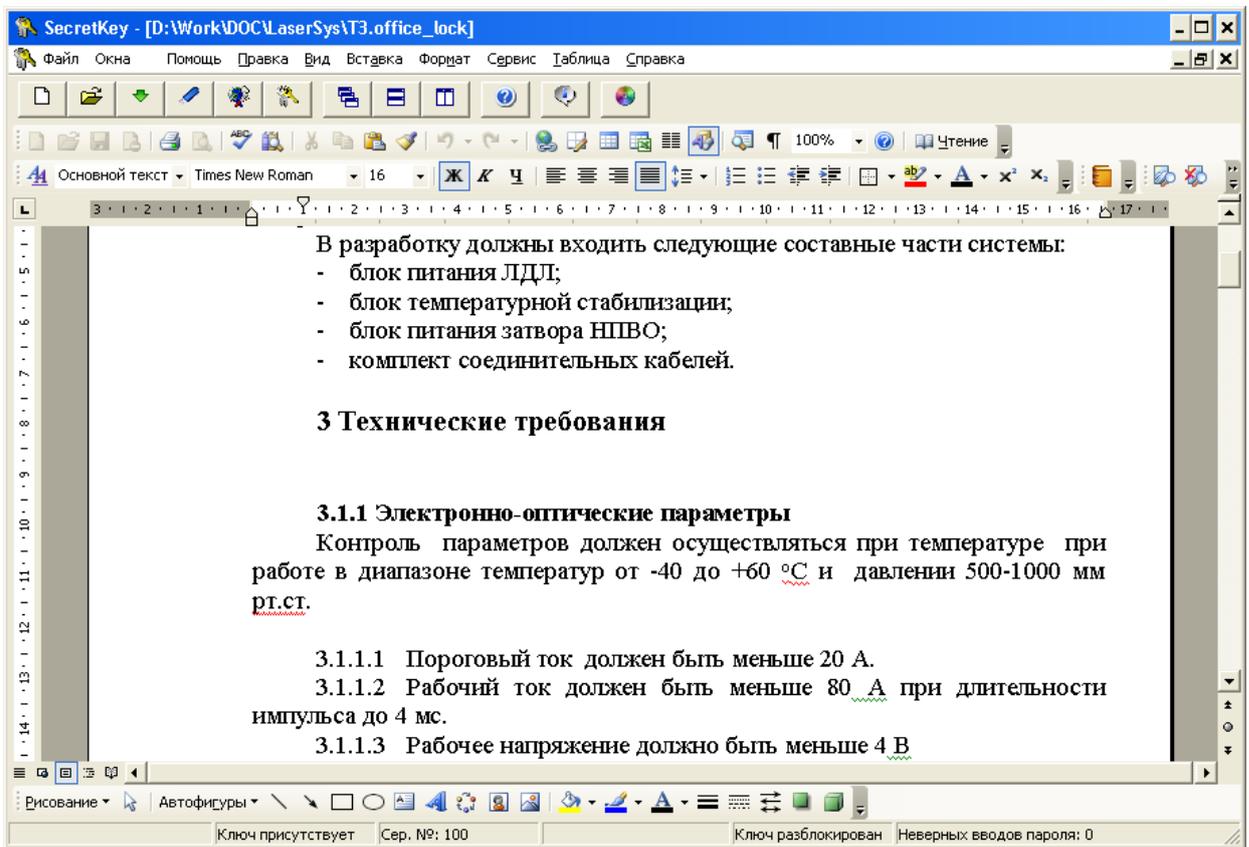


Рис. 3.2.Б. Работа с зашифрованным файлом.

Попытка расшифровки файла с использованием USB-ключа, содержащего неверный ключ шифрования, делает невозможным работу с этим файлом.

3.3 Создание дубликата USB-ключа

Потребность в создании дубликатов USB-ключей может возникнуть в случае утраты оригинального USB-ключа, или при необходимости обеспечения доступа к информации нескольких лиц, например, для организации обмена зашифрованными файлами по электронной почте.

Необходимыми условиями для создания дубликата USB-ключа является наличие:

- USB-ключа «LOCK», предназначенного для работы в системе «**Astroma SecretKey**» (см. п. 2);
- Файла с копией ранее сгенерированного ключа шифрования (см. п. 2.4), содержащегося в памяти USB-ключа-оригинала.

Для создания дубликата USB-ключа следует на панели инструментов «**Astroma SecretKey**» (см. рис. 2.3.А) нажать на кнопку . После этого на экране появится окно «Генерация ключа шифрования», представленное на рис.2.4.В. В нем необходимо нажать кнопку «Дубликат ключа». При этом в USB-ключ, предназначенный для создания копии, должен быть записан тот же ключ шифрования, что содержится в памяти оригинального USB-ключа. Для подтверждения правильности этого действия Вам будет сделан запрос (рис. 2.4.Г).

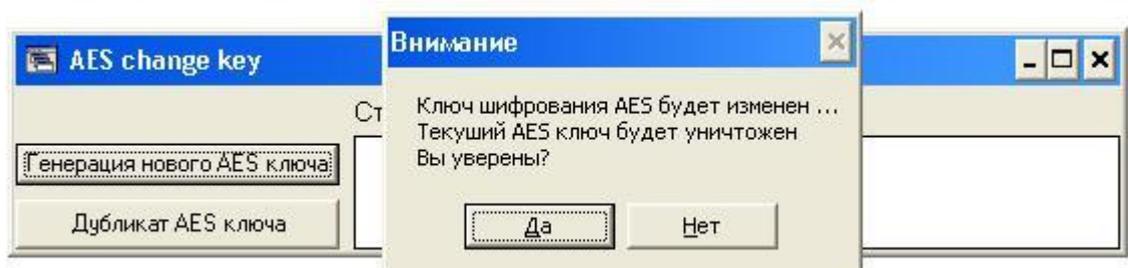


Рис. 3.3.А. Запрос о подтверждении генерации нового ключа шифрования

В случае положительного ответа на экране появится окно выбора файла (рис. 3.3.Б), содержащего ранее созданную копию ключа шифрования, используемого в USB-ключе-оригинале.

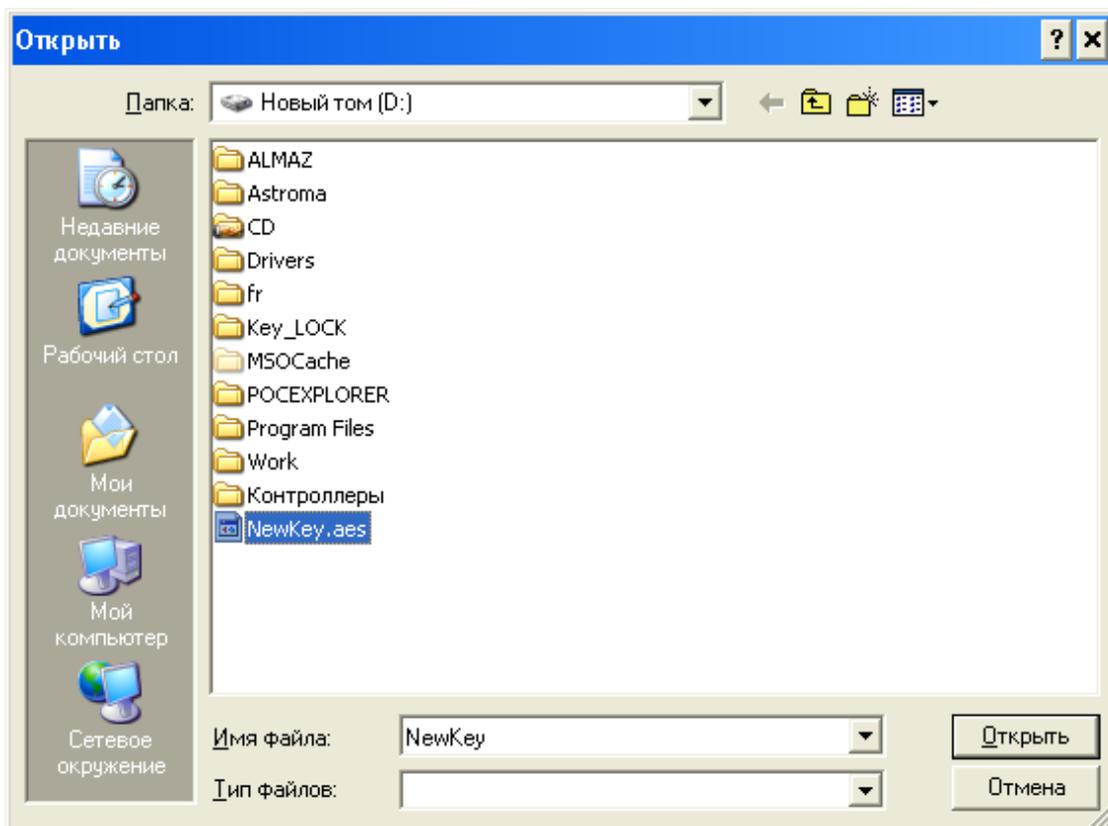


Рис. 3.3.Б Выбор файла, содержащего ранее созданную копию ключа шифрования

Выберите необходимый файл и нажмите кнопку «Открыть». При этом ключ шифрования будет загружен в память USB-ключа, и дубликат будет готов к работе. В случае же нажатия кнопки «Отмена» дубликат USB-ключа создан не будет, и при этом в памяти USB-ключа сохранится прежний ключ шифрования.

3.4 Перешифровка файлов

Иногда возникает необходимость в перешифровке информации на новый ключ шифрования. Это может потребоваться, например, когда существует предположение, что постороннее лицо каким-либо образом завладело ключом шифрования (именно ключом шифрования, а не USB-ключом). К тому же периодическая смена ключа шифрования полезна просто в целях профилактики, а точнее для большей уверенности, что информация остается надежно защищенной.

Для процедуры перешифровки файлов требуется два USB-ключа и два свободных USB-порта ПК. Один USB-ключ должен хранить в памяти текущий ключ шифрования, то есть ключ, с помощью которого на данный момент зашифрована информация, и второй USB-ключ с новым ключом шифрования.

Для перешифровки начните в соответствии с разделом 3 работу с программой «**Astroma SecretKey**» первым USB-ключом, хранящим в памяти текущий ключ шифрования. На панели инструментов «**Astroma SecretKey**» (см. рис. 2.3.А) следует нажать на кнопку . На экране появится окно, с просьбой подключить второй USB-ключ (см. рис. 3.4.А). В ответ на это вставьте второй USB-ключ в свободный порт и затем нажмите кнопку ОК. Далее повторно нажмите кнопку . На экране появится запрос пароля доступа ко второму USB-ключу. Введите пароль и нажмите кнопку «Ввести». После этого на экране появится окно, показанное на рис. 3.4.Б.

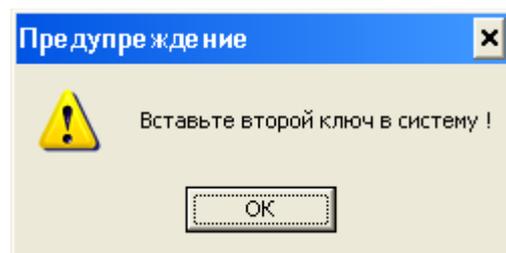


Рис. 3.4.А.

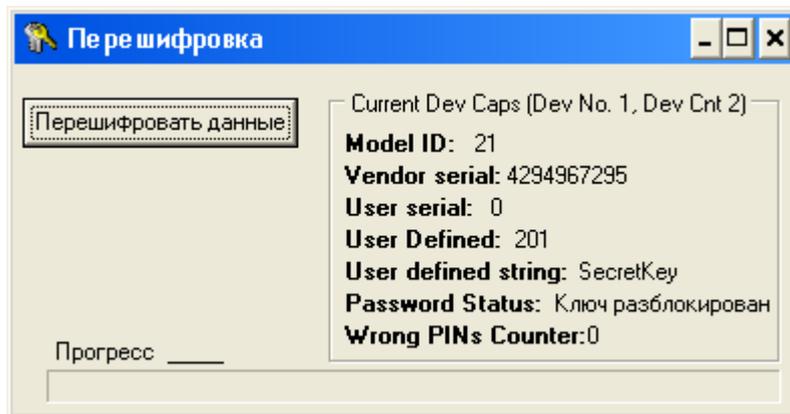


Рис. 3.4.Б.

Нажмите кнопку «Перешифровать данные». Для подтверждения правильности этого действия на экране появится предупреждение с запросом (см. рис. 3.4.В).

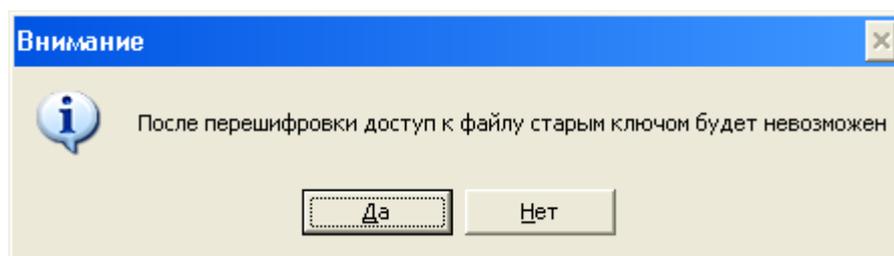


Рис. 3.4.В.

Для отмены процедуры перешифровки следует нажать кнопку «Нет». В случае положительного ответа выводится окно, где будет предложено выбрать файл, который требуется перешифровать (см. рис. 3.4.Г.).

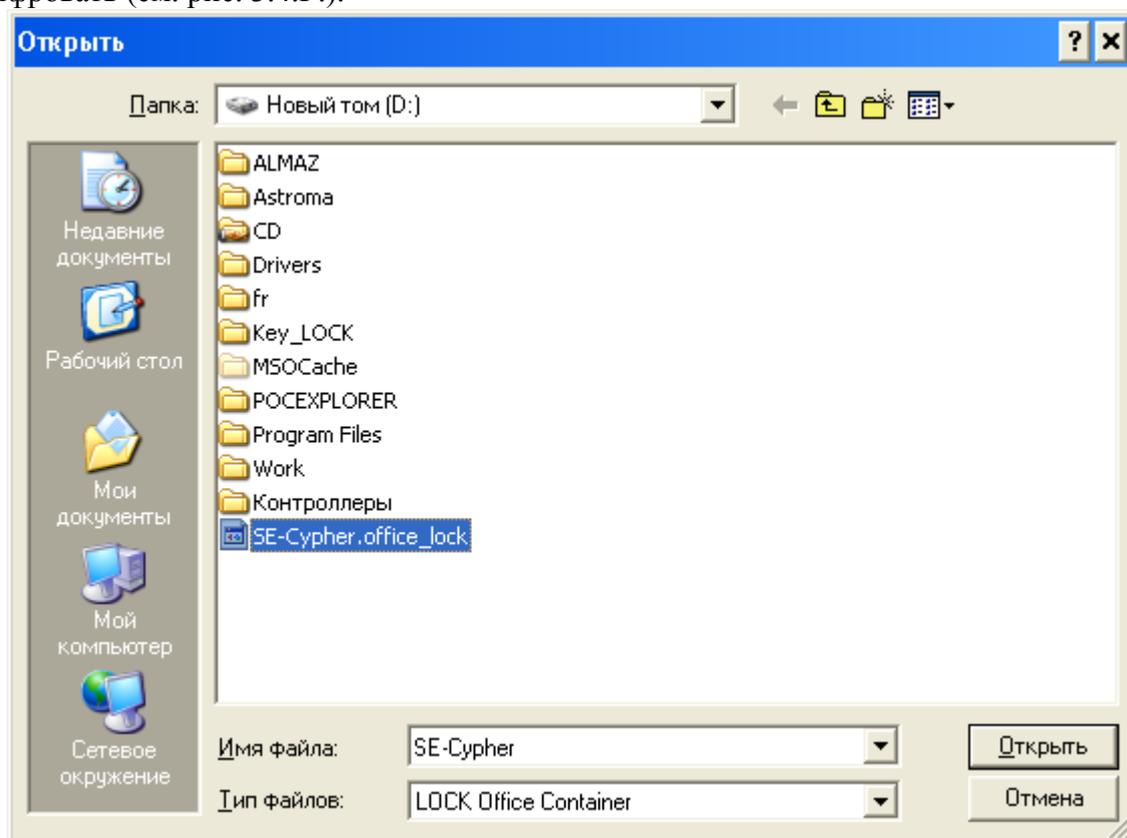


Рис. 3.4.Г. Окно выбора файла для перешифровки.

Здесь возможно отказаться от процедуры перешифровки, нажав кнопку «Отмена». Для продолжения следует выбрать из списка необходимый файл и нажать кнопку «Открыть». Программа произведет перешифровку указанного файла на новый ключ шифрования. При этом зашифрованный файл, будет расшифровываться первым USB-ключом и зашифровываться вторым. Процесс перешифровки показан на рис. 3.4.Д.



Рис. 3.4.Д. Процесс перешифровки файла на новый ключ шифрования.

После завершения перешифровки всех необходимых файлов для продолжения работы отключите один из USB-ключей (любой), затем закройте окно «Перешифровка». Попытка выхода из режима перешифровки с двумя подключенными USB-ключами вызовет появление предупреждения, показанного на рис. 3.4.Е.

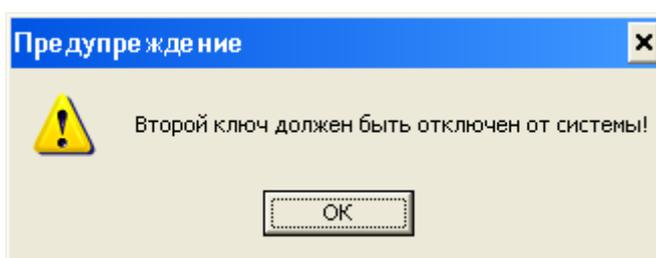


Рис. 3.4.Е. Некорректный выход из режима перешифровки.

В ответ на это отключите один из USB-ключей и нажмите кнопку «ОК», после чего закройте окно режима перешифровки файлов (см. рис. 3.4.Б).

3.5 Расшифровка файлов

Если нет необходимости в дальнейшем хранить какие-то файлы в зашифрованном виде, но информация, хранящаяся в них, еще востребована, такие файлы могут быть расшифрованы и записаны на носитель информации в открытом виде. Для процедуры расшифровки файла на панели инструментов «Astroma SecretKey» (см. рис. 2.3.А) следует нажать кнопку . После ее нажатия на экране отобразится окно для выбора зашифрованного файла (см. рис. 3.2.А), а после выбора такого файла Вам будет предложено указать файл, в котором будет сохранена незашифрованная информация (см. рис. 3.1.А).

ВАЖНО!!! При задании имени незашифрованного файла необходимо указывать тип файла (расширение), чтобы Windows в дальнейшем могла знать, какое приложение необходимо использовать для обработки данного файла. Так, например, для документов Microsoft Word следует указывать тип «.doc», для документов Microsoft Excel – тип «.xls», и т. д.