



Средство криптографической защиты информации

АККОРД-У

Руководство по эксплуатации

11443195.4012-023

Листов 49

Москва

2010

АННОТАЦИЯ

Настоящий документ является руководством по установке и эксплуатации средства криптографической защиты информации Аккорд-У (далее по тексту – Аккорд-У).

В документе приведены общие сведения об Аккорд-У, его основные функции, особенности установки и эксплуатации.

Перед установкой и эксплуатацией Аккорда-У необходимо внимательно ознакомиться с настоящим руководством.

Применение Аккорда-У должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ (РС).

Поскольку работы по развитию функциональности Аккорда-У продолжаются, в документации могут наблюдаться незначительные несоответствия в части описания пользовательского интерфейса.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	4
1.1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ	4
1.2. ТЕХНИЧЕСКИЕ УСЛОВИЯ ПРИМЕНЕНИЯ КОМПЛЕКСА	5
1.3. ОРГАНИЗАЦИОННЫЕ МЕРЫ	6
1.4. КОМПЛЕКТ ПОСТАВКИ	6
2. УСТАНОВКА И НАСТРОЙКА УСТРОЙСТВА АККОРД	7
2.1. ПОДКЛЮЧЕНИЕ АППАРАТНОЙ ЧАСТИ КОМПЛЕКСА – УСТРОЙСТВА АККОРД.....	7
УСТАНОВКА СИСТЕМОГО ДРАЙВЕРА УСТРОЙСТВА АККОРД	8
2.3. УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АККОРДА-У.....	11
2.4. ИНИЦИАЛИЗАЦИЯ И ФОРМАТИРОВАНИЕ ДАННЫХ КРИПТОГРАФИЧЕСКОЙ ПОДСИСТЕМЫ УСТРОЙСТВА АККОРД.....	15
2.5. УСТАНОВКА PIN-КОДА ДЛЯ КРИПТОГРАФИЧЕСКОЙ ПОДСИСТЕМЫ УСТРОЙСТВА АККОРД	23
2.6. РАЗБЛОКИРОВАНИЕ КРИПТОГРАФИЧЕСКОЙ ПОДСИСТЕМЫ УСТРОЙСТВА АККОРД.....	25
2.7. ВЕДЕНИЕ ВНУТРЕННЕГО ЖУРНАЛА РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ	27
3. ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКОЙ ПОДСИСТЕМЫ УСТРОЙСТВА АККОРД.....	28
3.1. ШИФРОВАНИЕ И ПОДПИСЬ ФАЙЛОВ НА ЖЕСТКОМ ДИСКЕ.....	28
3.1.1. Работа с ключами	28
3.1.2. Шифрование файлов на диске.....	39
3.1.3. Подпись файлов на диске.....	42
ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА	45
КОНТАКТЫ.....	46
ПРИЛОЖЕНИЕ 1. ВОЗМОЖНЫЕ ЗАТРУДНЕНИЯ ПРИ РАБОТЕ С АККОРД-У И СПОСОБЫ ИХ РЕШЕНИЯ	47
ПРИЛОЖЕНИЕ 2. ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ПО СКЗИ АККОРД-У.....	48

1. Общие сведения

1.1. Назначение и особенности защитных функций

Средство криптографической защиты информации Аккорд-У – это плата расширения, в которой аппаратно реализован набор алгоритмов защиты информации, а также набор драйверов и библиотек для использования криптографических функций в различных прикладных программах. Аккорд-У предназначен для применения на ПЭВМ (рабочих станциях и терминалах ЛВС) типа IBM PC, функционирующих под управлением ОС Microsoft Windows 2000/XP/2003/Vista/2008/7.

Аккорд-У базируется на контроллере Аккорд-АМДЗ, поэтому совмещает криптографическую функциональность с функциями обеспечения доверенной загрузки операционной системы.

ВНИМАНИЕ! При использовании Аккорда-У, соответствующего классу KB2, при каждом старте системы к USB-хосту контроллера *обязательно должно быть* подключено ПСКЗИ ШИПКА, которое использовалось при форматировании Аккорда-У.

Аккорд-У может использоваться:

- для **шифрования и/или подписи файлов** на жестком диске ПЭВМ или съемных носителях (флоппи дисках, USB флэш-дисках и др.). При этом ключевая информация генерируется и хранится в устройстве ШИПКА, а криптографические преобразования выполняются внутренним ПО, что исключает передачу ключевой информации в оперативную память ПЭВМ;
- для обеспечения доверенной загрузки операционной системы;
- для защищенного **хранения ключей** шифрования и подписи и в качестве аппаратного **датчика случайных чисел**;
- для защиты **информационных технологий** с помощью защитных кодов аутентификации.

Комплекс Аккорд-У включает:

- I. Контроллер Аккорд на базе контроллера Аккорд-5.5 или Аккорд-5.5.e с USB-хостом;

- II. Кабель соединительный, тип miniUSB (A) - AM (0,9 -1,0 м);
- III. USB-устройство ПСКЗИ ШИПКА;
- IV. Специальное ПО для ПСКЗИ ШИПКА, устанавливаемое на жесткий диск компьютера (см. «Руководство администратора» (11443195.4012-022 90 01));
- V. Устройство отключения питания EATX;
- VI. Специальное ПО, устанавливаемое на жесткий диск компьютера:
 - драйвер Аккорда-У для работы в операционных системах Microsoft Windows 2000/XP/2003;
 - библиотека для доступа к функциям Аккорд-У с уровня прикладного ПО;
 - набор программ для назначения параметров авторизации и инициализации (форматирования) устройства;
 - набор программ для шифрования, подписи файлов на жестком диске;
 - криптопровайдер ГОСТ – специальная библиотеки для доступа алгоритмам ГОСТ через функции CryptoAPI с уровня прикладного программного обеспечения Windows;
 - библиотеку поддержки стандарта PKCS#11.

Аккорд-У имеет следующие ресурсы:

1. Аппаратную реализацию российских криптографических алгоритмов:
 - ❖ шифрование (ГОСТ 28147-89),
 - ❖ вычисление хэш-функции (ГОСТ Р 34.11-94),
 - ❖ вычисление и проверка ЭЦП (ГОСТ Р 34.10-2001),
 - ❖ имитовставка (ГОСТ 28147-89),
 - ❖ вычисление и проверка ЗКА (защитных кодов аутентификации).
2. Реле коммутации внешних устройств до 3-х штук.
3. Внутреннюю энергонезависимую память объемом 4 Кбайт для хранения критичной ключевой информации непосредственно в вычислителе.
4. Отдельный блок памяти объемом 512 Кбайт для хранения дополнительной ключевой информации, паролей, сертификатов и т.п.
5. Встроенный аппаратный генератор случайных чисел.

1.2. Технические условия применения комплекса

Для использования Аккорда-У требуется следующий минимальный состав технических и программных средств:

- установленная операционная система Microsoft Windows 2000/XP/2003;

- свободный слот PCI или PCI-Express;

- объем дискового пространства для размещения программного обеспечения на жестком диске ПЭВМ – около 30 Мбайт.

1.3. Организационные меры

Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов **необходимы:**

- физическая охрана ПЭВМ и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;

- наличие администратора безопасности информации (АБИ) – пользователя, имеющего особый статус и полномочия. Администратор БИ планирует мероприятия по защите информации, определяет права доступа пользователей в соответствии с утвержденным Планом защиты, организует установку комплекса в ПЭВМ, и эксплуатацию защищенной ПЭВМ, ведет учет выданных ТМ-идентификаторов, осуществляет периодическое тестирование комплекса;

- использование в ПЭВМ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ.

1.4. Комплект поставки

Аккорд-У поставляется в следующем составе:

- Контроллер Аккорд-АМДЗ с USB-хостом – 1 шт.
- Устройство отключения питания EATX – 1 шт.;
- USB-устройство ШИПКА – 1 шт.;
- Специальное ПО ПСКЗИ ШИПКА на CD – 1 шт.;
- Специальное ПО Аккорд-У на CD – 1 шт.;
- Эксплуатационная документация на CD;
- Формуляр – 1 брошюра;
- Руководство по быстрой установке ПСКЗИ ШИПКА – 1 брошюра;
- Руководство по быстрой установке Аккорд-У – 1 брошюра;

- Комплект упаковки.

По дополнительному заказу в комплект поставки может входить ПО Аккорд-NT/2000 V3.0.

2. Установка и настройка устройства АККОРД

Установка и настройка Аккорда-У производится в несколько этапов:

- 1) Установка аппаратной части комплекса в свободный слот материнской платы компьютера.
- 2) Установка системного драйвера Аккорда-У.
- 3) Установка ПО Аккорда-У
- 4) Настройка Аккорда-У (этот этап включает в себя инициализацию устройства, начальное форматирование и установку PIN-кода).

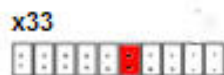
ВНИМАНИЕ! Устройство АККОРД формально представляет собой два независимых друг от друга устройства – АМДЗ и криптографическая подсистема. Использовать возможности криптографической подсистемы и АМДЗ можно как по отдельности, так и совместно, при этом работа с одной частью не влияет на работу другой.

2.1. Подключение аппаратной части комплекса – устройства АККОРД

Подключение устройства АККОРД осуществляется стандартным образом, т. е. установкой контроллера комплекса в свободный слот материнской платы ПЭВМ (РС) – см. «Руководство по установке» (11443195.4012-006 98 03).

ВНИМАНИЕ: Если на одном ПК планируется использование двух устройств АККОРД – первое как АМДЗ, а второе как криптографическое устройство, то для того чтобы устройства не конфликтовали, на втором необходимо

установить джампер в технологический разъем Х33 на шестую позицию слева:



Установка системного драйвера устройства АККОРД

ВНИМАНИЕ: Если Вы приобрели комплекс Аккорд-NT/2000 на базе Аккорд-У, то на диске с СПО «Аккорд-NT/2000» Вы обнаружите папку «АМДЗ», в которой будет также находиться драйвер для контроллера Аккорд. Однако необходимо установить не его, а именно тот драйвер, который находится на диске с СПО «Аккорд-У».

ВНИМАНИЕ! Для корректной установки драйвера необходимо идентифицироваться в операционной системе как пользователь с правами Администратора.

После включения компьютера, с установленным в соответствующий слот устройством АККОРД, операционная система обнаружит новое устройство. Если в настройках Вашей операционной системы включен режим автоматического обновления, то появляется предложение выполнить поиск подходящего драйвера в Интернете. Выбирайте опцию «Нет, не в этот раз» и нажмите кнопку «Далее». Запустится «Мастер нового оборудования» (Рис. 1). Следует выбрать пункт «Автоматическая установка» и нажать кнопку «Далее».

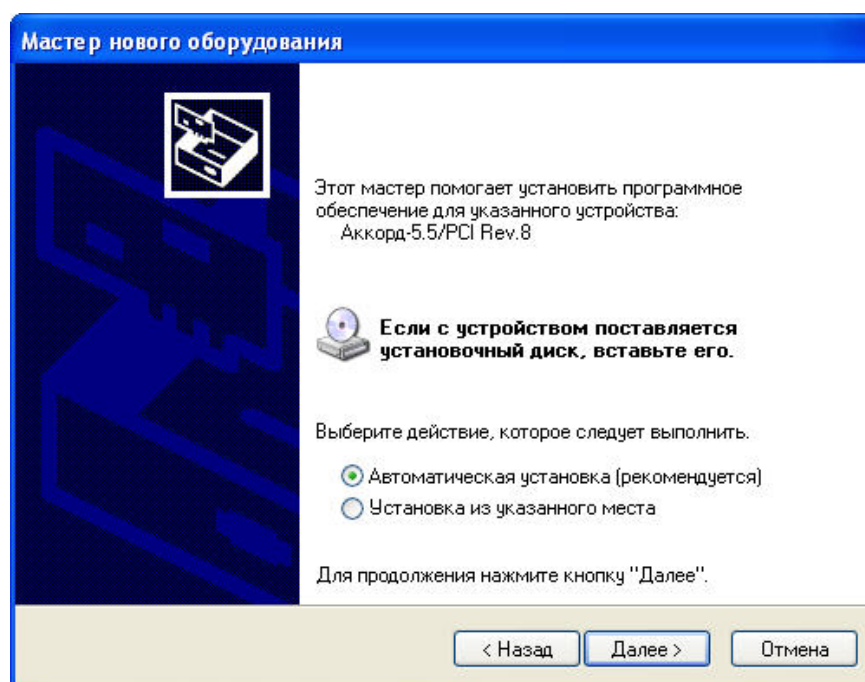


Рис. 1. Окно установки нового оборудования

Начнется установка драйвера устройства АККОРД. После установки драйвера в системе (он помещается в папку \WINDOWS\System32\Drivers\) на экран выводится окно завершения работы «Мастера установки оборудования». Щелкните мышью на кнопке «Готово».

Драйвер устройства установлен, и разъём TM-идентификатора устройства АККОРД подсвечивается зеленым цветом.

ВНИМАНИЕ: Драйвер АККОРД в системе устанавливается один раз. Если Вы используете несколько устройств АККОРД на одном компьютере, то повторной установки драйвера не потребуется. Однако инициализацию и форматирование данных криптографической подсистемы нужно проводить для каждого устройства отдельно!

ВНИМАНИЕ: Необходимо убедиться в том, что установленный драйвер поддерживает работу с криптографической подсистемой устройства АККОРД. Сделать это можно несколькими способами. Во-первых, в папке \WINDOWS\System32\Drivers\ должны появиться файлы: ac55wdm.sys и TmFilter.sys. Во-вторых, можно посмотреть сведения о драйвере устройства (Рис. 2) – там будут указаны эти два названия. Если названия файлов отличаются от ac55wdm.sys и TmFilter.sys, то установлен драйвер, не поддерживающий работу с криптографической подсистемой устройства

АККОРД. В этом случае его необходимо удалить и установить драйвер, поддерживающий работу с криптографической подсистемой устройства.

ВНИМАНИЕ: Некоторые антивирусные программы, могут блокировать установку драйвера устройства АККОРД. В случае если ваша антивирусная программа заблокировала установку драйвера, потребуется на время отключить антивирус, и произвести повторно установку драйвера устройства АККОРД.

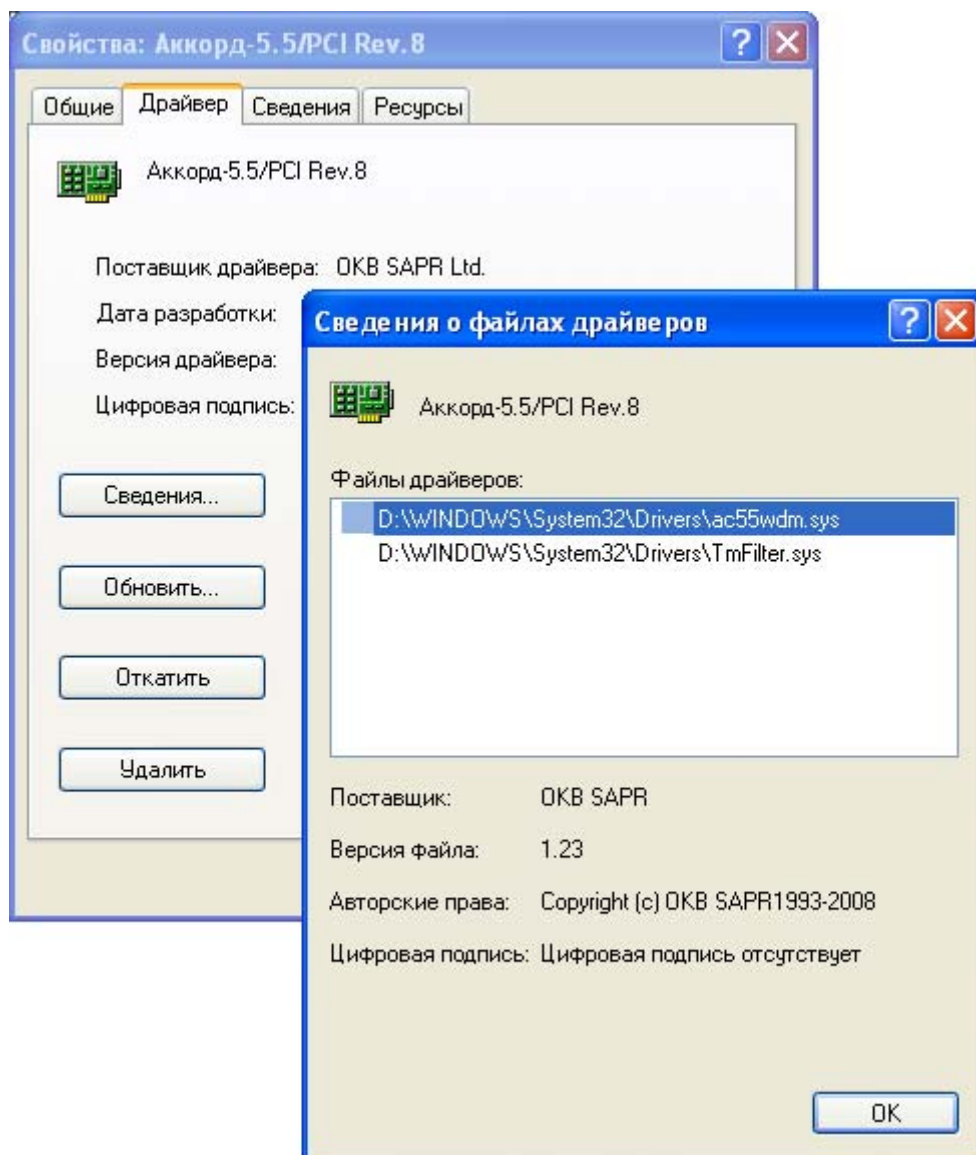


Рис. 2. Сведения о драйвере устройства

2.3. Установка программного обеспечения Аккорда-У

Для установки на жесткий диск ПЭВМ (PC) специального программного обеспечения следует запустить с CD программу AcUSetup.exe. Сначала на экран выводится окно выбора языка. В данный момент поддерживается вариант инсталляции (и дальнейшей работы всех программных компонент) на двух языках – русском и английском. После выбора языка выполняется процедура начальной подготовки к инсталляции и наверху экрана выводится стартовое окно с общей информацией (Рис. 3).

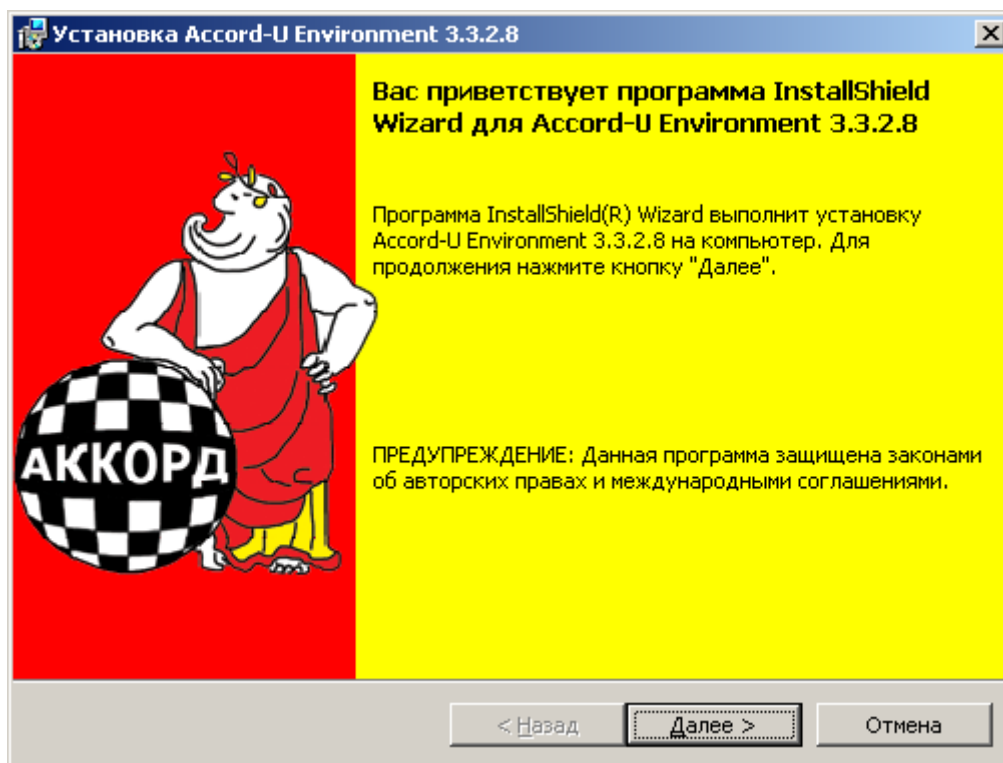


Рис.3. Стартовое окно процедуры инсталляции

Для продолжения процедуры нужно щелкнуть левой клавишей мыши по кнопке «Далее». Для прекращения инсталляции следует выбрать клавишу «Отмена».

В следующем окне выводится текст лицензионного соглашения (См. Приложение 1). Если пользователь согласен с условиями, то необходимо щелкнуть мышью на пункте «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее» (Рис. 4). Если по каким-то причинам Вас не устраивают положения лицензионного соглашения, Вы можете отказаться от установки, выбрав клавишу «Отмена».

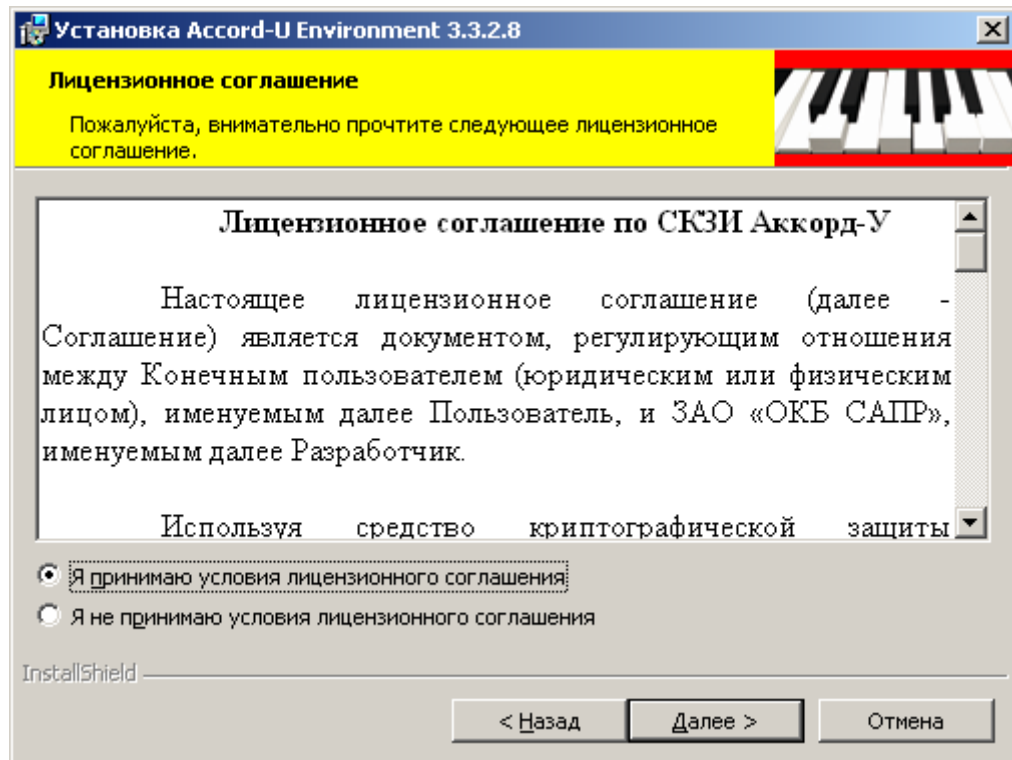


Рис. 4. Условия лицензионного соглашения

Следующее окно – это выбор варианта инсталляции (Рис. 5). В варианте «Полная» выполняется установка всех программных компонент и библиотек в каталог \Program Files\OKB SAPR JSC\Accord-U на системном диске.

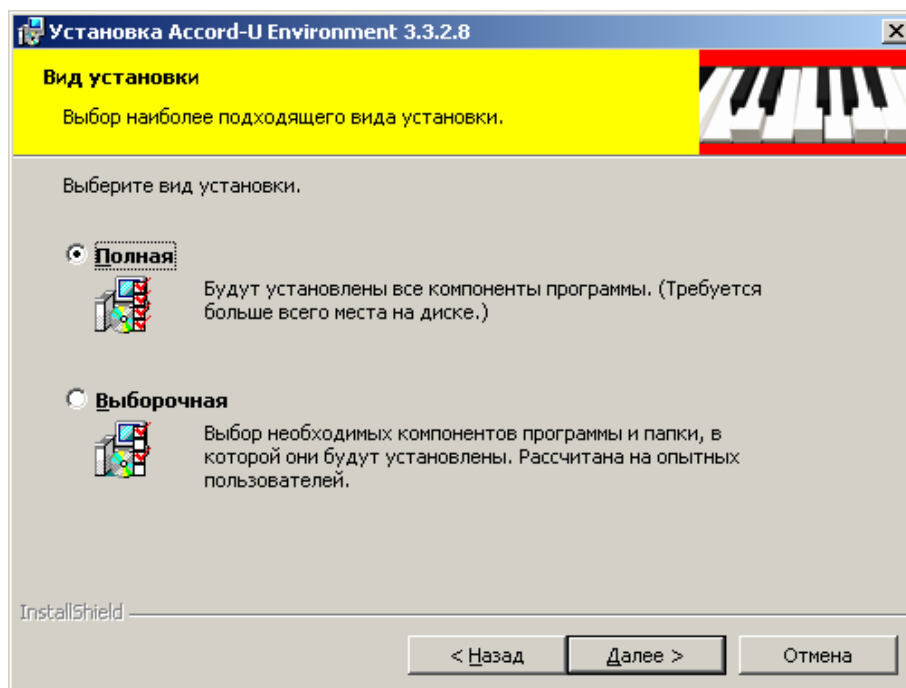


Рис. 5. Выбор варианта установки

На жесткий диск устанавливаются следующие компоненты:

- библиотека для доступа к функциям ШИПКА с уровня прикладного ПО;
- криптопровайдер для работы с алгоритмами ГОСТ через интерфейс Microsoft CryptoAPI;
- библиотека поддержки стандарта PKCS#11;
- программы для назначения параметров авторизации и инициализации устройства;
- программа шифрования/подписи файлов;
- фоновые рисунки для рабочего стола;
- руководство пользователя в формате WORD и PDF.

Вариант установки Выборочная позволяет самостоятельно выбрать устанавливаемые компоненты и папку для размещения файлов (Рис. 6). Щелкнув мышью по клавише «Изменить», можно выбрать любое имя папки. Если такого каталога нет на жестком диске, то он будет создан, если он существует, то на экран выводится окно выбора папки для резервного копирования установленных ранее файлов (если такая процедура нужна пользователю).

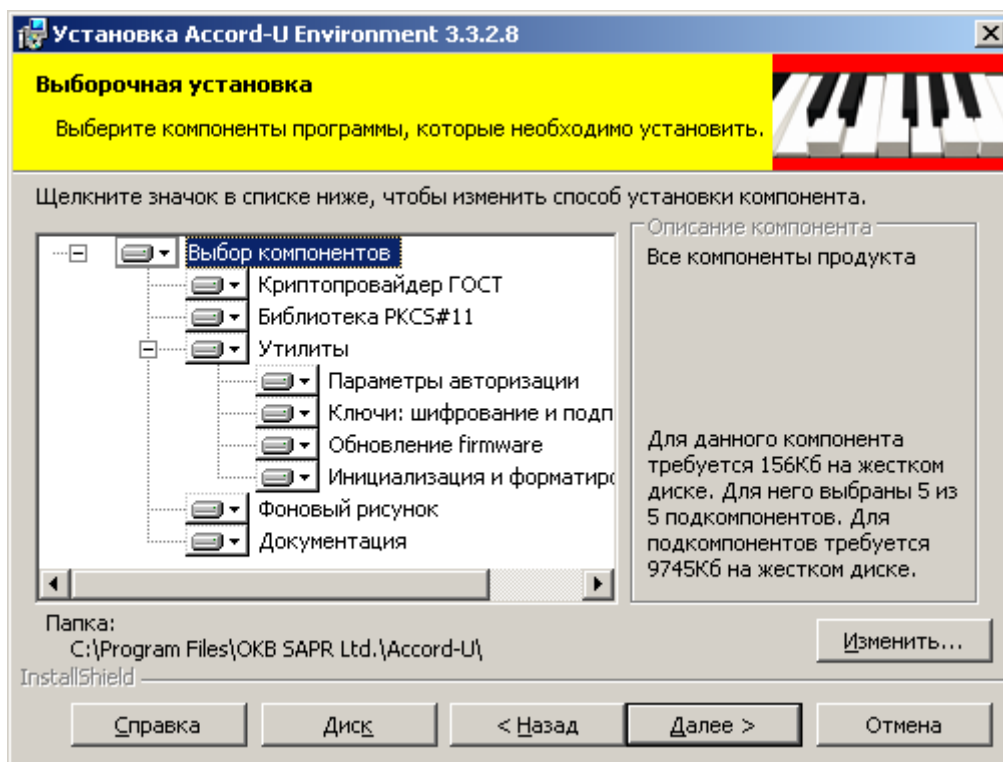


Рис. 6. Окно выбора установки отдельных компонентов

После того, как отмечены компоненты, которые будут устанавливаться на компьютере, нужно щелкнуть мышью на кнопке «Далее». На экран выводится окно готовности к установке. Выбор кнопки «Далее» подтверждает установку, начинается процесс копирования файлов на жесткий диск.

После завершения процесса копирования файлов на экран выводится сообщение об окончании установки.

Щелкните левой клавишей мыши по кнопке «Готово». На экран выводится запрос на перезагрузку компьютера. Для полного завершения процедуры установки компьютер необходимо перезагрузить.

Если при попытке инсталлировать ПО Аккорд-У выдается окно «Обслуживание программ» (Рис. 7), это значит, что у Вас уже установлено ПО Аккорд-У. Если Вы устанавливаете более новое ПО, то нужно выбрать «Удалить» и деинсталлировать старое.

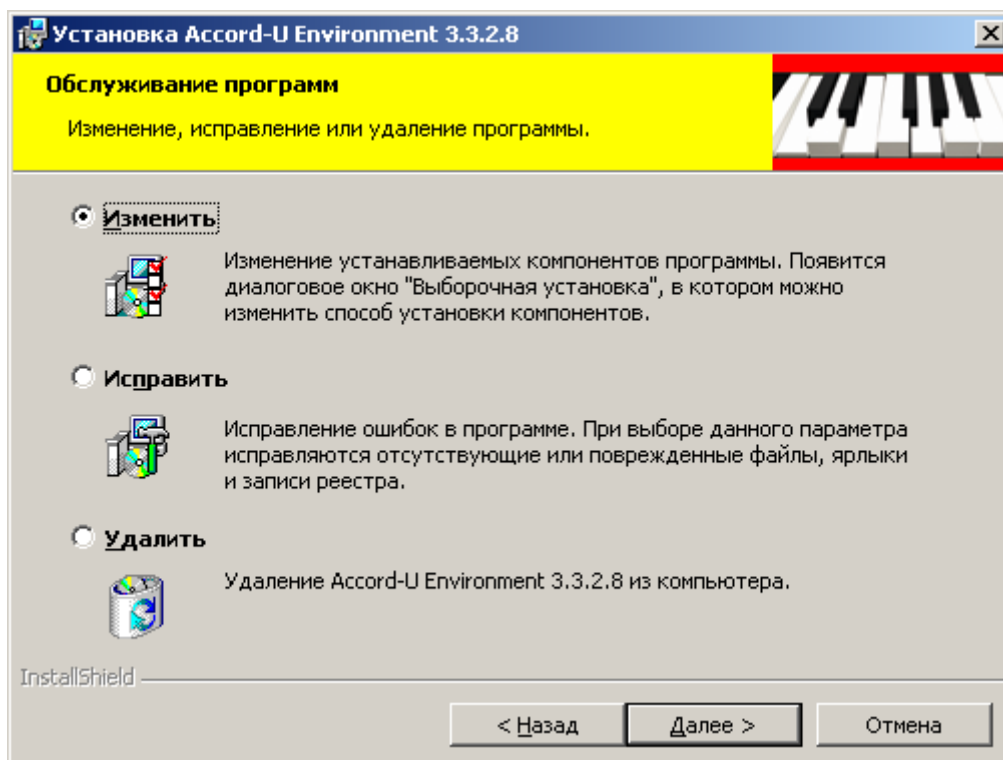


Рис. 7. Окно «Обслуживание программ»

Деинсталляция ПО Аккорд-У выполняется стандартно, как и любого другого ПО: кнопка <Пуск>-<Настройка>-<Панель управления>-<Установка и удаление программ>-<Accord-U Environment >-<Удалить>. Деинсталляцию можно выполнить и таким образом: <Пуск>-<Программы>-<Аккорд-У>-<Удаление ПО Аккорд-У>.

2.4. Инициализация и форматирование данных криптографической подсистемы устройства АККОРД

ВНИМАНИЕ! При использовании Аккорда-У, соответствующего классу KB2, при каждом форматировании (включая установку параметров авторизации) к USB-хосту контроллера должно быть подключено ПСКЗИ ШИПКА*.

* - При форматировании в утилите «Инициализация и форматирование» с выработкой PUK-кода используемое ПСКЗИ ШИПКА должно быть отформатировано перед процедурой, при этом в ПСКЗИ ШИПКА будет удалена вся содержащаяся в ней информация. Это необходимо иметь в виду, выбирая режим форматирования.

Прежде чем начать использование криптографической подсистемы устройства АККОРД, необходимо провести процедуру инициализации (начального форматирования).

ВНИМАНИЕ! Без выполнения этой процедуры пользователю недоступны никакие внутренние криптографические функции устройства АККОРД.

Доступ к встроенным криптографическим функциям АККОРД и персональной информации пользователя (ключам, паролям и пр.) предоставляется пользователю только после ввода аутентифицирующей информации (PIN-кода).

Перед выполнением процедуры инициализации необходимо установить параметры PIN-кода: минимальную длину, количество попыток ввода, алфавит символов, а также наличие/отсутствие PUK-кода и его параметры. Для этого предназначена специальная программа «Параметры авторизации».

PIN-код представляет собой последовательность символов длиной от 6 до 32 знаков. В качестве символов PIN-кода можно использовать цифры, буквы, спецсимволы. Комбинирование различных типов символов повышает надежность процедуры аутентификации. Мощность алфавита (общее число символов) становится больше, а, следовательно, количество вариантов PIN-кода резко возрастает. Минимальная длина PIN-кода и алфавит используемых символов задаются в программе настройки параметров авторизации.

Следующий важный параметр – количество попыток для ввода PIN-кода. Если за отведенное количество попыток пользователь не введет правильный PIN-код, то доступ к криптографической подсистеме устройства АККОРД блокируется.

Возможность разблокирования устройства также задается в программе настройки параметров инициализации. Если данные криптографической подсистемы устройства отформатировать с формированием специального PUK-кода, то с помощью этого кода можно разблокировать АККОРД. Если форматирование данных криптографической подсистемы выполнялось без формирования PUK-кода, то разблокировать устройство нельзя, можно только повторно отформатировать, но при этом стираются во внутренней памяти **ВСЕ** персональные ключи и пароли пользователя.

Поэтому рекомендуется очень внимательно относиться к настройке параметров авторизации.

Параметры авторизации в АККОРД устанавливаются от лица администратора устройства, и могут изменяться в дальнейшем только после введения пароля администратора. Администратор криптографической подсистемы АККОРДа может только назначать параметры авторизации в устройстве, никаких других прав у него нет. Изначально администратор получает неинициализированные устройства, после чего он проводит первичную настройку, т.е. устанавливает параметры авторизации и регистрирует пользователей, присваивая каждому персональный идентификатор. После первичной настройки, администратор передает устройства пользователям, которые в свою очередь проводят инициализацию и форматирование данных криптографической подсистемы устройства АККОРД и устанавливают PIN-код.

Для запуска программы настройки следует последовательно выбрать <Пуск>-<Программы>-<Аккорд-У>-<Настройка>-<Параметры авторизации>. На экран выводится окно выбора параметров (Рис. 8).

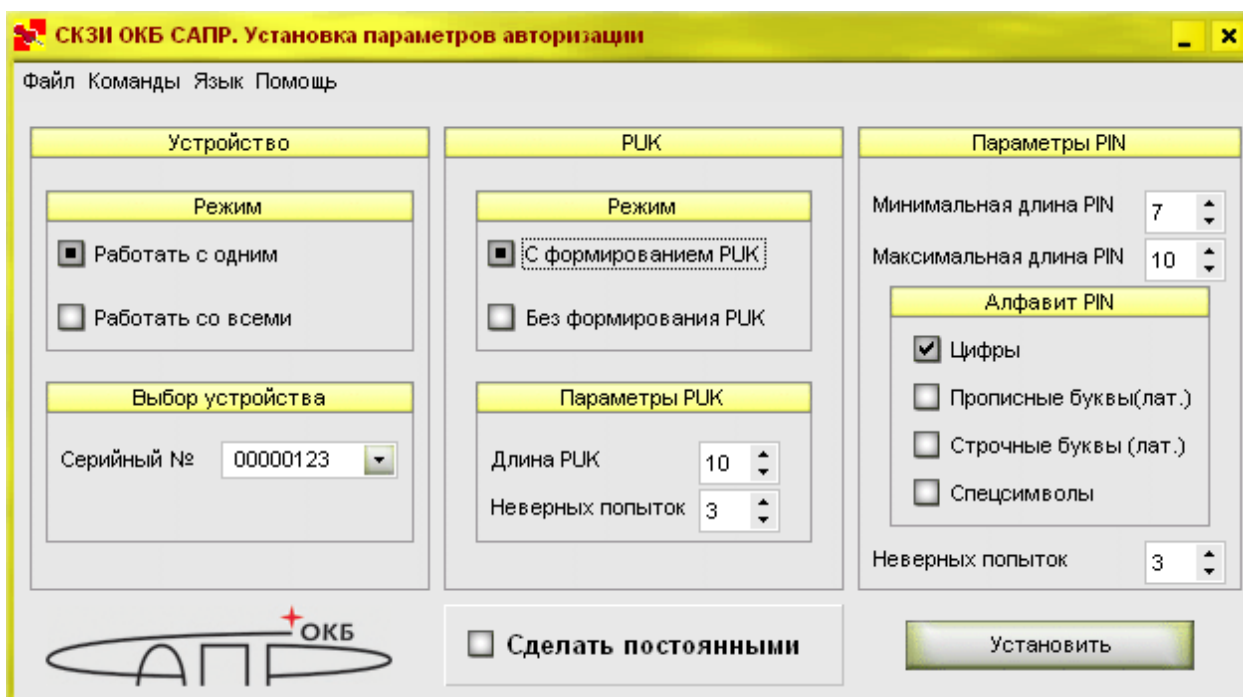


Рис. 8. Окно установки параметров авторизации Аккорда-У

В левой части окна можно выбрать конкретное устройство по серийному номеру, либо установить режим «Работать со всеми». В этом случае параметры авторизации будут установлены для всех устройств ШИПКА и

АККОРД, подключенных в данный момент времени к USB-портам и разъемам материнской платы компьютера соответственно.

В средней части окна можно настроить режим форматирования «С форматированием PUK», или «Без форматирования PUK».

PUK-код представляет собой последовательность из цифр и букв, выработанную случайным образом в процессе форматирования. Параметры PUK-кода задаются в этой же части окна:

- «длина PUK» – число символов в PUK-коде. Число символов в PUK должно быть обязательно четным! Если задать нечетное число, то при выработке PUK-кода количество символов будет округлено до четного в меньшую сторону;

- «неверных попыток» – количество ошибок, допустимых при вводе PUK-кода. После исчерпания числа попыток ввода PUK-кода доступ к криптографической подсистеме устройства АККОРД полностью блокируется.

В правой части окна устанавливаются параметры PIN-кода.

- **минимальная и максимальная длина** – эти параметры определяют нижнюю и верхнюю границы для количества знаков в PIN-коде.

ВНИМАНИЕ: После выполнения инициализации (форматирования) устройства АККОРД, PIN-код не задается автоматически и не устанавливается администратором. Пользователь должен ввести собственный PIN-код (см. п.2.5).

- Параметр «**Алфавит**» определяет множество символов, которые будут использоваться при первом вводе PIN-кода и его последующих сменах. Можно указать как один, так и несколько наборов символов, поставив отметку напротив нужного пункта. Набор «Спецсимволы» содержит символы, вводимые при нажатии комбинации клавиш Shift-(0-9).

ВНИМАНИЕ: При выборе алфавита следует учитывать, что PIN-код должен содержать *хотя бы по одному символу из каждого выбранного набора*. Возможна установка PIN-кода, который, кроме символов из «обязательных» наборов содержит другие символы, например, при установленном флаге «Цифры» можно использовать в PIN-коде буквы, но ввести PIN-код из одних букв нельзя.

- Параметр **«Неверных попыток»** характеризует количество допустимых ошибок при вводе PIN. После превышения количества попыток криптографическая подсистема устройства АККОРД блокируется.

ВНИМАНИЕ! Следующий параметр очень важен для всей последующей работы с криптографической подсистемой устройства АККОРД. Если включить флаг **«Сделать постоянными»** и нажать кнопку **«Установить»**, то выбранные параметры авторизации криптографической подсистемы устройства АККОРД будут установлены раз и навсегда, т. е. изменить их будет невозможно даже с помощью данной программы. Задавать этот параметр следует только в том случае, если есть уверенность, что выбранные настройки будут полностью удовлетворять политике безопасности, и не придется в дальнейшем задавать другие параметры. Если такой уверенности нет, лучше не использовать эту опцию.

Если флаг **«Сделать постоянными»** не включен, то при выборе кнопки **«Установить»** выводится запрос на ввод и подтверждение пароля администратора.

Если администратор задает одинаковые параметры авторизации подряд для большого количества устройств, и параметры, которые он устанавливает, отличаются от предлагаемых по умолчанию, то чтобы не изменять параметры каждый раз, он может изменить параметры по умолчанию, выбрав в меню **«Файл»** пункт **«Сохранить параметры»**.

ВНИМАНИЕ! *Сохранение параметров по умолчанию не устанавливает эти параметры для выбранного устройства! Для установки параметров нужно нажать «Установить»!*

Если выбран режим работы со всеми устройствами, установленными на этом компьютере, то предполагается, что пароль администратора одинаков для всех устройств.

После нажатия кнопки **«Установить»** и ввода пароля администратора выполняется очистка области памяти, отведенной для пользовательской информации (ключи, пароли и пр.), и записываются в служебную память установленные параметры, в соответствии с которыми пользователь может в дальнейшем выполнять форматирование и разблокировку устройства. Пароль

администратора также записывается в устройство АККОРД и потребуется для последующих изменений параметров авторизации.

Администратор в любой момент может поменять свой пароль через меню <Команды>-<Сменить пароль>. Все остальные данные криптографической подсистемы в устройстве АККОРД при этой операции не меняются.

Пароль администратора позволяет многократно изменять параметры авторизации устройства АККОРД. При изменении параметров авторизации область данных пользователя очищается, и поэтому после установки новых параметров, криптографическую подсистему устройства **обязательно нужно отформатировать** и установить новый PIN-код и PUK-код, если его наличие предписано новыми правилами.

ВНИМАНИЕ! Пароль администратора размещен в отдельной области памяти криптографической подсистемы устройства АККОРД и не очищается ни при форматировании данных этой подсистемы, ни при замене внутреннего ПО устройства.

ВНИМАНИЕ! После установки параметров авторизации выполняется очистка области данных пользователя, при этом удаляются все ключи, содержащиеся на устройстве. Дальнейшая работа будет возможна только после форматирования данных криптографической подсистемы устройства АККОРД!

ВНИМАНИЕ! При форматировании криптографической системы АККОРД, данные АМДЗ не стираются.

Все действия с параметрами авторизации и паролем администратора регистрируются в журнале. По умолчанию журнал ведется в файле AcshInit.log в той папке, в которую установлены утилиты ПО ПСКЗИ ШИПКА. В меню «Файл» > «Журнал» программы «Установка параметров авторизации» можно указать другой файл для сохранения журнала или другое размещение файла.

Следующий шаг – непосредственная инициализация (форматирование) криптографической подсистемы устройства АККОРД, которая выполняется отдельной утилитой.

Вызов утилиты инициализации выполняется следующим образом: <Пуск>-<Программы>-<Аккорд-У>-<Настройка>-<Инициализация и форматирование>. В главном окне программы (Рис. 9) три закладки: «Сменить PIN», «Форматировать» и «Разблокировать».

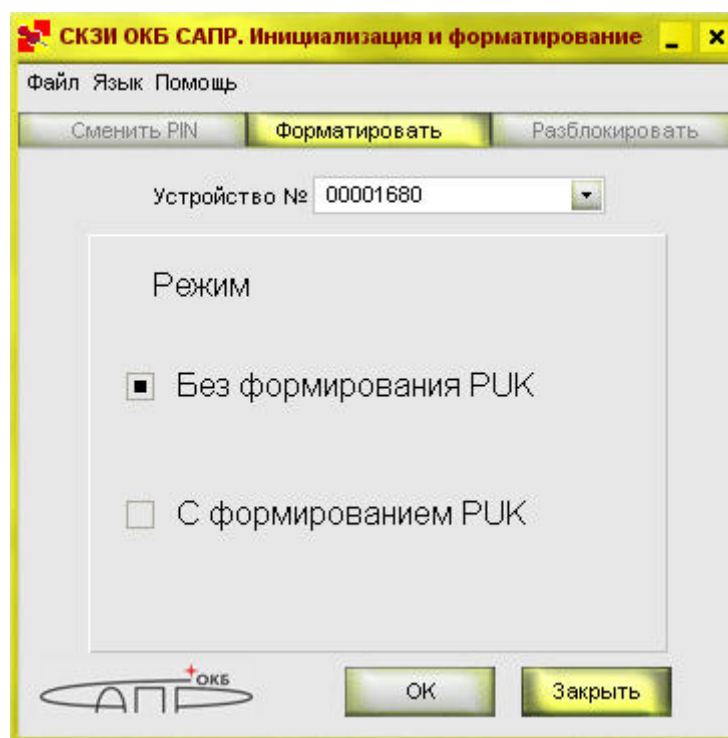


Рис. 9. Форматирование устройства АККОРД

Первая операция, которая выполняется с новым устройством АККОРД, – это форматирование данных криптографической подсистемы устройства.

Выберите закладку «Форматировать» и нажмите кнопку «Ок». Если администратором установлен режим форматирования с формированием PUK-кода (настоятельно рекомендуется устанавливать именно этот режим, потому что это поможет избежать проблем в случае блокировки устройства), то первое форматирование должно обязательно производиться с формированием PUK, обойти это правило нельзя (Рис. 10).

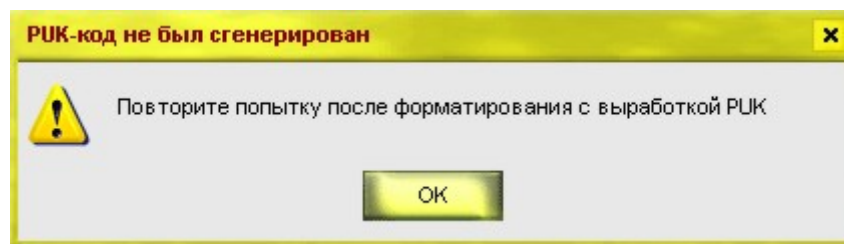


Рис.10. Предупреждение о невозможности отформатировать данные криптографической подсистемы устройства АККОРД без формирования PUK-кода

В процессе выполнения операции выводится окно со сгенерированным PUK-кодом и предложением сохранить этот PUK-код в файл (Рис. 11).

Пользователь может принять сохранение, или отказаться от него, но резервная копия кода разблокировки поможет в случае, если пользователь его забыл. Этот файл необходимо перенести на любое сменное устройство и хранить в надежном месте.

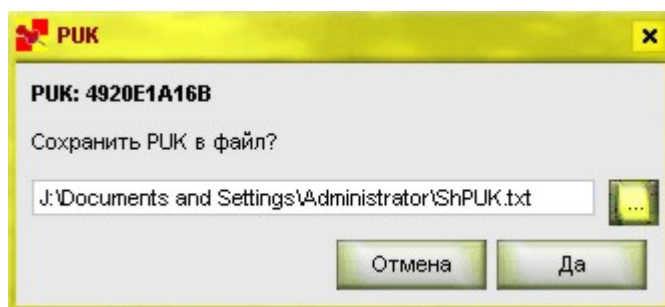


Рис.11. Запрос на сохранение PUK-кода в файл

Форматирование и успешное сохранение PUK-кода подтверждается сообщением с указанием пути к файлу (Рис. 12).

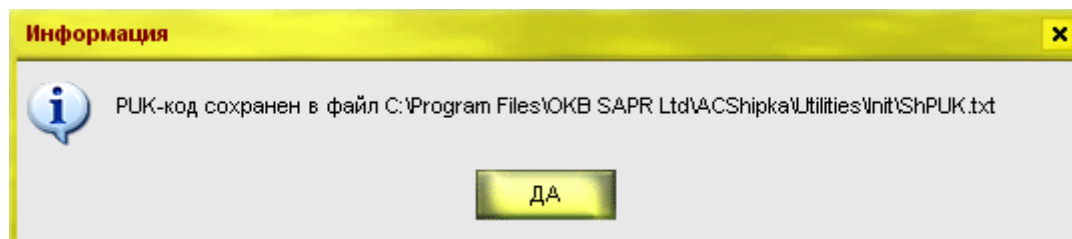


Рис.12. Подтверждение записи PUK-кода в файл

Последующие форматирования можно производить и без выработки PUK-кода, и тот PUK, что был выработан последним, будет оставаться действительным (Рис. 13).

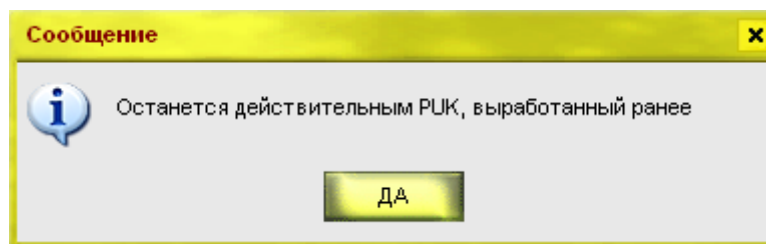


Рис. 13. Сообщение, выводящееся в том случае, если производится форматирование без выработки нового PUK-кода, а в Параметрах авторизации задано правило «Форматирование с выработкой PUK»

2.5. Установка PIN-кода для криптографической подсистемы устройства АККОРД

Следующий этап в работе с криптографической подсистемой устройства АККОРД – установка PIN-кода. После операции форматирования PIN-код сбрасывается, и пользователь должен установить новый PIN. Для этого в программе инициализации нужно выбрать закладку «Сменить PIN-код». Эта закладка используется и для ввода нового кода в отформатированное устройство, и для смены PIN-кода по желанию пользователя. При записи нового PIN-кода в отформатированное устройство ввода старого кода не требуется (поле «старый PIN-код» заблокировано). Достаточно дважды ввести новый код и нажать кнопку «Ок» (Рис. 14).

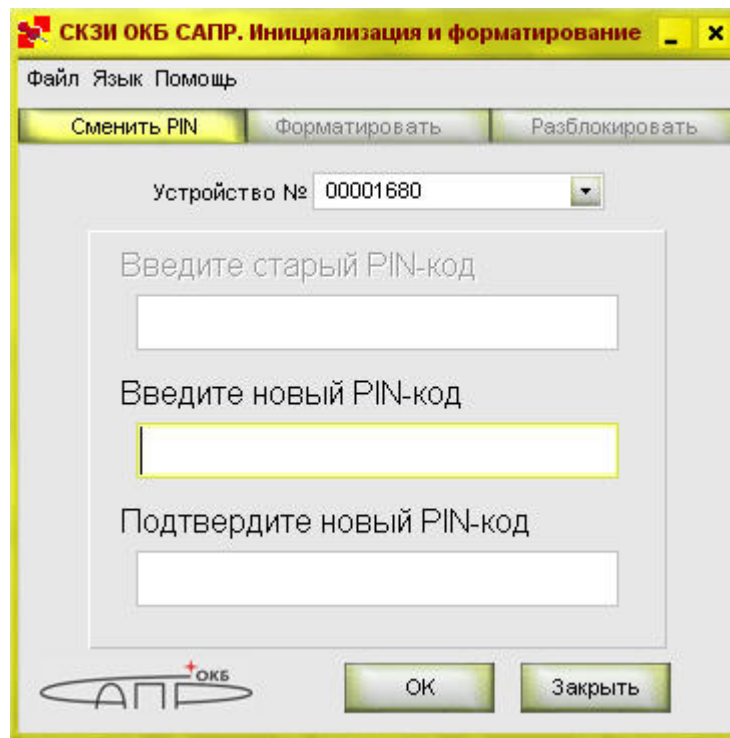


Рис. 14. Процедура ввода нового PIN-кода

Если код введен дважды одинаково, то на экране появляется сообщение об успешной смене PIN-кода.

При неправильном повторном вводе выдается сообщение о несовпадении двух последовательностей символов.

Пользователь может сменить существующий PIN-код в любой момент времени. Достаточно правильно ввести старый PIN-код и дважды ввести новый (Рис. 15).

ВНИМАНИЕ! При использовании в PIN-коде буквенных символов рекомендуется ввод на английской раскладке клавиатуры.

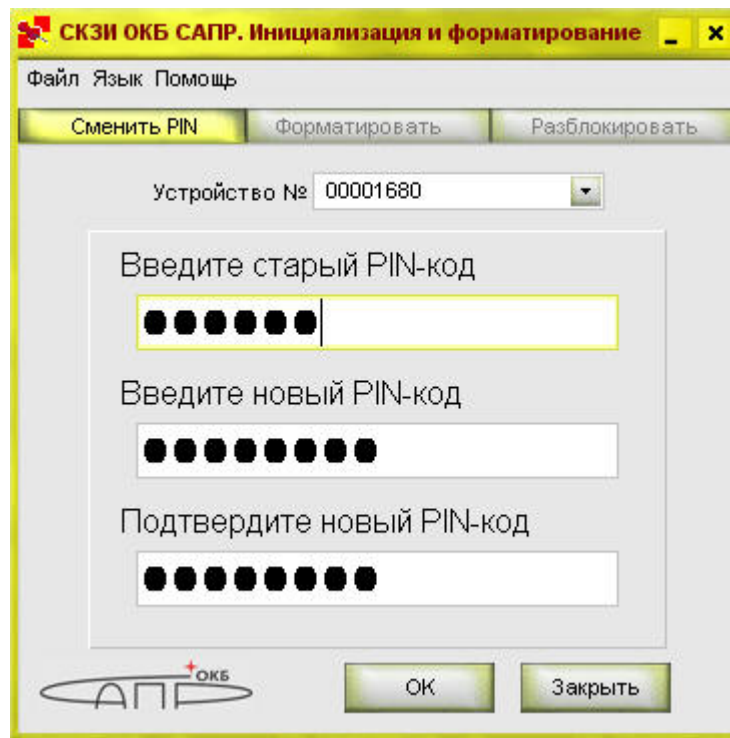


Рис.15. Смена установленного PIN-кода для криптографической подсистемы устройства АККОРД

2.6. Разблокирование криптографической подсистемы устройства АККОРД

Если количество неверных вводов PIN-кода превысит установленное в параметрах авторизации допустимое количество попыток, то криптографическая подсистема устройства АККОРД будет заблокирована (Рис. 16).

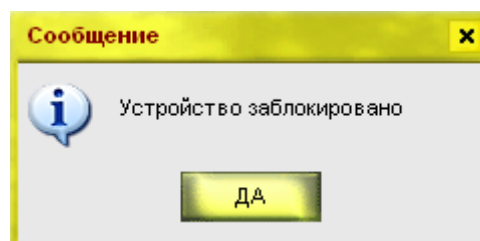


Рис. 16. Предупреждение о блокировке криптографической подсистемы устройства АККОРД

Если форматирование выполнялось с генерацией PUK-кода, то пользователь сможет самостоятельно разблокировать криптографическую подсистему устройства АККОРД без потери записанных в ней данных.

Для этого в программе инициализации нужно выбрать закладку «Разблокировать» и после корректного ввода PUK-кода дважды ввести новый PIN-код (Рис. 17).

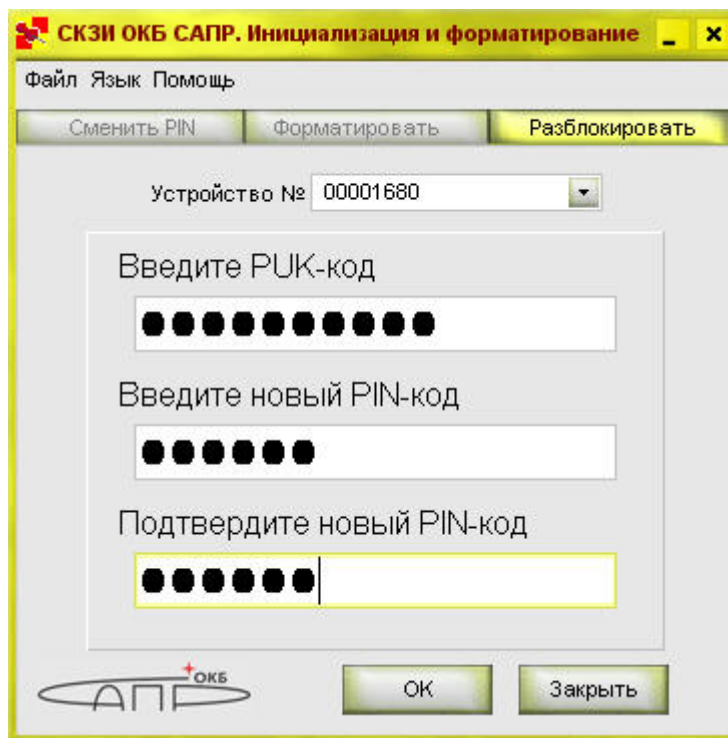


Рис. 17. Разблокирование устройства с помощью PUK-кода

ВНИМАНИЕ! Если данные криптографической подсистемы устройства АККОРД форматировались без генерации PUK-кода, то в случае блокировки, её невозможно разблокировать! Последующее использование такого устройства возможно только после форматирования с потерей ВСЕХ пользовательских данных.

ВНИМАНИЕ! Если при попытке разблокирования устройства PUK-код был введен неправильно несколько раз (это число определено в параметрах авторизации), то криптографическая подсистема устройства АККОРД блокируется окончательно. Разблокирование такого устройства невозможно. При этом АМДЗ будет продолжать функционировать.

2.7. Ведение внутреннего журнала регистрации событий безопасности

Если политика безопасности, принятая в организации, требует ведения внутреннего журнала регистрации событий безопасности, то включить эту опцию в АККОРД-У можно следующим образом:

- добавить в файл ACshParams.ini, расположенный в \Program Files\ОКБ SAPR JSC\Accord-U\Utilities\AParams или по тому пути, куда было установлено ПО АККОРД-У, секцию:

[LOG]

SetLog = 1

- заново установить параметры авторизации (см. пункт 2.4).

А для просмотра внутреннего журнала регистрации событий безопасности необходимо запустить утилиту InternalLog.exe, расположенную в \Program Files\ОКБ SAPR JSC\Accord-U\Utilites\InternalLog или по тому пути, куда было установлено ПО АККОРД-У (Рис. 18).

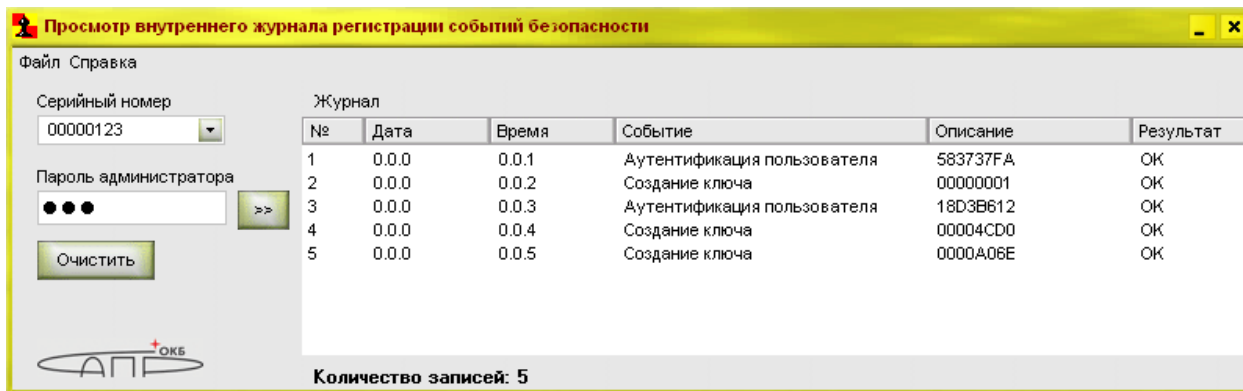


Рис. 18. Утилита просмотра внутреннего журнала регистрации событий безопасности

ВНИМАНИЕ! Если опция ведения журнала регистрации событий безопасности не была включена, то при просмотре в данной утилите журнал будет пустым.

3. Использование криптографической подсистемы устройства АККОРД

3.1. Шифрование и подпись файлов на жестком диске

3.1.1. Работа с ключами

Любые криптографические преобразования производятся с использованием криптографических ключей, которые являются критически важной с точки зрения безопасности информацией.

Криптографическая подсистема устройства АККОРД реализована таким образом, что вся работа с ключами производится строго внутри устройства. Ключи генерируются в АККОРДе с применением физического датчика случайных чисел (ДСЧ), защищены от несанкционированного копирования в процессе хранения в памяти устройства, а поскольку все вычисления производятся процессором устройства АККОРД, то ключи никогда не попадают в оперативную память компьютера.

Устройство АККОРД поддерживает работу как с симметричной, так и с асимметричной криптографией. В соответствии с российскими нормативными документами симметричная криптография применяется для шифрования, а асимметричная – для шифрования и выработки/проверки ЭЦП.

Различается симметричная и асимметричная криптография по тому, как реализована в ней работа с ключами. Если при зашифровании и при расшифровании используется один и тот же ключ, то это симметричный процесс, а если разные (пара – закрытый и открытый), то процесс называется асимметричным. Традиционно симметричные ключи называют ключами шифрования, а ключевые пары – ключами подписи.

Если вы только что инициализировали криптографическую подсистему или произвели форматирование данных криптографической подсистемы устройства АККОРД, то внутри этого устройства никаких ключей не содержится, все ключи пользователь генерирует самостоятельно каким-либо из перечисленных ниже способов или импортирует в свой АККОРД. До этого

никакие криптографические операции не будут доступны (об этом будут выводиться специальные сообщения).

3.1.1.1. Генерация ключей

Симметричные ключи

Работать с симметричными ключами в устройстве АККОРД можно с помощью программы «Ключи: шифрование и подпись файлов» и с помощью специальной программной оболочки PRIVACY, которая не входит в состав стандартного ПО Аккорд-У, представляя собой отдельный продукт.

С помощью программы «Ключи: шифрование и подпись файлов» можно сгенерировать и в дальнейшем применять симметричные ключи ГОСТ 28147-89.

Программу можно запустить через меню программ: <Пуск>-<Программы>-<Аккорд-У>-<Применение>-<Шифрование и подпись файлов>. После запуска программы открывается главное окно, в котором пользователь может выбрать файлы на своем жестком диске и выполнить над ними необходимую операцию (Рис. 19).

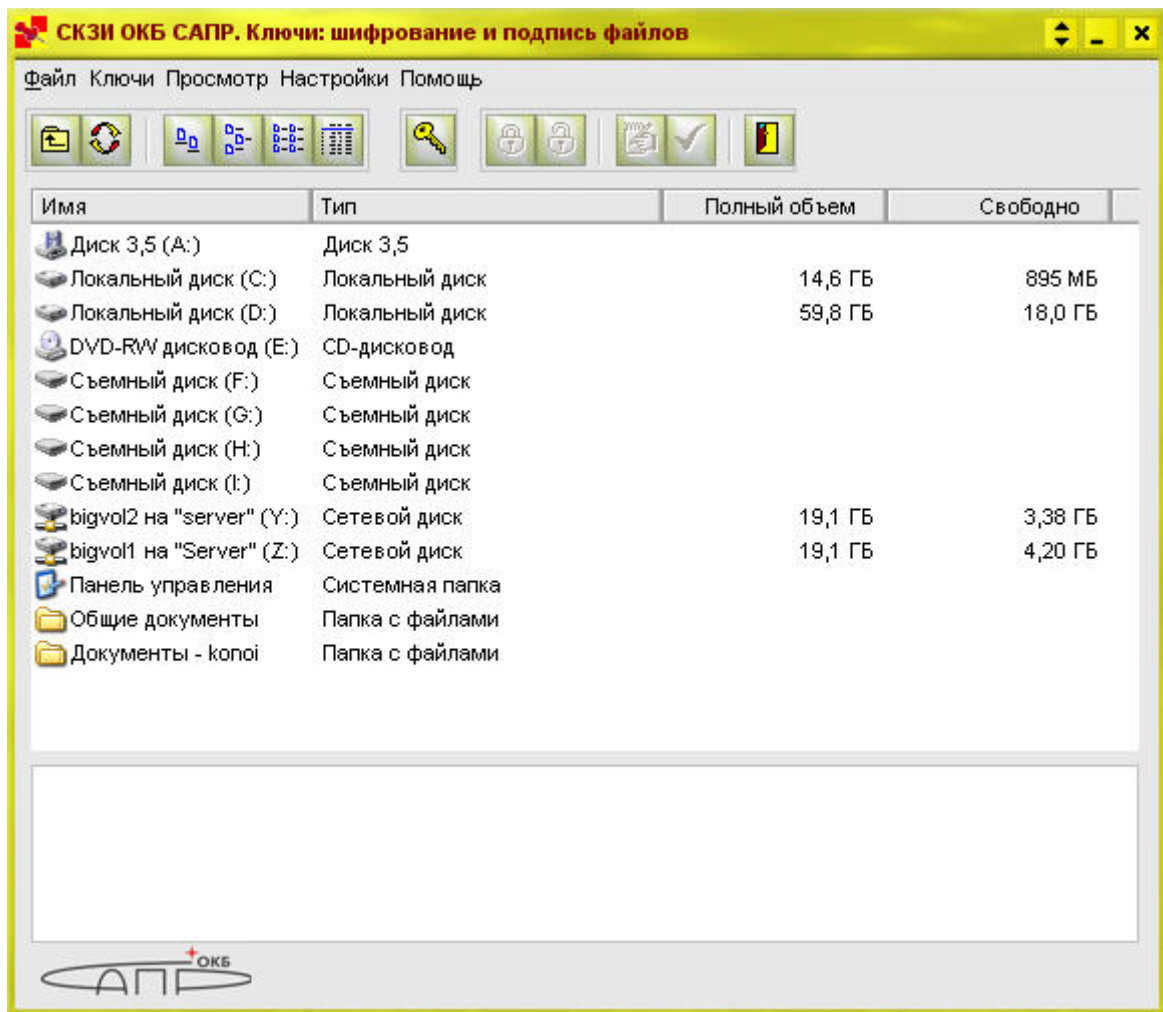


Рис. 19. Главное окно программы шифрования/подписи файлов

После форматирования в устройстве не содержится никакой ключевой информации, и в случае попытки выполнить операцию «Шифрование» или «Подпись» на экране появится сообщение об ошибке: «Ни одного ключа не найдено в устройстве ШИПКА №...».

Значит, необходимо выполнить процедуру генерации ключей.

На панели задач находится специальная кнопка с изображением ключа, а в пункте меню «Ключи» есть команда «Управление ключами». Выбор этой команды выводит на экран окно ключевого менеджмента (Рис. 20).

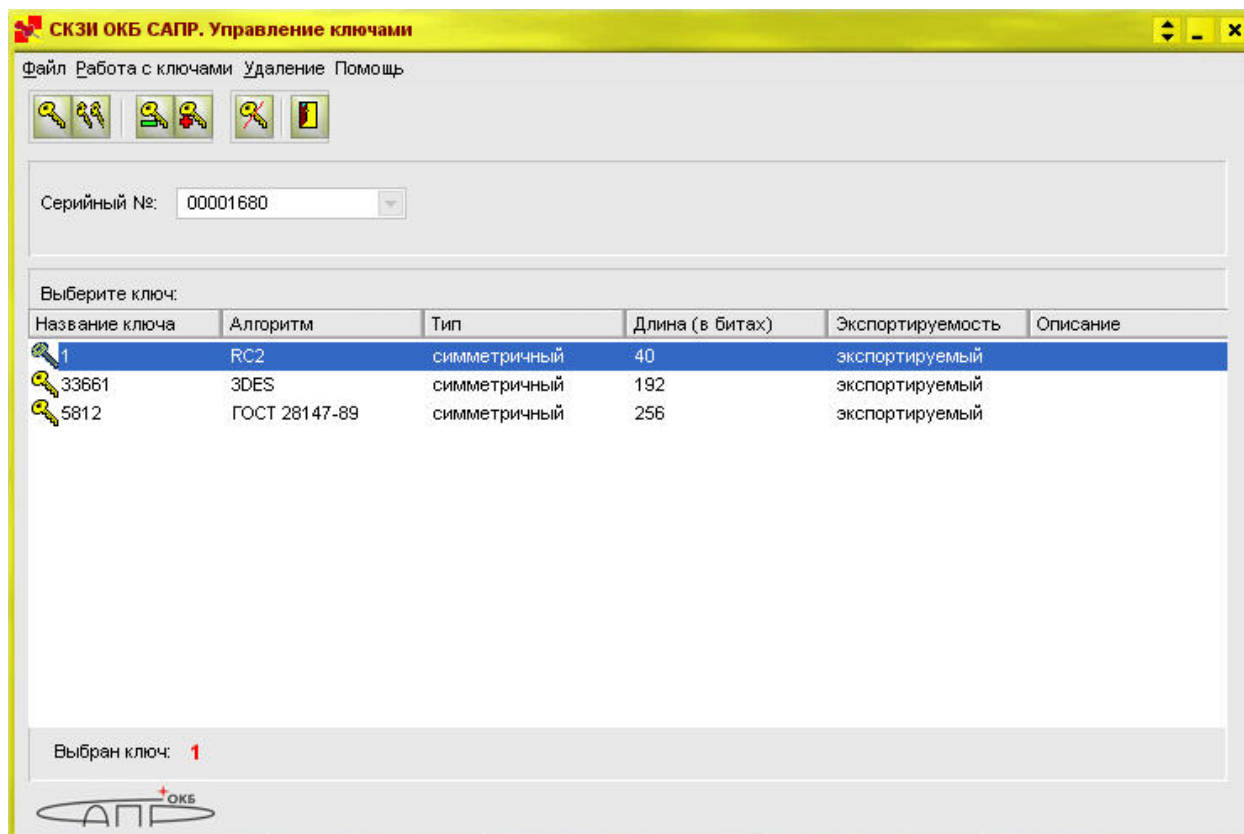


Рис. 20. Окно управления ключами устройства АККОРД

При нажатии на кнопку с изображением одного ключа, или вызове команды «Генерация» -> «Генерировать ключ» открывается окно генерации симметричного ключа (Рис. 21).

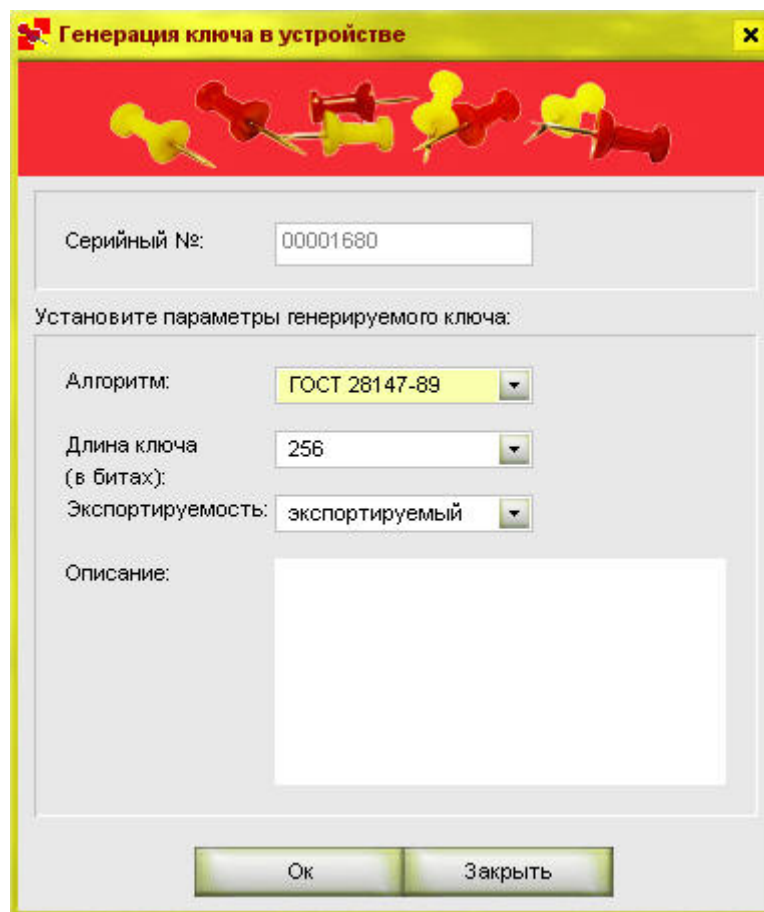


Рис. 21. Генерация ключа для операции шифрования

Если на ПЭВМ используется несколько устройств АККОРД, то генерация будет производиться в том устройстве, которое было выбрано в окне «Управление ключами». Перед генерацией необходимо задать параметры ключа (алгоритм шифрования, длина, экспортируемость) и затем нажать кнопку «Генерировать».

Запрашивается PIN-код (Рис. 22) и после его ввода ключ генерируется и записывается в память устройства АККОРД. Операция генерации и записи ключа выполняется внутренним ПО устройства АККОРД с использованием аппаратного датчика случайных чисел. Теперь этот ключ может использоваться при шифровании файлов.

ВНИМАНИЕ! Устройство АККОРД работает только с алгоритмами ГОСТ.

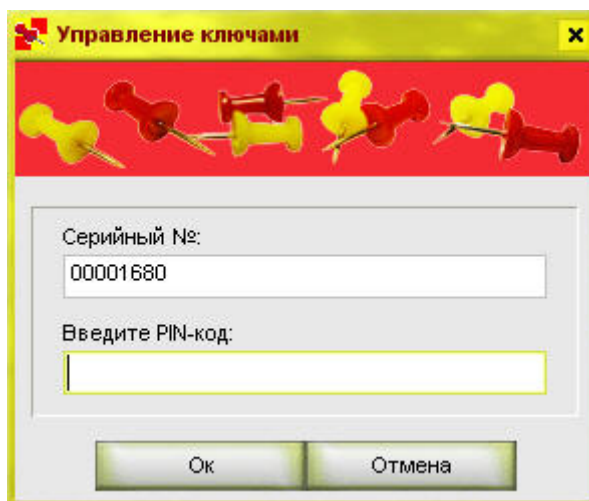


Рис. 22. Ввод PIN-кода перед записью ключа

Операция завершается выводом сообщения об успешном выполнении. После этого нужно нажатием кнопки «Заккрыть» закончить работу с программой генерации ключа.

Пары ключей

В программе «Ключи: шифрование и подпись файлов» пары ключей генерируются так же, как и симметричные ключи.

Для подписи файлов могут использоваться пары ключей, сгенерированные с помощью устройства АККОРД, в других системах, например, в программе PGP. Все эти ключи видны в окне программы «Управление ключами» и могут быть выбраны для операций в программе «Шифрование и подпись файлов».

Те ключи и ключевые пары, которые утратили актуальность, могут быть удалены из памяти криптографической подсистемы устройства АККОРД. Для этого нужно выбрать ставший ненужным ключ и нажать на кнопку «Удалить» (перечеркнутый ключ).

ВНИМАНИЕ! Устройство АККОРД работает только с алгоритмами ГОСТ.

3.1.1.2 Экспорт/импорт ключевой информации

Открытые ключи

Если в свойствах ключа при генерации был указан параметр «Экспортируемый», то **открытый ключ** ключевой пары ЭЦП можно экспортировать в файл на жестком диске. Для этого нужно нажать кнопку «Экспорт» на панели задач и указать имя файла (Рис. 23).

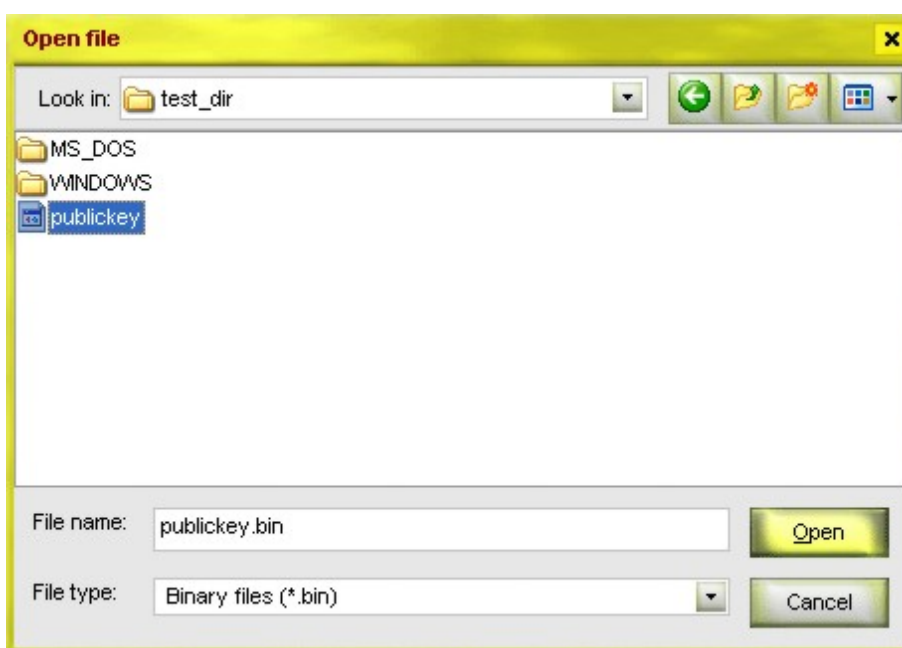


Рис. 23. Выбор файла для экспорта открытого ключа

После этого файл publickey нужно передать пользователю, с которым производится обмен. Это можно сделать, передав файл по электронной почте или на любом носителе.

Для импорта ключа необходимо нажать кнопку «Импортировать», указать файл открытого ключа на жестком диске и ввести PIN-код того устройства, в которое мы импортируем ключ. На экран выводится окно импорта ключа (Рис. 24), в котором можно дать дополнительное описание, например, «ключ для обмена». После нажатия на кнопку «Ок» открытый ключ запишется в память устройства АККОРД.

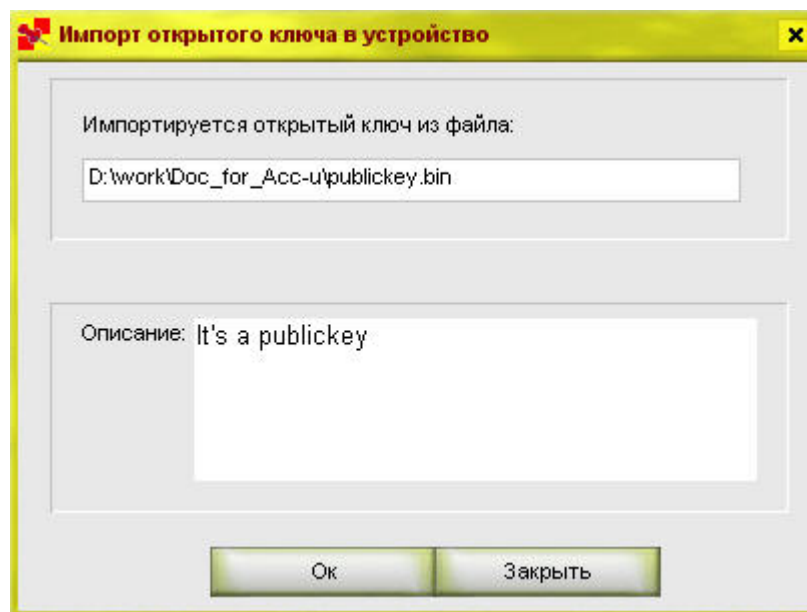


Рис. 24. Окно подтверждения операции импорта

Симметричные ключи

Экспортировать/импортировать **симметричные ключи шифрования** возможно только в зашифрованном виде. Импортированный симметричный ключ принято называть сессионным, потому что в целях повышения безопасности обмена данными рекомендуется каждый ключ использовать только для одной сессии.

Экспорт/импорт симметричных ключей шифрования для обмена с абонентом выполняется при помощи своего закрытого ключа ЭЦП и импортированного открытого ключа ЭЦП, выработанных по ГОСТ Р 3410-2001.

Для экспорта/импорта симметричного ключа ГОСТ и выполняется при помощи своего закрытого ключа ЭЦП и импортированного открытого ключа ЭЦП, выработанных по ГОСТ Р 3410-2001. Процедура в этом случае выглядит следующим образом:

- на устройстве АККОРД №1 сгенерировать ключевую пару ЭЦП по ГОСТ Р.3410-2001 (**П1**). Открытый ключ экспортировать в файл на диске;
- передать файл на компьютер второго пользователя. Импортировать открытый ключ в устройство №2, нажав соответствующую кнопку на панели команд (при импорте называем его **О1**);
- сгенерировать в устройстве №2 ключевую пару ЭЦП ГОСТ Р 3410-2001 (**П2**);

- сгенерировать в устройстве №2 симметричный ключ по ГОСТ 28147-89 для операций шифрования (**C2**). Ключ должен генерироваться только с параметром «Экспортируемый»! Рекомендуется в поле «Описание» ввести какое-либо слово, или фразу, которое поможет Вам в дальнейшем легко выбрать ключ из списка;

- экспортировать из устройства №2 симметричный ключ **C2** в файл на жестком диске (Рис. 25). Для этого нужно нажать кнопку «экспорт ключа» на панели инструментов, или выбрать команду в меню «Работа с ключами». При этом следует указать именно тот открытый ключ, который получен от устройства №1 и закрытый ключ ЭЦП, полученный в результате генерации пары в устройстве №2, то есть **O1** и **P2**;

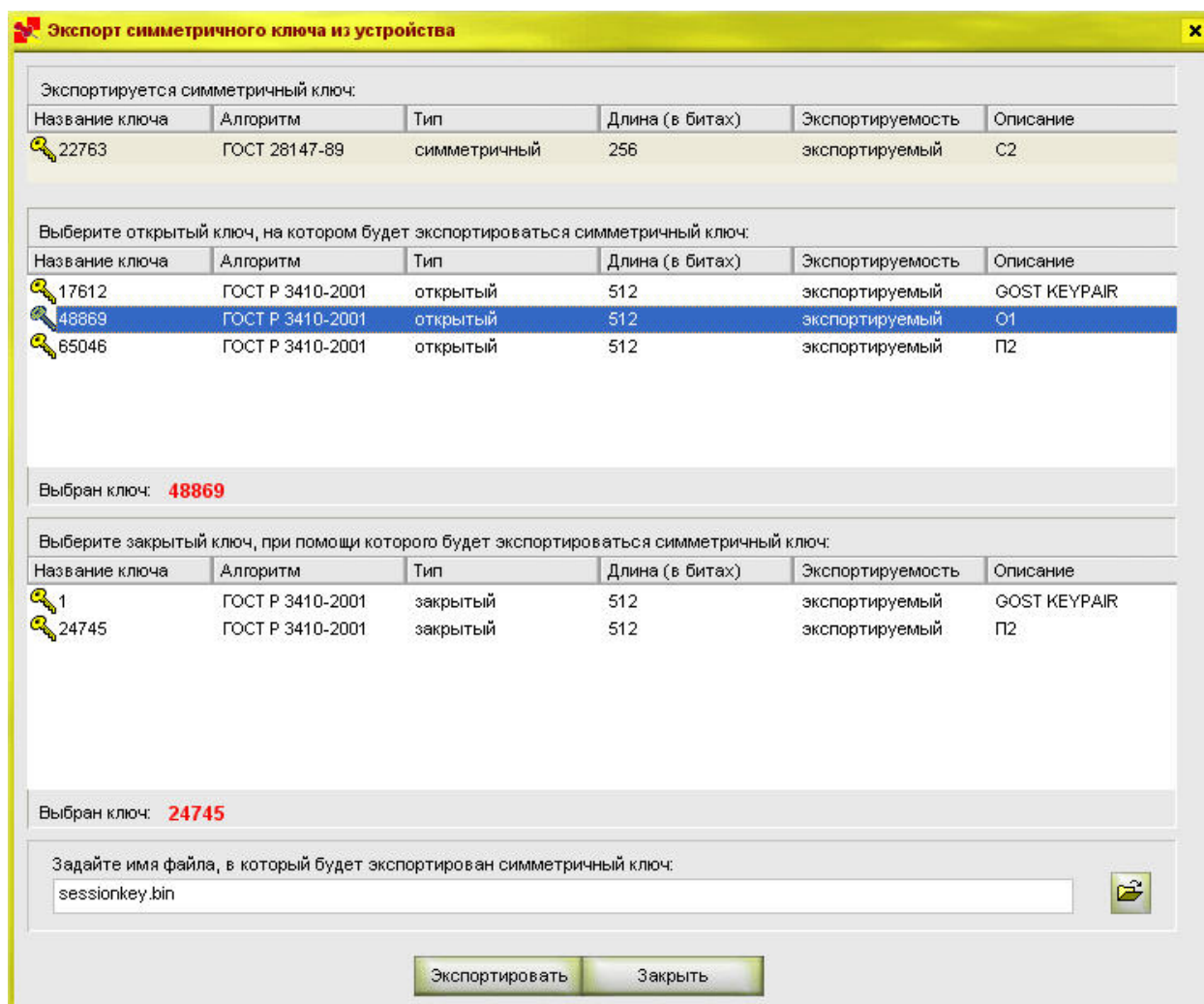


Рис. 25. Выбор ключей ЭЦП для экспорта симметричного ключа

- экспортировать из устройства №2 открытый ключ пары ЭЦП (**P2**) в другой файл на жестком диске, например, publickey2.bin, и передать его второму пользователю;

- второй пользователь импортирует ключ publickey2.bin, выбрав команду «Импортировать ключ». Открытый ключ ЭЦП из устройства АККОРД №2 запишется в устройство №1 (при импорте назовем его **O2**).

- теперь можно приступить к основной операции. Еще раз выполнить команду «Импортировать ключ», указав на диске файл sessionkey.bin. Если вы ошиблись при выборе ключевых пар ЭЦП в момент формирования файла сессионного ключа, то на экран выводится сообщение об ошибке.

Расшифровать сессионный ключ можно только с помощью закрытого ключа пары, сгенерированного в устройстве №1 и открытого ключа пары, сгенерированной в устройстве №2 – **П1** и **O2**. Если при формировании сессионного ключа все части ключевых пар ЭЦП выбраны правильно, то Вам останется только подтвердить операцию в окне импорта ключа (Рис. 26). В этом окне уже нельзя выбирать открытый/закрытый ключи, только можно ввести дополнительное описание импортируемого симметричного ключа **C2**.

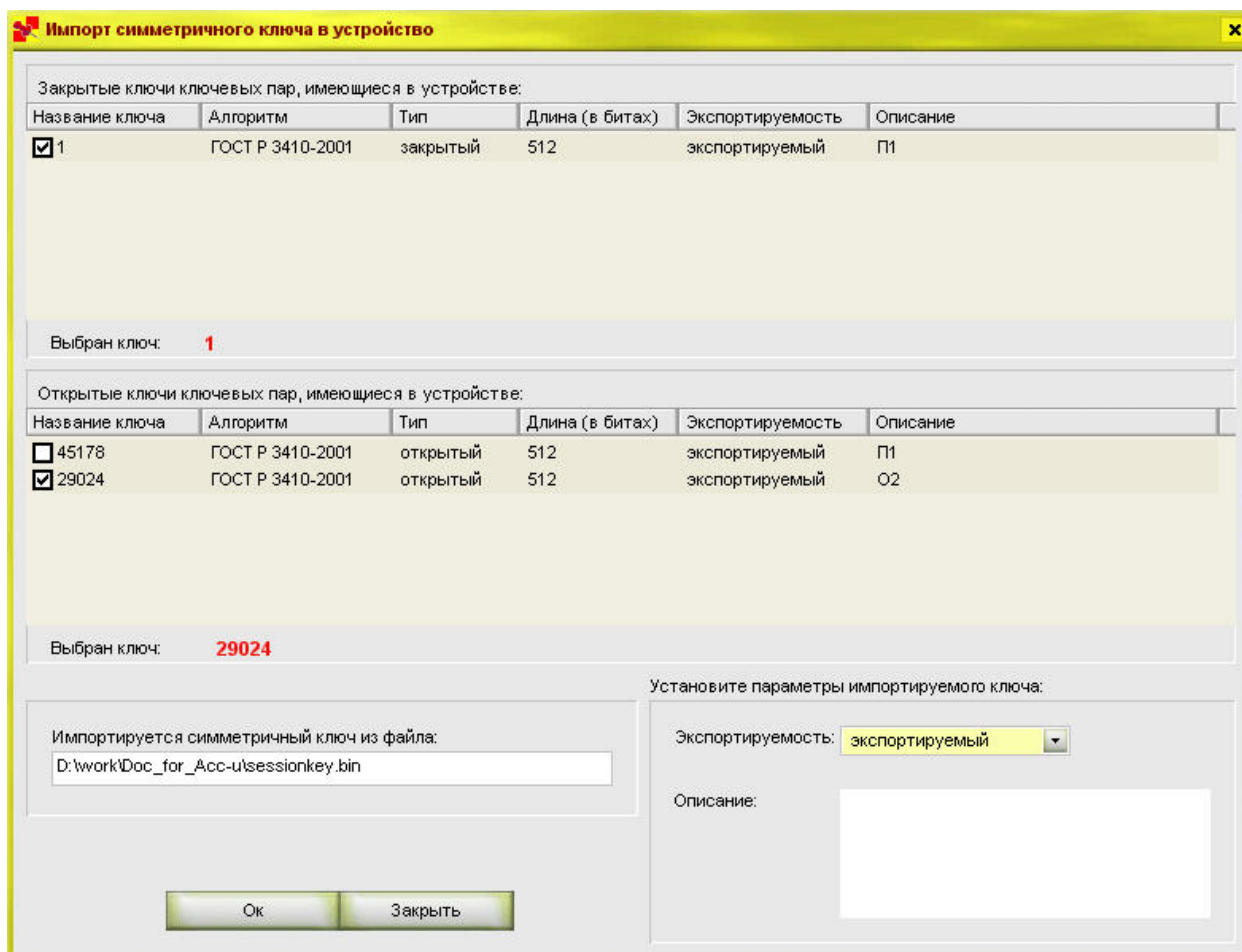


Рис. 26. Окно импорта симметричного ключа

В случае, если при выполнении импорта симметричного ключа возникла следующая ошибка (Рис. 27)

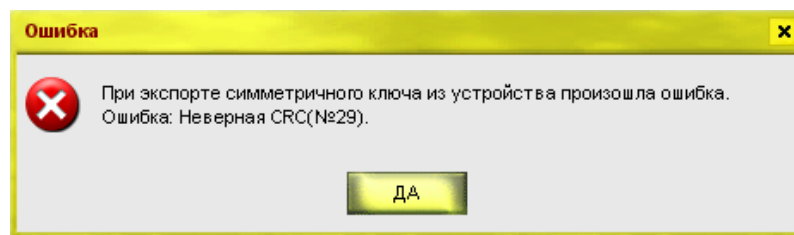


Рис. 27. Ошибка при импорте симметричного ключа

то возможной причиной является тот факт, что устройство пользователя, экспортировавшего симметричный ключ, использует более раннюю версию алгоритма экспорта/импорта. Порядок действий в этой ситуации указан в пункте 1 Приложения 1.

После сообщения об успешном завершении операции импорта импортированный симметричный ключ находится в защищенной памяти устройств №1 и №2. Теперь Вы можете обмениваться с Вашим партнером информацией, шифруя и расшифровывая файлы на этом ключе с помощью разных устройств АККОРД и ПСКЗИ ШИПКА.

Кроме обмена с абонентом, экспорт/импорт симметричного ключа может быть нужен еще в одном случае – если Вы не хотите хранить в устройстве ключи, которыми в данный момент не пользуетесь, но которые понадобятся Вам позже, или, например, если для работы Вам необходимо больше ключей, чем могут одновременно храниться в памяти устройства АККОРД. В этом случае симметричный ключ может быть экспортирован на своей ключевой паре, без участия импортированных ключей.

Для экспорта ключа ГОСТ используется пара ЭЦП ГОСТ Р 3410-2001.

Экспортированный таким образом ключ может быть импортирован только в то же самое устройство АККОРД, из которой был экспортирован. Каким-либо другим устройством или программой такой ключ применяться не может (так как для его расшифровки необходима пара, находящаяся в устройстве АККОРД).

Важно помнить, что ключевая пара, на которой был экспортирован симметричный ключ, не должна быть удалена из устройства, иначе импорт симметричного ключа будет невозможен.

В окне управления ключами можно удалить ключ (или ключевую пару), если он Вам не нужен для дальнейшей работы.

3.1.2. Шифрование файлов на диске

С использованием симметричных ключей, сгенерированных, как описано выше, можно выполнять процедуры шифрования с помощью программы «Шифрование и подпись файлов».

В главном окне программы «СКЗИ ОКБ САПР. Ключи: шифрование и подпись файлов» (Рис. 19) выбираем файл, нажимаем кнопку «Зашифровать» на панели задач. На экран выводится список ключей, которые хранятся в памяти устройства АККОРД и пользователю необходимо отметить один, на котором и будет выполнена операция (Рис. 28).

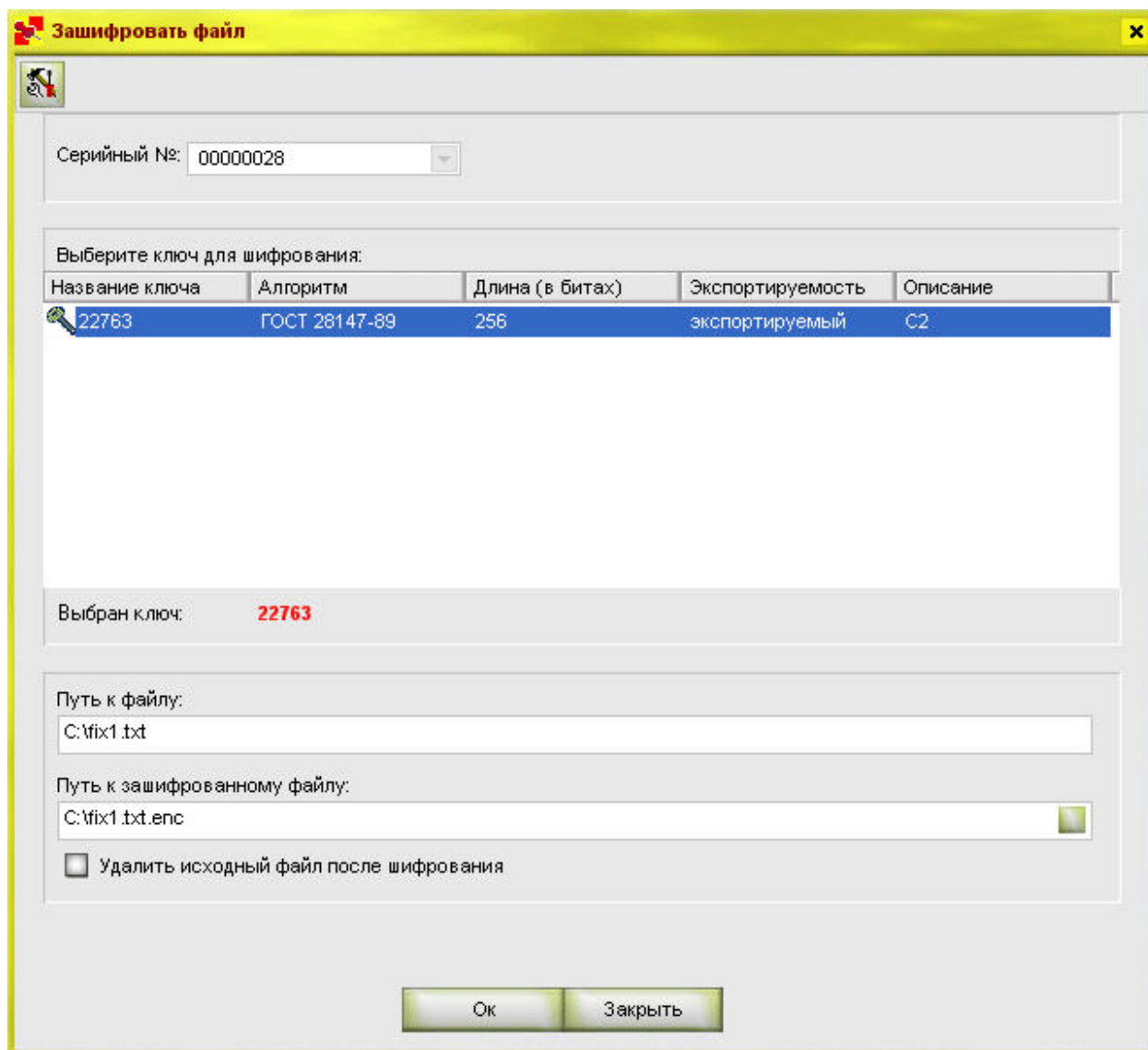


Рис. 28. Выбор ключа для шифрования из списка.

В нижней части окна можно установить флаг «Удалить исходный файл после шифрования». Нажимаем кнопку **Ок**, вводим PIN-код. Полученный зашифрованный файл имеет расширение *.enc.

Не бойтесь перепутать ключи! При расшифровке файла устройство само определит, на каком ключе был зашифрован или подписан файл (Рис. 29).

Для того чтобы расшифровать файл, нужно отметить нужный файл с расширением .enc и выбрать в меню «Файл» команду «Расшифровать» или щелкнуть мышью по кнопке «Расшифровать» на панели задач главного окна программы.

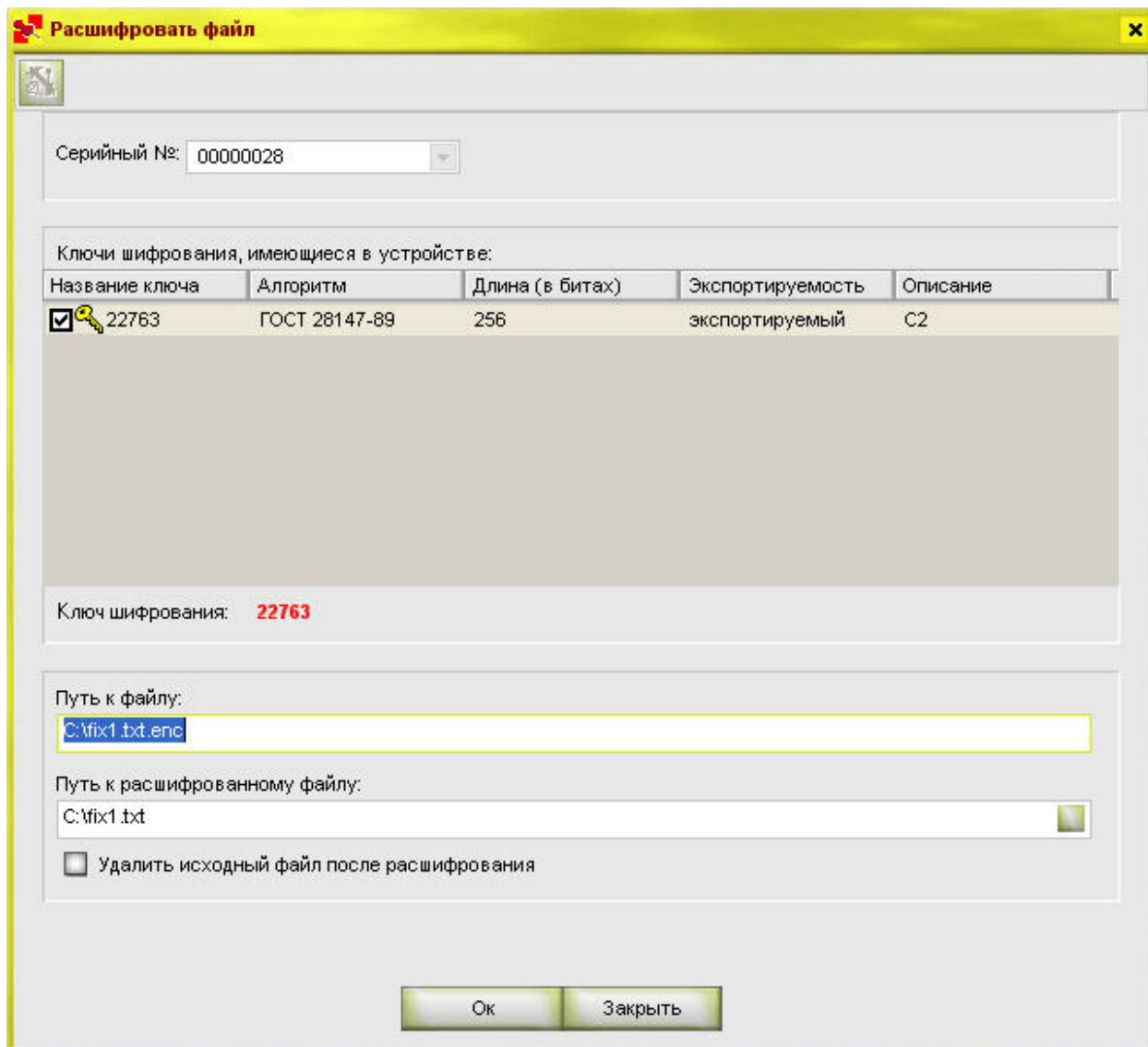


Рис. 29. Расшифровка файла. Ключ определяется автоматически

Если при попытке расшифровать файл (или проверить подпись) выдается следующее сообщение (Рис. 30), то это означает, что файл был зашифрован с помощью другого устройства АККОРД, или же ключ был удален из памяти устройства.

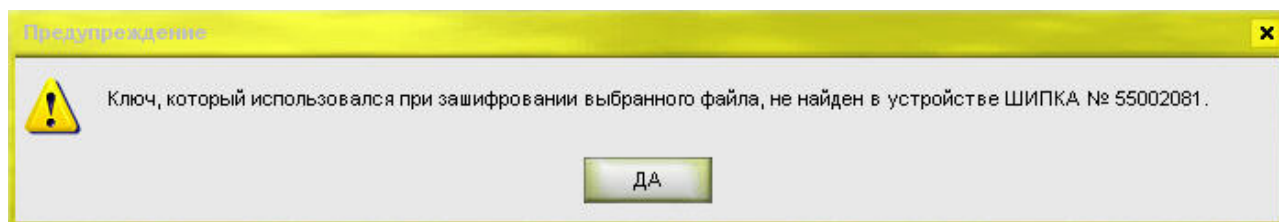


Рис. 30. Сообщение об ошибке при поиске ключа

3.1.3. Подпись файлов на диске

ВНИМАНИЕ! Если есть необходимость обработки файлов очень большого размера или папок с множеством файлов, рекомендуем их архивировать перед подписыванием.

В главном окне программы «СКЗИ ОКБ САПР. Ключи: шифрование и подпись файлов» (Рис. 19) выбираем файл, нажимаем кнопку «Подписать» на панели задач.

На экран выводится список ключей, которые хранятся в памяти Аккорда-У и пользователю необходимо отметить один, на котором и будет выполнена операция подписи (Рис. 31).

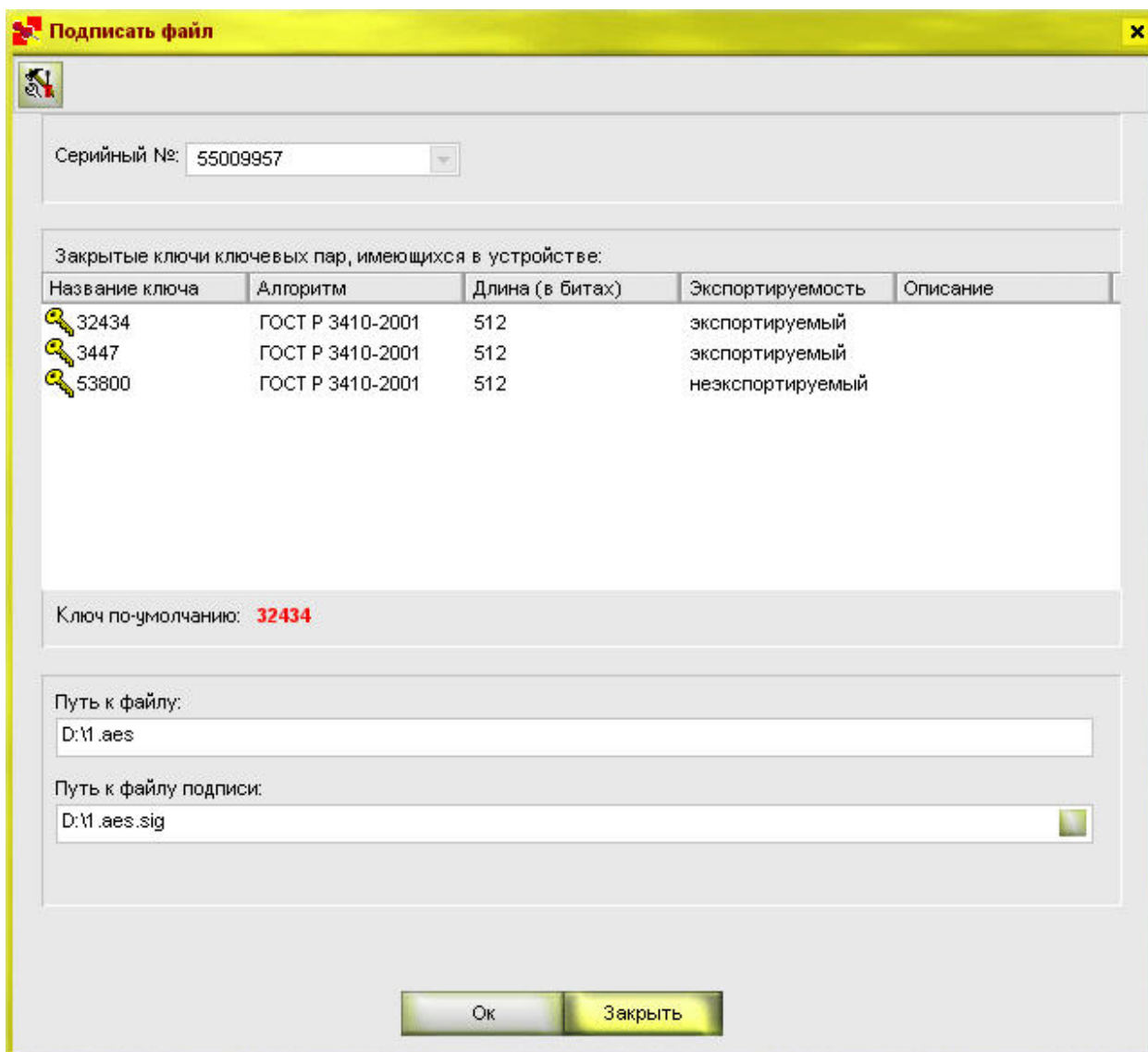


Рис. 31. Выбор ключа для подписи из списка

Выбираем один из ключей, нажимаем кнопку **Ок**, вводим PIN-код. Подпись файла по умолчанию лежит в той же директории, что и подписанный файл, и имеет расширение *.sig.

Можно выбрать другой файл и подписать его на том же или другом ключе.

Для того чтобы проверить подпись файла, нужно отметить файл подписи с расширением .sig и выбрать в меню «Файл» команду «Проверить» или щелкнуть мышью по кнопке «Проверить» на панели задач главного окна программы.

При проверке подписи файла программа сама определит, на каком ключе был подписан файл (Рис. 32).

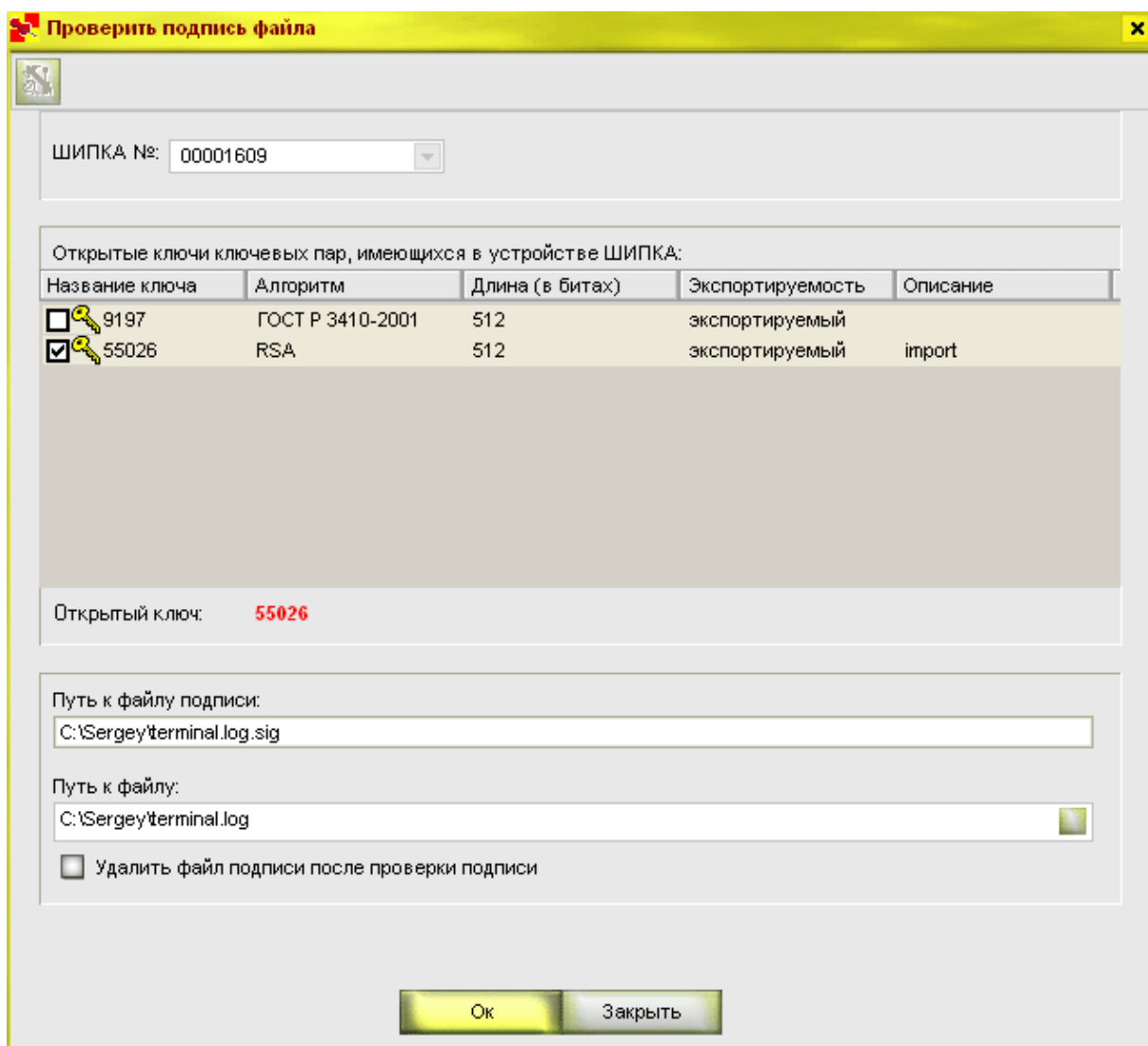


Рис. 32. Проверка подписи файла. Ключ определяется автоматически

Если открытый ключ, которым можно проверить выбранную подпись, отсутствует в памяти устройства, то при попытке проверить подпись выдается следующее сообщение (Рис. 33).

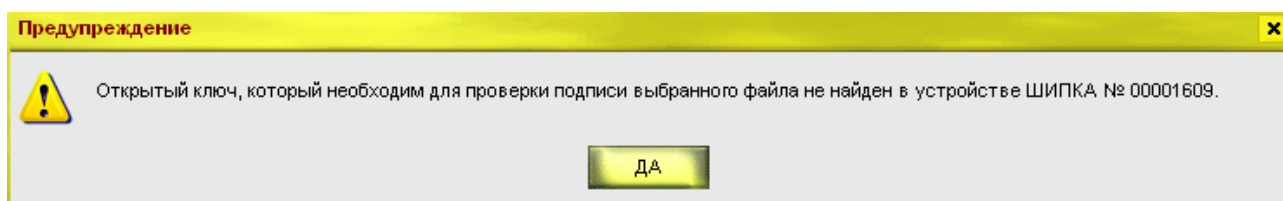


Рис. 33. Сообщение об ошибке при поиске ключа

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА

Аккорд-У и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора.

Авторские права на данное изделие принадлежат ЗАО «ОКБ САПР» (С), Россия, 115114, г. Москва, 2-й Кожевнический пер. д.8, тел. + 7 (495) 235 2990, 235 6265, факс: +7 (495) 234 0310, E-mail: okbsapr@okbsapr.ru.

Предприятие-изготовитель разрешает делать архивные копии программного обеспечения Аккорд-У для использования потребителем, который приобрел комплекс в установленном порядке.

Ни при каких обстоятельствах программное обеспечение Аккорд-У не должно распространяться между другими предприятиями (фирмами) и лицами. Удалять в продукции Аккорд-У уведомление об авторских правах недопустимо.

Применение Аккорд-У для целей, отличных от описанных в документации, возможно только при наличии письменного согласия ЗАО «ОКБ САПР».

Отметим, что эти ограничения не запрещают распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения Аккорд-У. Однако тот, кто получает от Вас такие исходные коды или модули, должен приобрести собственную копию нашего программного обеспечения, чтобы использовать его на законном основании, имея сертификат соответствия.

Относительно физических экземпляров аппаратуры и документации, поставляемых в составе Аккорд-У, предприятие-изготовитель гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в Формуляре.

При обнаружении ошибок или дефектов пользователь Аккорд-У должен направить в адрес предприятия-изготовителя подробный отчет о возникших проблемах, который позволит определить и зафиксировать проблему.

Аккорд-У поставляются по принципу «as is», т. е. предприятие-изготовитель (ОКБ САПР) ни при каких обстоятельствах не предусматривает никакой компенсации за Ваши дополнительные убытки, включая любые

потери прибыли, потери сохранности или другие убытки вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования комплекса.

При покупке и применении Аккорд-У предполагается, что Вы знакомы с данными требованиями и согласны с положениями настоящего раздела.

Контакты

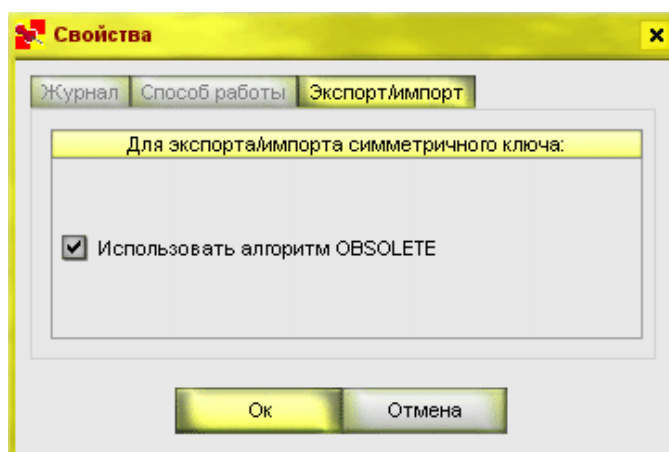
В случае необходимости консультации ОКБ САПР предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам (495) 235-78-17 и (495) 235-89-17 или по адресам электронной почты support@okbsapr.ru и help@shipka.ru. Наш адрес в Интернете www.accord.ru, www.shipka.ru .

Приложение 1. Возможные затруднения при работе с Аккорд-У и способы их решения

1. Как импортировать симметричный ключ ГОСТ 28147-89, если устройство пользователя, экспортировавшего симметричный ключ, использует более раннюю версию алгоритма экспорта/импорта?

Отметим, что алгоритм экспорта/импорта изменился в версиях внутреннего ПО, начиная с 44.57. Соответственно, указанная ситуация возникает в случае, если версия ПО пользователя, экспортировавшего ключ младше, а Ваша старше или в точности 44.57.

Для импорта необходимо выполнить следующие действия. В программе «Ключи: шифрование и подпись файлов» в меню «Настройки» выбрать пункт «Свойства». Зайти во вкладку «Экспорт/импорт» и выбрать «Использовать алгоритм OBSOLETE».



После этого импорт производится в порядке, описанном в пункте 3.1.1.2 «Экспорт/импорт ключевой информации» данной документации.

ВНИМАНИЕ! Не забудьте после окончания ключевого обмена с данным пользователем отключить эту опцию.

Приложение 2. Лицензионное соглашение по СКЗИ Аккорд-У

Настоящее лицензионное соглашение (далее – Соглашение) является документом, регулирующим отношения между Конечным пользователем (юридическим или физическим лицом), именуемым далее Пользователь, и ЗАО «ОКБ САПР», именуемым далее Разработчик.

Используя средство криптографической защиты информации (далее - СКЗИ) Аккорд-У и устанавливая специальное программное обеспечение, Пользователь принимает на себя обязательства по выполнению условий настоящего Соглашения. В случае несогласия с условиями Соглашения, Пользователь не должен устанавливать на своем компьютере или использовать какие-либо компоненты СКЗИ Аккорд-У.

СКЗИ Аккорд-У представляет собой комплекс, состоящий из аппаратной части - PCI/PCI-Express-устройства с внутренним программным обеспечением – и специального программного обеспечения (далее – СПО) на компакт-диске. СПО включает в себя драйверы, библиотеки и служебные программы и может устанавливаться на любой персональный компьютер, на котором Пользователь предполагает использовать аппаратную часть СКЗИ Аккорд-У.

Исключительные имущественные права на СКЗИ Аккорд-У принадлежат Разработчику. Право собственности и авторские права на СПО, компоненты и любые копии СПО принадлежат Разработчику.

Пользователь при приобретении СКЗИ Аккорд-У получает от Разработчика неисключительное возмездное право (неисключительную платную лицензию) на его использование.

Пользователю предоставляется право создавать копии СПО исключительно в архивных целях. Порядок использования архивных копий устанавливается законодательством РФ.

Ни при каких обстоятельствах СПО СКЗИ Аккорд-У не должно распространяться между другими организациями и лицами. Удалять в продукции СКЗИ Аккорд-У уведомление об авторских правах недопустимо.

Применение СКЗИ Аккорд-У для целей, отличных от описанных в документации, возможно только при наличии письменного согласия Разработчика.

Разработчик без ущерба для любых других своих прав вправе прекратить действие настоящего Соглашения при несоблюдении (или неспособности далее выполнять его условия) Пользователем условий

данного Соглашения. Никакие уплаченные Пользователем суммы не подлежат возврату в случае такого прекращения.

Пользователь может прекратить действие настоящего Соглашения в любое время, полностью прекратив использование комплекса СКЗИ Аккорд-У. Никакие уплаченные Пользователем суммы не подлежат возврату в случае такого прекращения.

Настоящее Соглашение регулируется действующим законодательством Российской Федерации. Недействительность какого-либо положения настоящего Соглашения не влечет за собой недействительность остальных его положений.

Пользователь принимает на себя в полном объеме риск использования СКЗИ Аккорд-У.