



ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Средство криптографической защиты информации

АККОРД-У

Руководство по быстрой установке

11443195.4012-023

Листов 16

Москва

2010

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.

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.

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).

2. Установка системного драйвера устройства АККОРД

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». Следует выбрать пункт «Автоматическая установка» и нажать кнопку «Далее».

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 ТМ-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 – 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: 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».

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. 1).

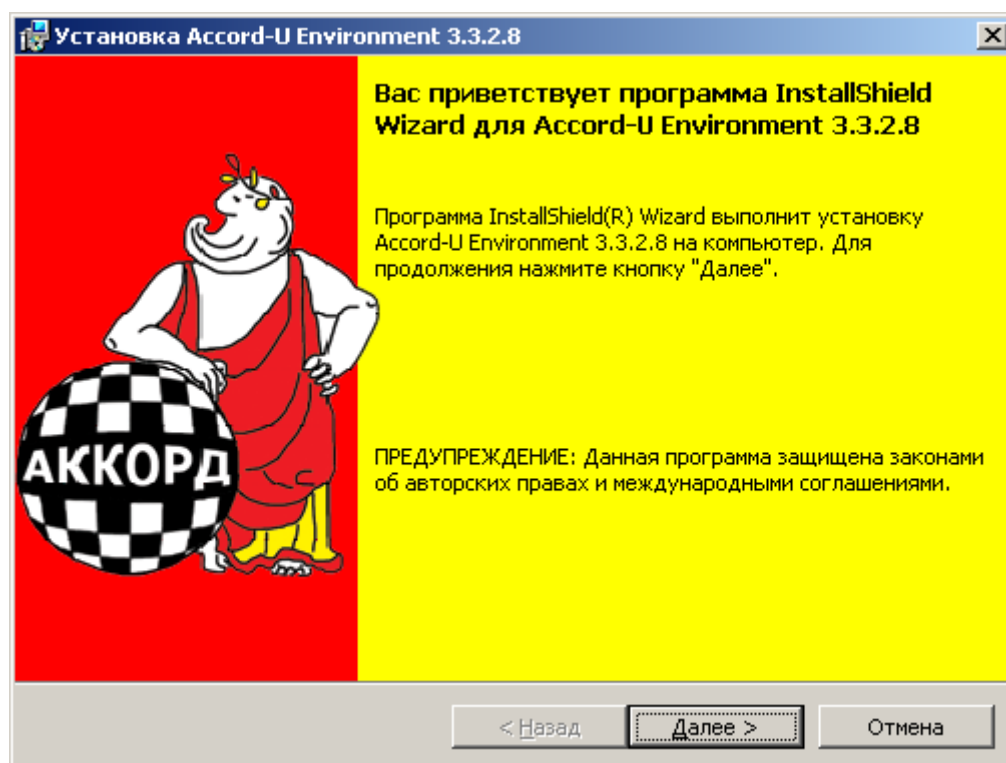


Рис.1. Стартовое окно процедуры инсталляции

Для продолжения процедуры нужно щелкнуть левой клавишей мыши по кнопке «Далее».

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

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

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. 2).

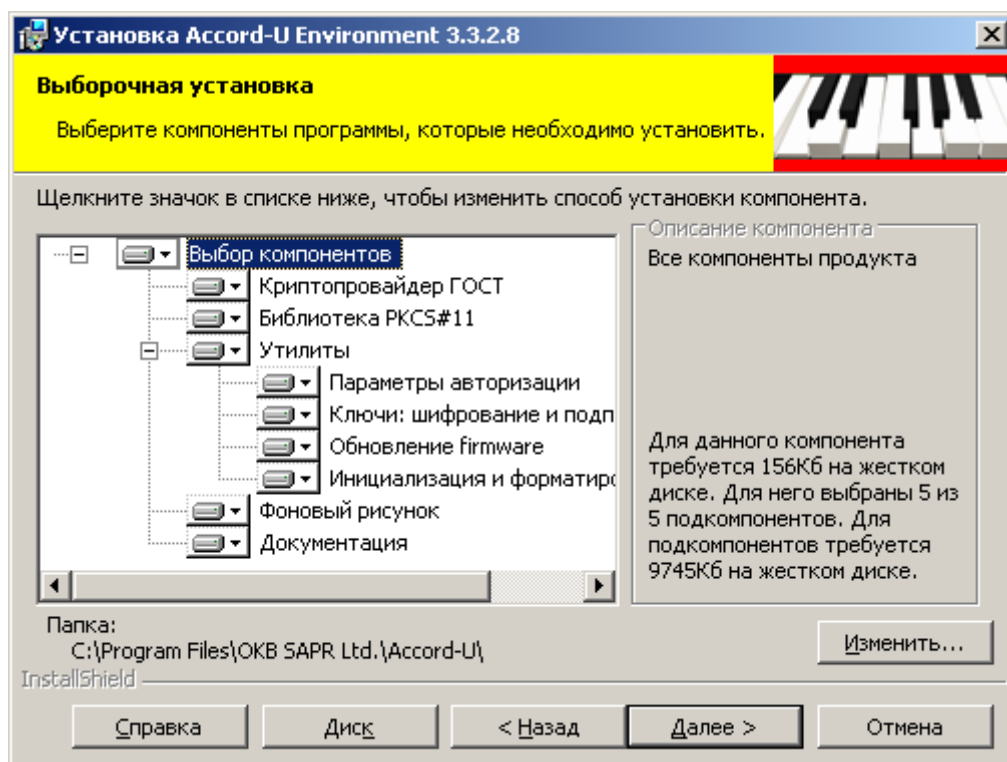


Рис.2. Окно выбора установки отдельных компонентов

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).

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 установить ПО Аккорд-У выдается окно «Обслуживание программ» (Рис. 3), это значит, что у Вас уже установлено ПО Аккорд-У. Если Вы устанавливаете более новое ПО, то нужно выбрать «Удалить» и деинсталлировать старое.

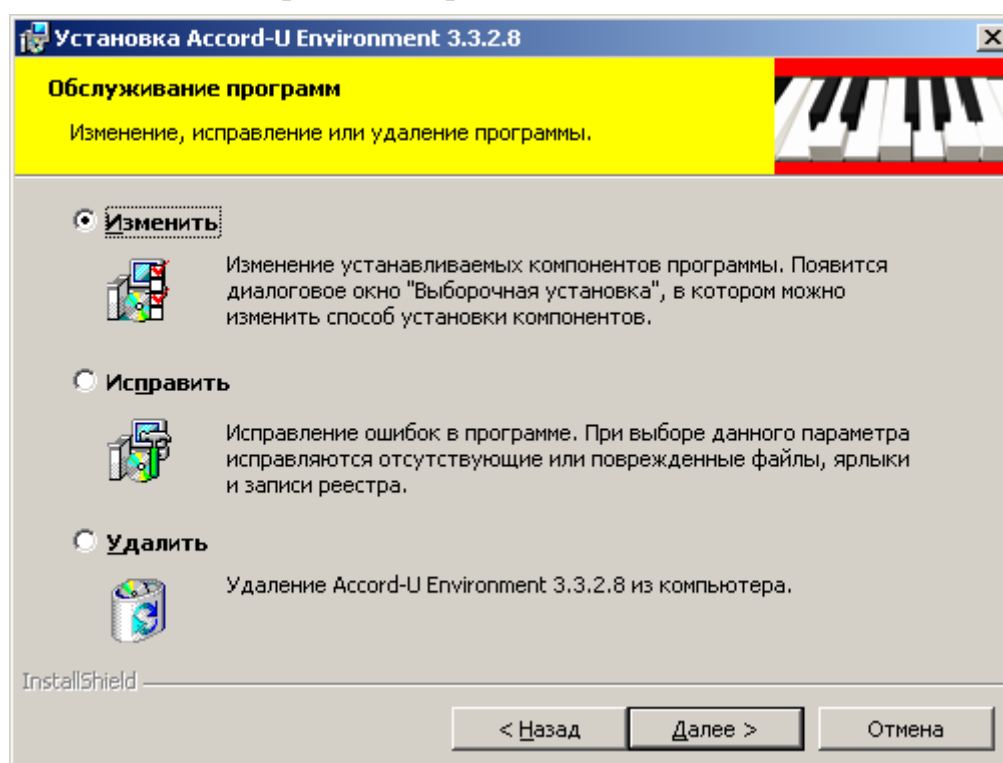


Рис.3. Окно «Обслуживание программ»

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>.

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 *отформатированное** 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. 3).

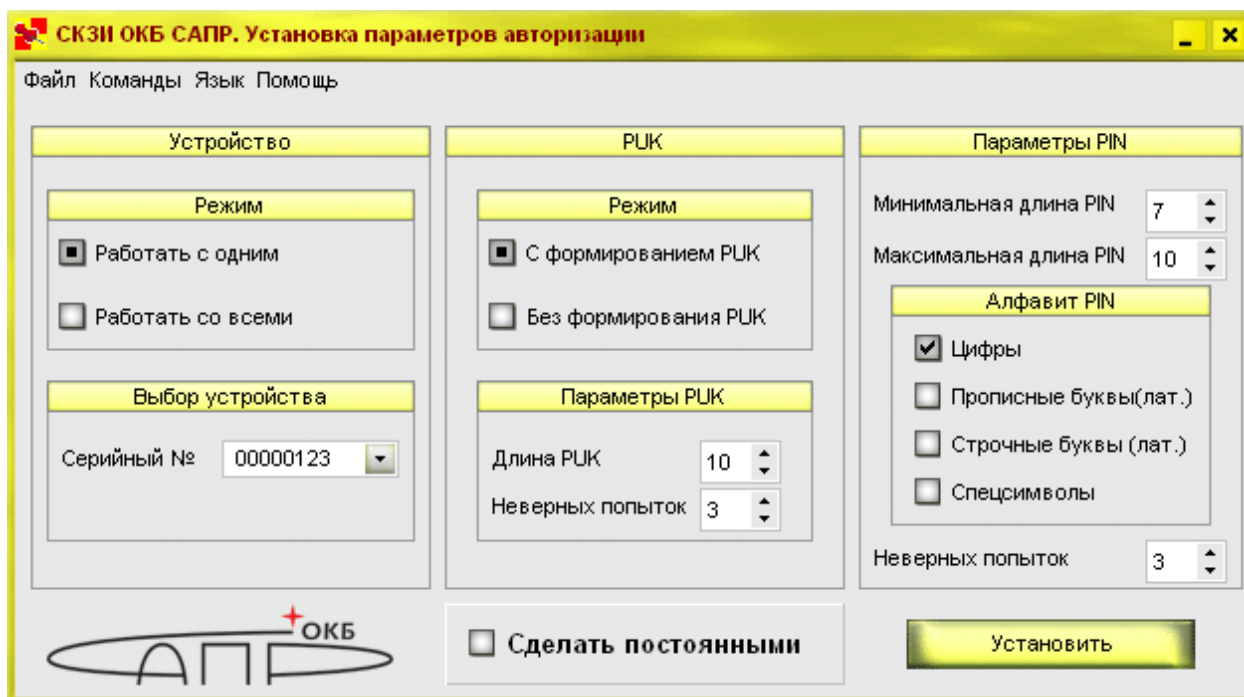


Рис. 3. Окно установки параметров авторизации Аккорда-У

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 формированием PUK», или «Без формирования 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. 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. 4) три закладки: «Сменить PIN», «Форматировать» и «Разблокировать».

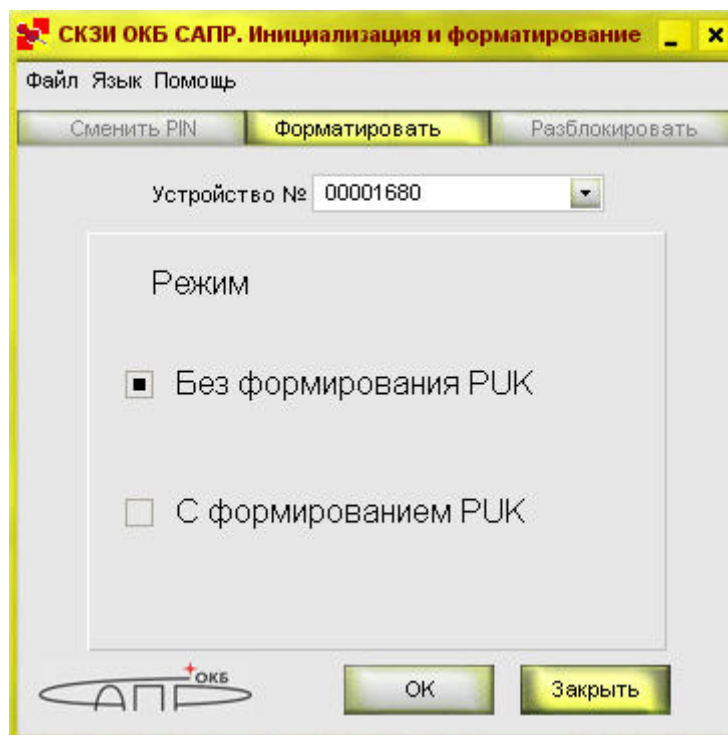


Рис. 4. Форматирование устройства АККОРД

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. 5).

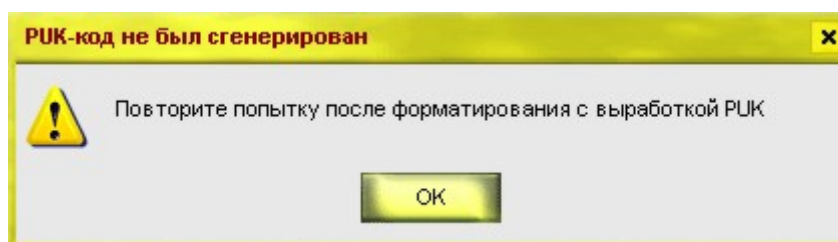


Рис.5. Предупреждение о невозможности отформатировать данные криптографической подсистемы устройства АККОРД без формирования PUK-кода

В процессе выполнения операции выводится окно со сгенерированным PUK-кодом и предложением сохранить этот PUK-код в файл (Рис. 6).

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.

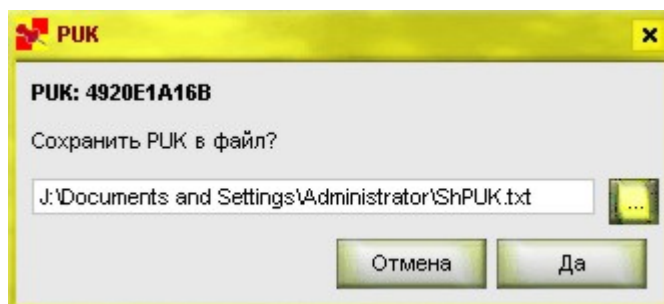


Рис.6. Запрос на сохранение PUK-кода в файл

Форматирование и успешное сохранение PUK-кода подтверждается сообщением с указанием пути к файлу (Рис. 7).

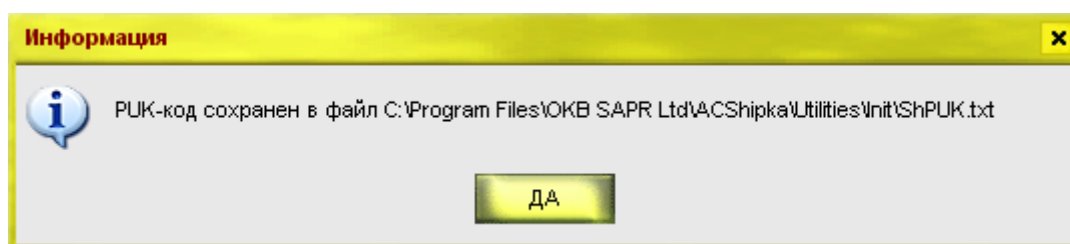


Рис.7. Подтверждение записи PUK-кода в файл

Последующие форматирования можно производить и без выработки PUK-кода, и тот PUK, что был выработан последним, будет оставаться действительным (Рис. 8).

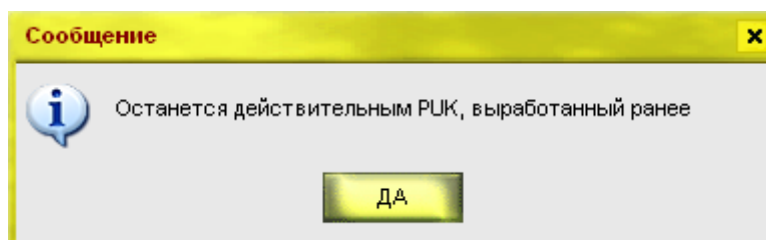


Рис. 8. Сообщение, выводящееся в том случае, если производится форматирование без выработки нового PUK-кода, а в Параметрах авторизации задано правило «Форматирование с выработкой PUK»

5. Установка PIN-кода для криптографической подсистемы устройства АККОРД

Следующий этап в работе с криптографической подсистемой устройства АККОРД – установка PIN-кода. 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. 9).

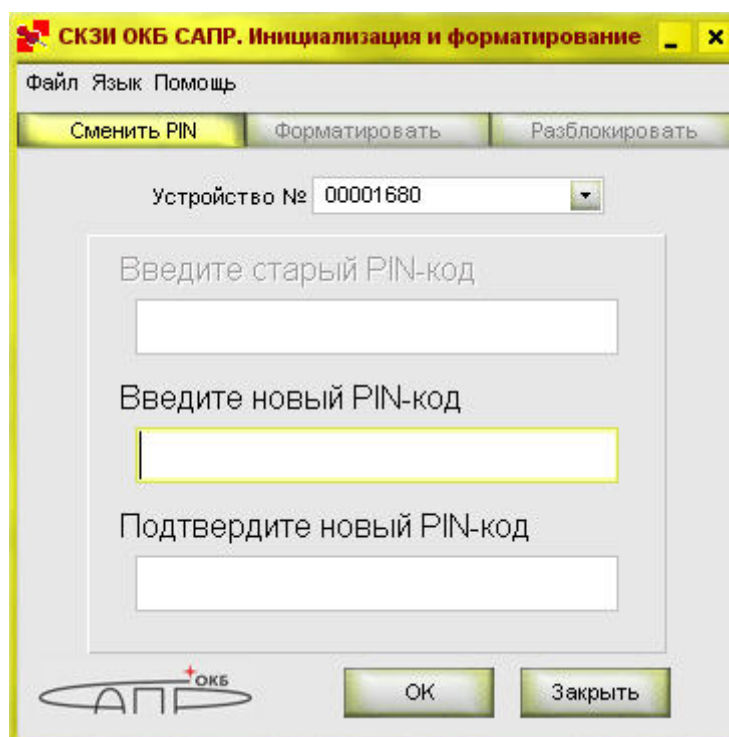


Рис. 9. Процедура ввода нового PIN-кода

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. 10).

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

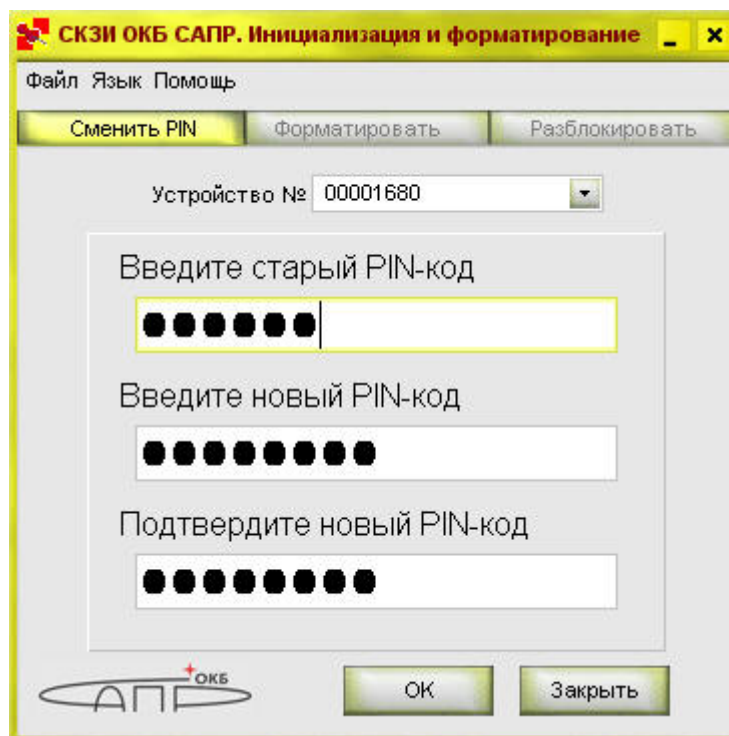


Рис.10. Смена установленного PIN-кода для криптографической подсистемы устройства АККОРД