



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Флешка «Секрет Фирмы»
Инструкция по настройке

Москва
2012

АННОТАЦИЯ

В этом документе описаны действия Администратора флешки «Секрет Фирмы» (или просто «Секрет»), то есть непосредственно того человека, который будет ее настраивать, а не того, кто будет записывать на нее и считывать с нее файлы.

«Секрет» используется как служебная флешка и выдается на работе. Настраивать «Секрет» должен специально назначенный сотрудник – Администратор, имеющий необходимые знания и полномочия. Пользователь «Секрета Фирмы» является исключительно оператором «Секрета», т.е. подключает флешку к компьютеру, записывает на нее и считывает с нее служебную информацию (но не может настраивать «Секрет»).

В этом документе написано, как устанавливать и настраивать «Секрет», и другие функции, которые в работе с «Секретом» должен выполнять Администратор.

Прежде чем устанавливать и настраивать «Секрет», обязательно прочитайте эту инструкцию.

В любом случае относитесь внимательно к своему компьютеру и хранимым на нем данным!

СОДЕРЖАНИЕ

АННОТАЦИЯ	2
1. Общие сведения.....	5
1.1. Из чего состоит и для чего предназначен «Секрет Фирмы»	5
1.2. Что нужно для применения Секрета	6
1.3. Комплектность поставки «Секрета Фирмы»	6
2. Установка и настройка комплекса «Секрет Фирмы»	7
2.1. Установка ПО комплекса «Секрет Фирмы»	7
2.1.1. Установка ПО «АРМ Администратора»	7
2.1.2. Установка ПО «Секретный Агент»	11
2.2. Подключение «Секрета Фирмы» и флешки Сервера Аутентификации (флешки СА).....	16
2.3. Установка системного драйвера «Секрета» и флешки СА.....	16
2.4. Начало работы.....	19
3. Управление «Секретом»	21
3.1. Создание эталонной флешки СА.....	21
3.2. Дублирование флешек СА.....	24
3.3. Регистрация «Секрета Фирмы».....	28
3.4. Подготовка «Секрета» к работе	33
3.4.1. Настройка списков доступа	33
3.4.2. Настройка сетевых параметров	36
3.5. Загрузка ключевой информации флешки СА в сервис СА.....	36
3.6. Регистрация «Секрета Фирмы» на другом компьютере.....	38
3.6.1. Подготовка «Секрета» к регистрации на другом компьютере (повторной регистрации).....	38
3.6.2. Повторная регистрация «Секрета».....	41
3.7. Отмена регистрации «Секрета Фирмы»	44
3.8. Смена PIN-кода флешки СА	47
3.9. Смена PIN-кода флешки «Секрет».....	49
3.10. Разблокирование «Секрета»	53
3.11. Разблокирование флешки СА	57
4. Журнал регистрации событий	59
5. Как применять «Секрет Фирмы» безопасным образом	65
5.1. Общие сведения	65
5.2. Вход в систему с обязательным вводом пароля	65
5.3. Включение режима автоматической блокировки экрана.....	66

6. Перечень принятых сокращений и обозначений.....	68
7. Возможные сообщения в журнале событий «Секрета Фирмы»	68

1. Общие сведения

1.1. Из чего состоит и для чего предназначен «Секрет Фирмы»

«Секрет Фирмы» - это комплект, в который входят:

- 1) флешка «Секрет Фирмы» («Секрет»);
- 2) 2 специальных флешки сервера аутентификации (эталонная и рабочая);
- 3) 2 специальных флешки эмитента (эталонная и рабочая). Эмитент позволяет различать флешки «Секрет Фирмы», принадлежащие различными организациями;
- 4) диск с:
 - программным обеспечением (ПО) рабочей станции (РС) – «Секретный Агент», которое устанавливается на «свои» компьютеры;
 - ПО Сервера Аутентификации или СА – «АРМ Администратора» (устанавливается на отдельный компьютер сети), с помощью этого ПО Администратор может настраивать флешку «Секрет»;
 - ПО эмиссии, которое устанавливается на отдельный компьютер.

ПО эмиссии и ПО Сервера Аутентификации поставляются только в том случае, если их наличие оговаривается при заказе!

Флешка «Секрет Фирмы» предназначена для защищенного хранения и переноса корпоративной информации. То есть то, что на нее записано, может прочитать только тот Пользователь, чья это флешка, и только на тех компьютерах, на которых ему можно. «Секрет Фирмы» нельзя использовать дома или где-то еще.

ПО «Секретный Агент» предназначено для опознавания «Секрета» на компьютере и компьютера в «Секрете» с участием СА: чтобы «Секрет» выяснил, «свой» или «чужой» компьютер, можно открываться или нельзя.

ПО «Секретный Агент» устанавливается на компьютер и требует для установки примерно 20 Mb памяти.

ПО «АРМ Администратора» предназначено для удаленного опознавания «Секрета» на компьютере и администрирования (настройки) «Секрета».

ПО «АРМ Администратора» устанавливается на отдельный компьютер и требует для установки примерно 40 Mb памяти.

ПО эмиссии нужно для того, чтобы отличить «Секрет Фирмы» «своей» организации от «Секрета» «чужой» организации.

ПО РС устанавливается на отдельный компьютер и требует для установки примерно 16 Mb памяти.

«Секрет Фирмы» может использоваться на компьютерах типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP/Vista/7 SP1 (x32 или x64).

Доступ к защищаемой информации предоставляется только на тех компьютерах, на которых именно этот «Секрет» был зарегистрирован его владельцем, и только после ввода PIN-кода, известного владельцу. Незарегистрированный «Секрет» не обнаруживается операционной системой компьютера как флешка и его PIN-код не запрашивается. Поэтому если «Секрет» украли или случайно нашли, то прочитать из него файлы – не смогут.

1.2. Что нужно для применения Секрета

1) для рабочей станции:

- установленная ОС Microsoft Windows XP/Vista/7 SP1 (x32 или x64);
- свободный разъем USB;
- объем дискового пространства для размещения программного обеспечения на жестком диске компьютера – примерно 20 Мбайт;
- связь с сервером аутентификации с использованием протоколов TCP/IP;

2) для сервера аутентификации (в случае, если поставляется не в сборе, а только ПО):

- установленная ОС Microsoft Windows XP/2003/Vista/2008/7 SP1 (x32 или x64);
- два свободных разъема USB;
- ПАК «Аккорд-Win32» («Аккорд-Win64»);
- объем дискового пространства для размещения программного обеспечения на жестком диске ПЭВМ – примерно 40 Мбайт;
- связь с рабочими станциями с использованием протоколов TCP/IP;

3) для АРМ эмиссии (в случае, если поставляется не в сборе, а только ПО):

- установленная ОС Microsoft Windows XP/2003/Vista/2008/7 SP1 (x32 или x64);
- два свободных разъема USB;
- ПАК «Аккорд-Win32» («Аккорд-Win64»);
- объем дискового пространства для размещения программного обеспечения на жестком диске ПЭВМ – примерно 16 Мбайт.

1.3. Комплектность поставки «Секрета Фирмы»

«Секрет Фирмы» поставляется в составе:

- флешка «Секрет Фирмы»;
- CD со специальным ПО и инструкциями;
- гарантийный талон;
- комплект упаковки.

ВНИМАНИЕ! Для подключения к компьютеру двух или более флешек (флешка «Секрет Фирмы», флешка СА, флешка эмиссии) может использоваться USB-хаб. В этом случае USB-хаб должен быть подключен к собственному источнику питания.

2. Установка и настройка комплекса «Секрет Фирмы»

2.1. Установка ПО комплекса «Секрет Фирмы»

Сначала на СА и «свои» компьютеры нужно установить программы «АРМ Администратора» и «Секретный Агент».

ВНИМАНИЕ! Если у Вас уже были раньше установлены эти программы, то сначала их нужно удалить, перезагрузить компьютер, а потом уже устанавливать новые версии этих программ.

2.1.1. Установка ПО «АРМ Администратора»

ВНИМАНИЕ! При приобретении СА в сборе выполнять этот пункт не нужно, следует сразу перейти к пункту 2.1.2.

Для управления флешкой «Секрет Фирмы» необходимо установить на СА ПО «АРМ Администратора».

Для этого следует запустить с CD, входящего в комплект поставки, файл SetupSecretBusinessServer_v1.0.exe¹.

После этого на экране появляется окно с общей информацией, в котором нажимаем кнопку <Далее> (рисунок 1).

¹⁾ Для ОС x64 этот файл имеет название SetupSecretBusinessServer_v1.0_x64.exe

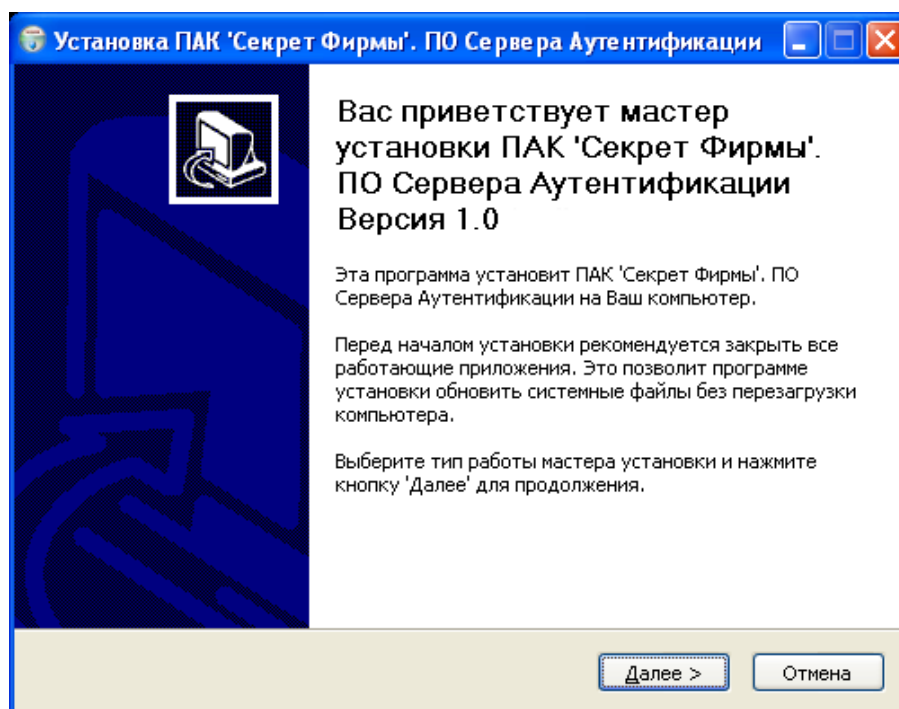


Рисунок 1 - Стартовое окно процедуры установки ПО СА

В следующем окне выбираем, все мы будем устанавливать на компьютер или нет, и нажимаем кнопку <Далее> (рисунок 2).

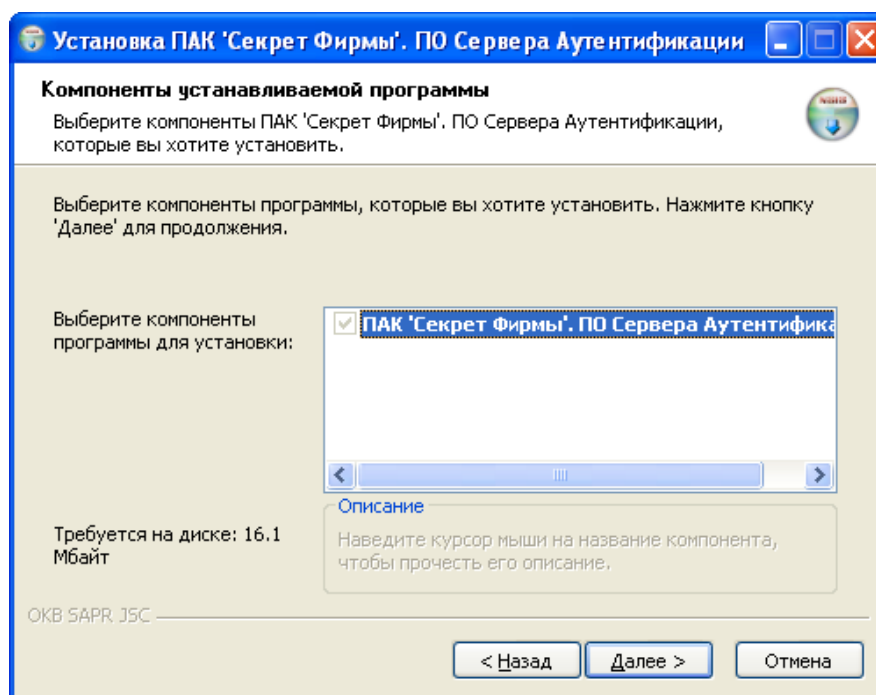


Рисунок 2 – Окно выбора компонентов устанавливаемого ПО СА

В следующем окне указываем, куда именно на компьютере установить программу (рисунок 3). Если ничего специально не указывать, то будет \Program Files\OKB SAPR JSC\Secret\Business\Server. Каталог (папка, в которую будет установлено ПО), предлагаемый программой, может быть изменен с помощью кнопки <Обзор...>. Если указанного каталога, в который Вы хотите

установить ПО, не существует, то он будет создан программой установки автоматически.

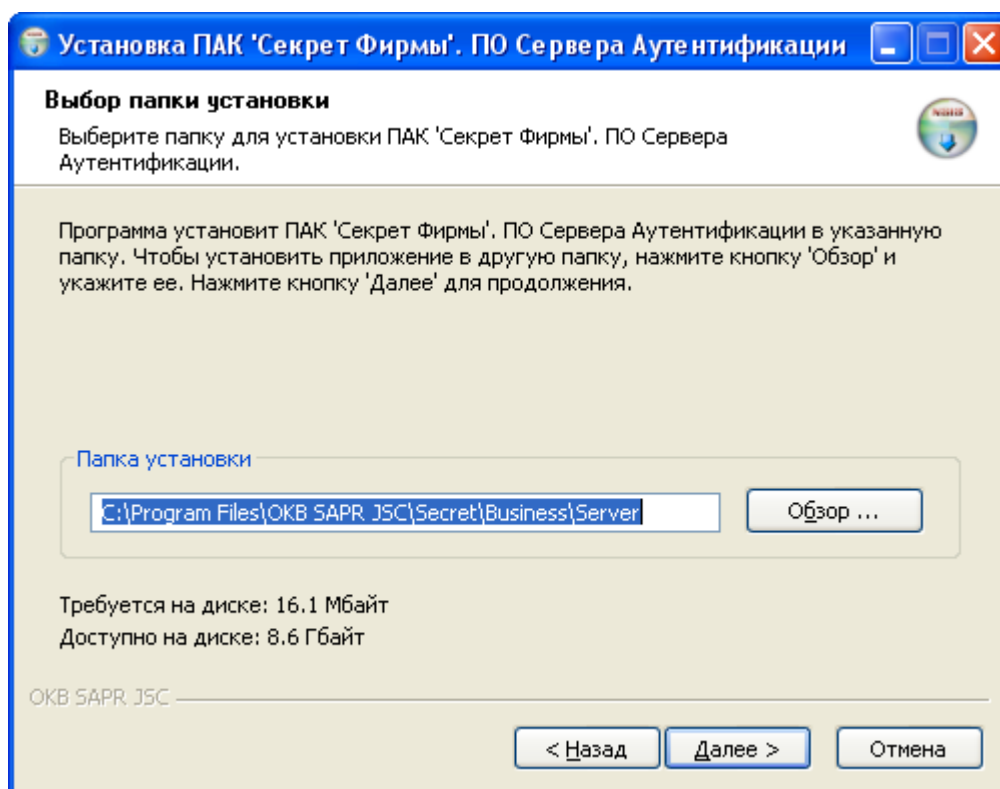


Рисунок 3 - Выбор каталога установки ПО СА

Потом нажимаем <Далее>, выбираем место, где именно в меню «Пуск» будут находиться ярлыки программы, и нажимаем <Установить>. Файлы начнут копироваться (рисунок 4).

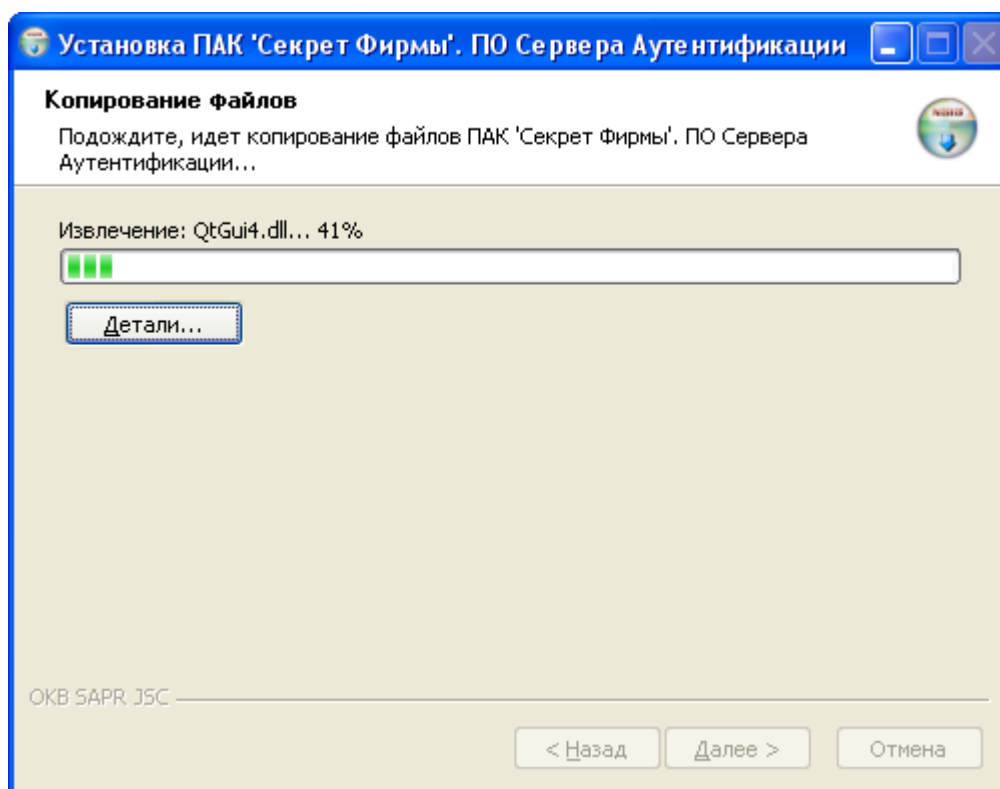


Рисунок 4 - Установка программных компонентов ПО СА

В процессе установки на экране может появиться предупреждающее сообщение (рисунок 5), это нормально. Выберите пункт <Все равно продолжить>.

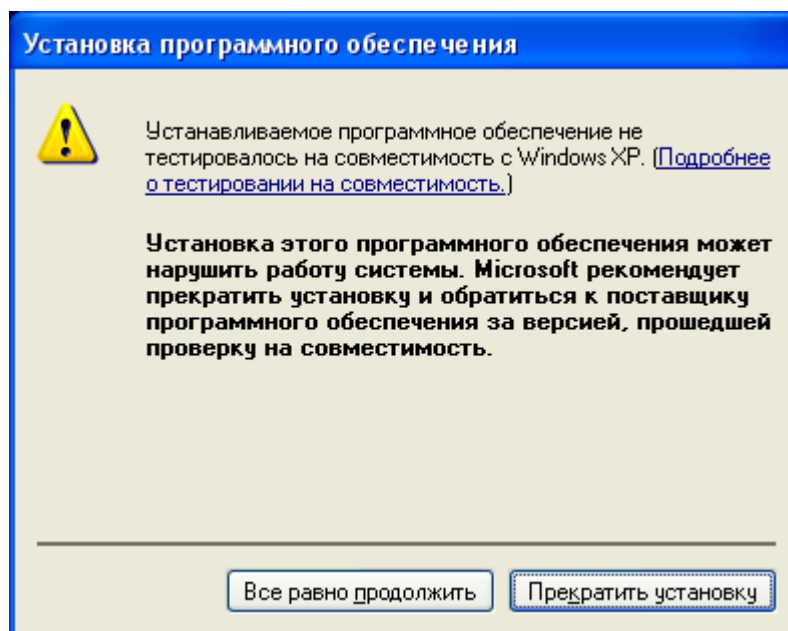


Рисунок 5 - Предупреждающее сообщение

Когда появится окно со словами о том, что установка выполнена (рисунок 6), нужно нажать кнопку <Готово>.

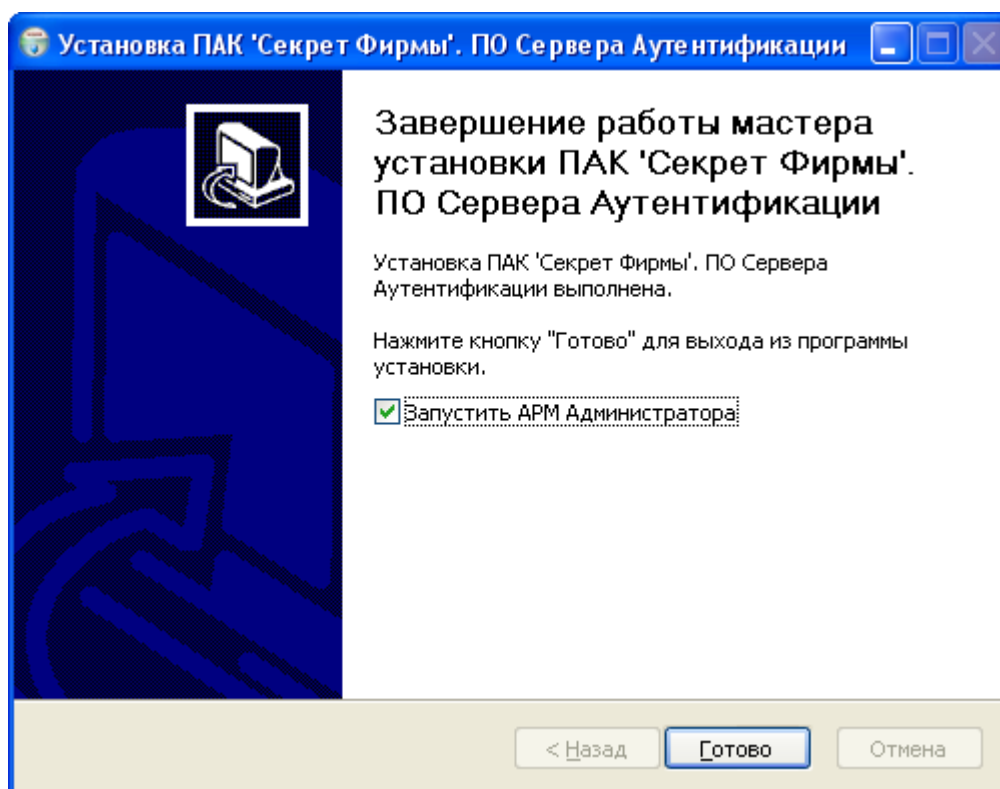


Рисунок 6 - Окно завершения установки ПО СА

Теперь можно настраивать флешку «Секрет».

ВНИМАНИЕ! Для работы с ПО «АРМ Администратора» на СА должна быть установлена плата «Аккорд»¹. Это позволит защитить все «свои» компьютеры от взлома и кражи информации.

При отсутствии платы «Аккорд» работа с «Секретом» невозможна.

Если Вы приобрели СА в сборе, то все необходимые компоненты на него предустановлены производителем!

Если на СА не установлена плата «Аккорд», то после запуска ПО «АРМ Администратора» на экран выводится сообщение (рисунок 7).

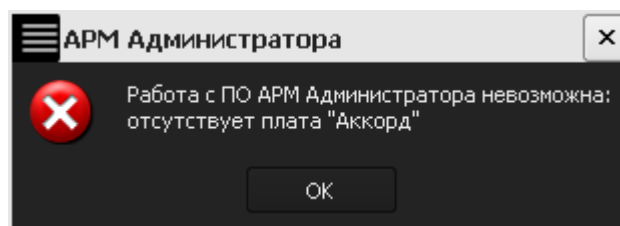


Рисунок 7 – Предупреждающее сообщение

2.1.2. Установка ПО «Секретный Агент»

До начала использования флешки «Секрет Фирмы» на компьютер (рабочую станцию) должно быть установлено ПО рабочей станции («Секретный

¹) Подробнее см. на сайте www.accord.ru.

Агент»). Для этого нужно запустить с CD, входящего в комплект поставки, файл SetupSecretBusinessWorkStation__v1.0.exe¹.

После этого на экране появляется окно с общей информацией, в котором нажимаем кнопку <Далее> (рисунок 8).

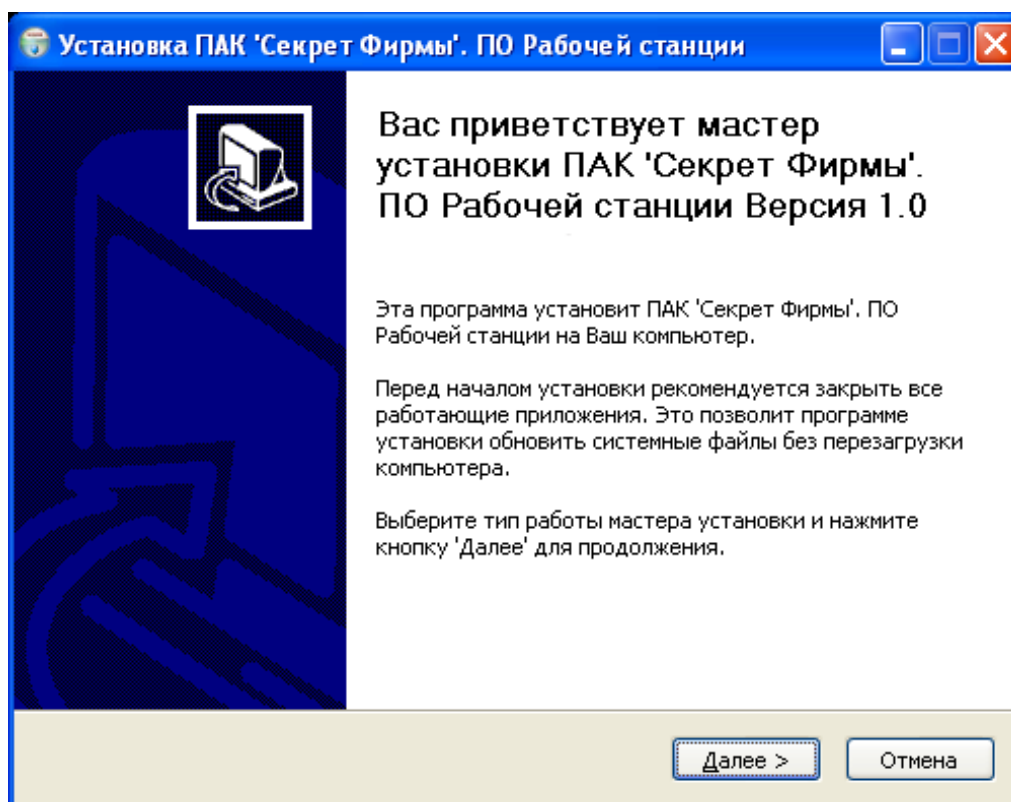


Рисунок 8 – Стартовое окно процедуры установки ПО компьютера

В следующем окне выбираем, все мы будем устанавливать на компьютер или нет, и нажимаем кнопку <Далее> (рисунок 9). «Все» – это:

- «Секрет Фирмы» – ПО рабочей станции («Секретный Агент»). Устанавливается в любом случае;
- Фильтр USB-устройств, с помощью которого на данном компьютере можно запретить использовать любые другие флешки кроме «Секрета».

¹⁾ Для ОС x64 исполняемый файл имеет название SetupSecretBusinessWorkStation_v1.0_x64.exe

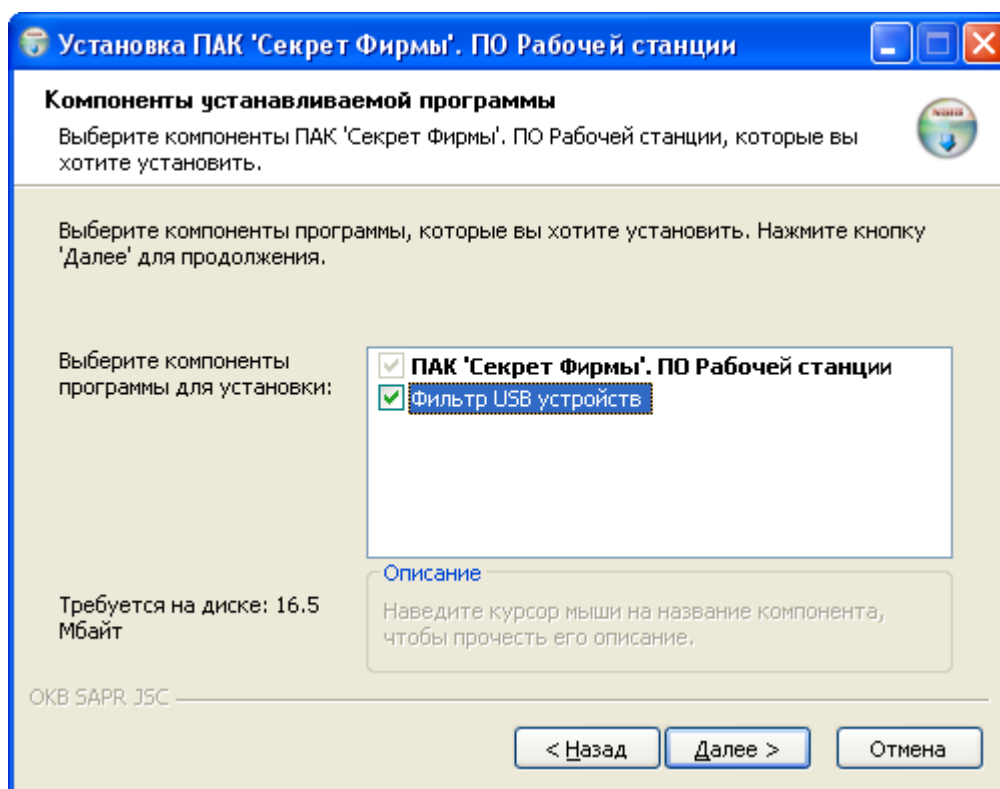


Рисунок 9 – Окно выбора компонентов устанавливаемого ПО компьютера

В следующем окне указываем, куда именно на компьютере установить программу (рисунок 10). Если ничего специально не указывать, то будет \Program Files\OKB SAPR JSC\Secret\Business\WorkStation. Каталог (папка, в которую будет установлено ПО), предлагаемый программой, может быть изменен с помощью кнопки <Обзор...>. Если указанного каталога, в который Вы хотите установить ПО, не существует, то он будет создан программой установки автоматически.

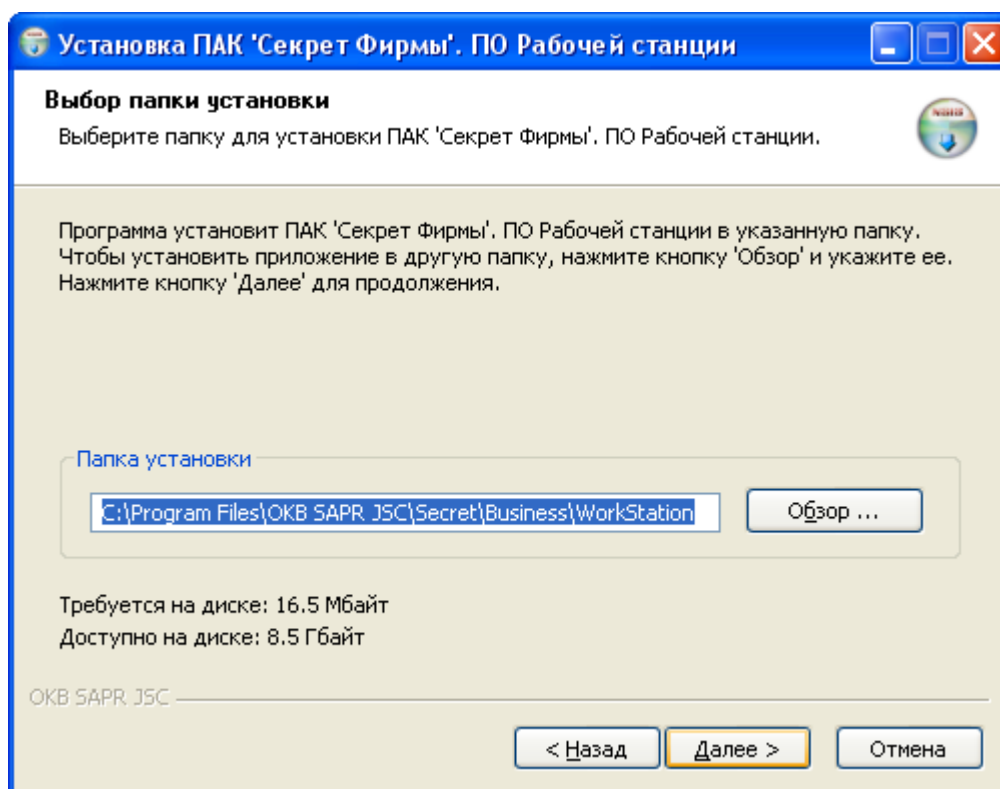


Рисунок 10 - Выбор каталога установки ПО компьютера

Потом нажимаем <Далее> выбираем место, где именно в меню «Пуск» будут находиться ярлыки программы, и нажимаем <Установить>. Файлы начнут копироваться (рисунок 11).

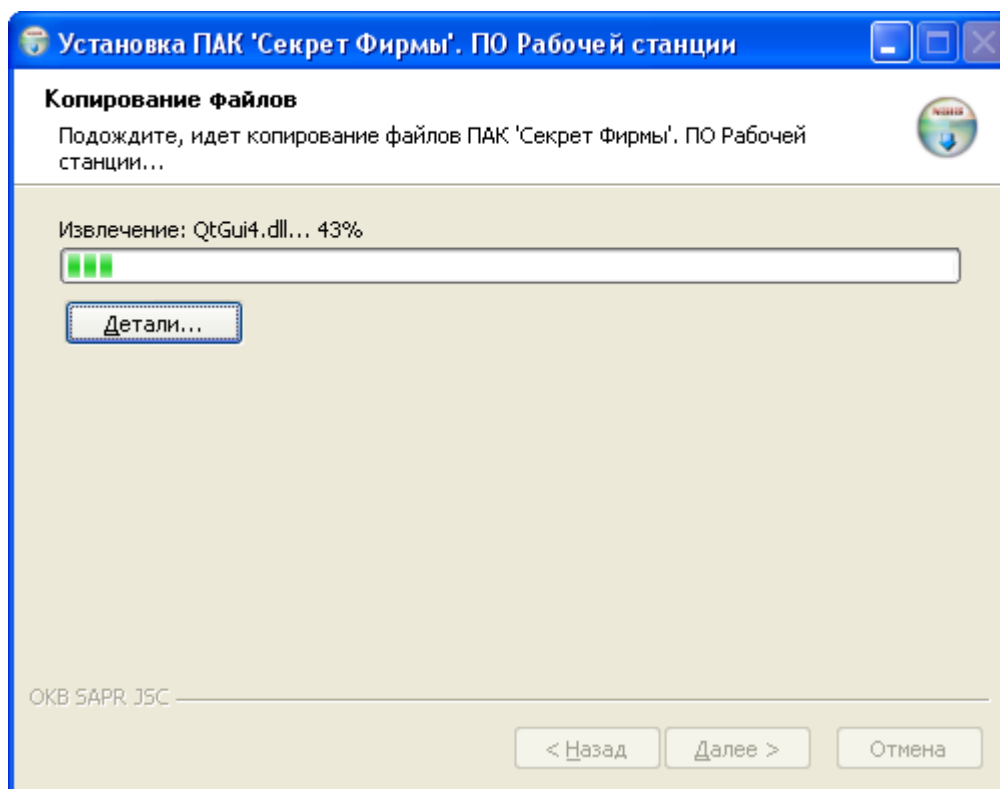


Рисунок 11 - Установка программных компонентов ПО компьютера

В процессе появится окно с предупреждением (рисунок 12), это нормально, выбираем <Все равно продолжить>.

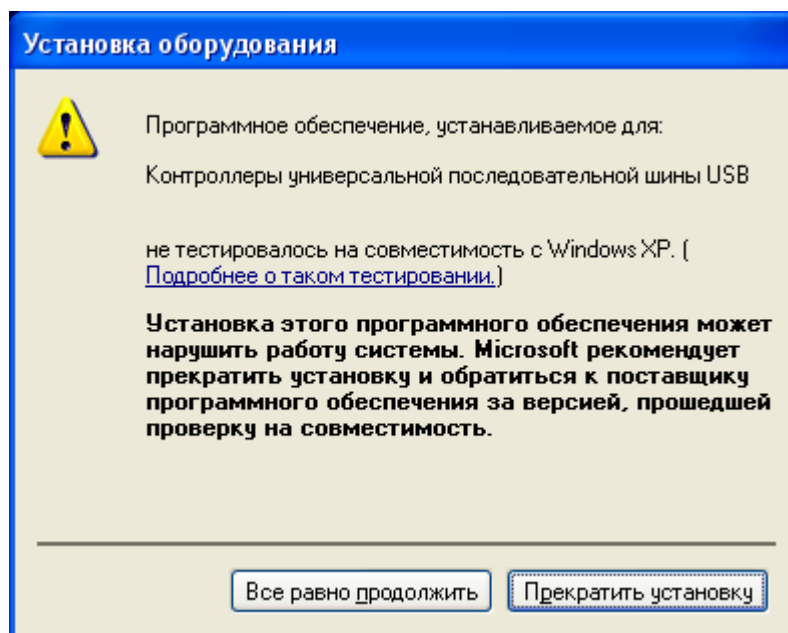


Рисунок 12 - Предупреждающее сообщение

Когда появится окно со словами о том, что установка выполнена (рисунок 13), нужно нажать кнопку <Готово>.

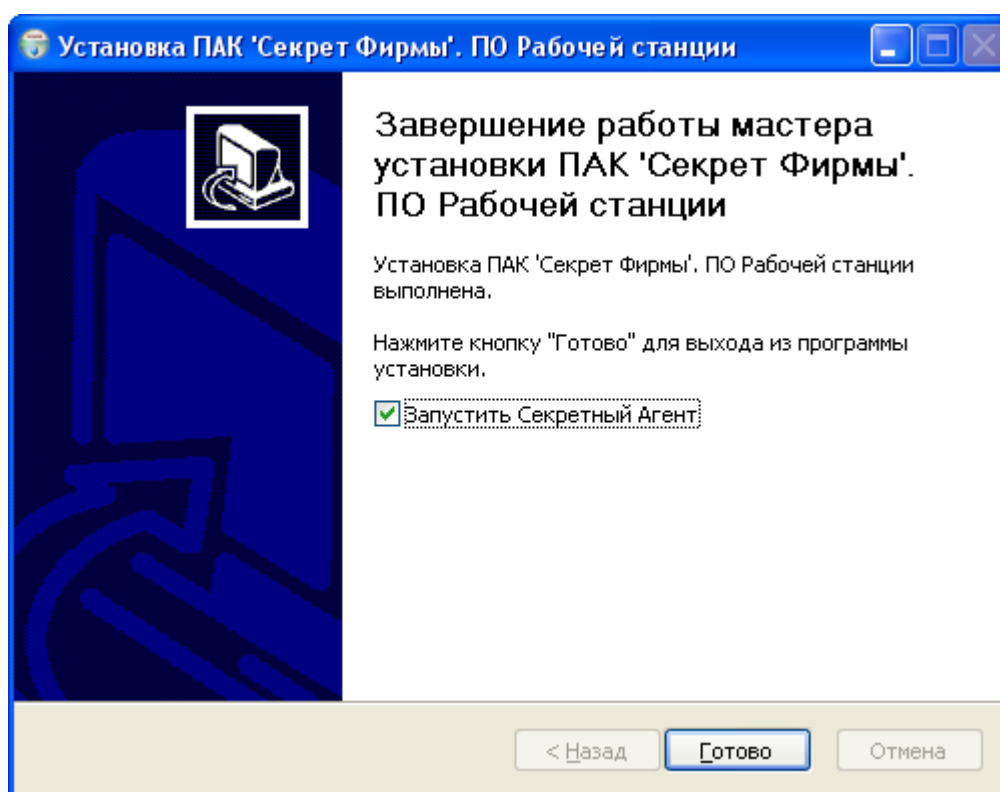


Рисунок 13 - Окно завершения установки ПО компьютера

После этого можно начать регистрацию «Секрета».

2.2. Подключение «Секрета Фирмы» и флешки Сервера Аутентификации (флешки СА)

«Секрет» и флешка СА подключаются так же, как обычные флешки – в свободный USB-разъем компьютера и СА¹.

2.3. Установка системного драйвера «Секрета» и флешки СА

ВНИМАНИЕ! Для корректной установки драйвера нужно, чтобы операционная система была запущена Администратором!

Когда «Секрет» подключается к компьютеру первый раз, операционная система обнаруживает новое устройство (рисунок 14).



Рисунок 14 – Оповещение об обнаружении «Секрета»

После этого происходит автоматический запуск системной программы «Мастер нового оборудования»². Если в настройках ОС включен режим автоматического обновления драйверов, то на экран выводится предложение выполнить поиск подходящего драйвера в сети Интернет (рисунок 15). Необходимо выбрать <Нет, не в этот раз> и нажать кнопку <Далее>.

¹В случае неудобного расположения USB-порта на компьютере (например, если он сзади или компьютер стоит под столом) рекомендуется использовать удлинительный кабель USB, это предохранит «Секрет» (а также и все другие применяемые USB-устройства) от поломок и облегчит его подключение и отключение.

² Если автоматического запуска «Мастера нового оборудования» не происходит, его можно инициировать двумя щелчками мыши по значку подключенного устройства, показанному на рисунке 14

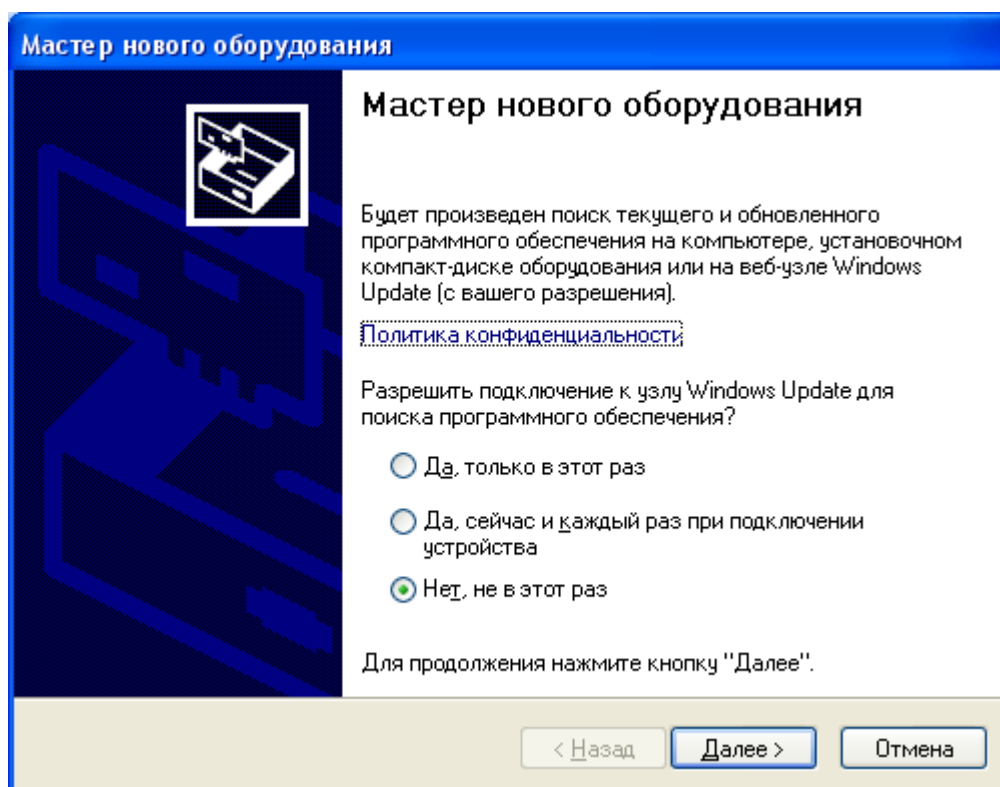


Рисунок 15 - Окно поиска текущего и обновленного ПО

В следующем окне программы «Мастер нового оборудования» следует выбрать пункт «Автоматическая установка» и нажать кнопку <Далее> (рисунок 16).

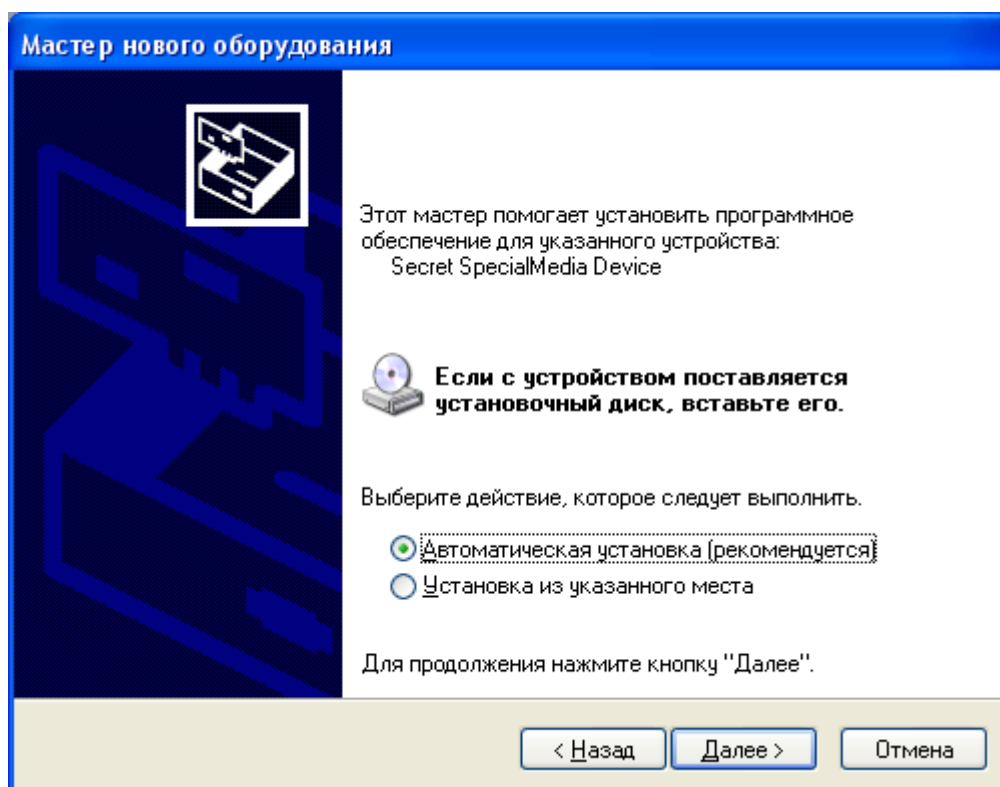


Рисунок 16 – Окно установки нового оборудования

После этого начинается процесс установки драйвера «Секрета» (рисунок 17).

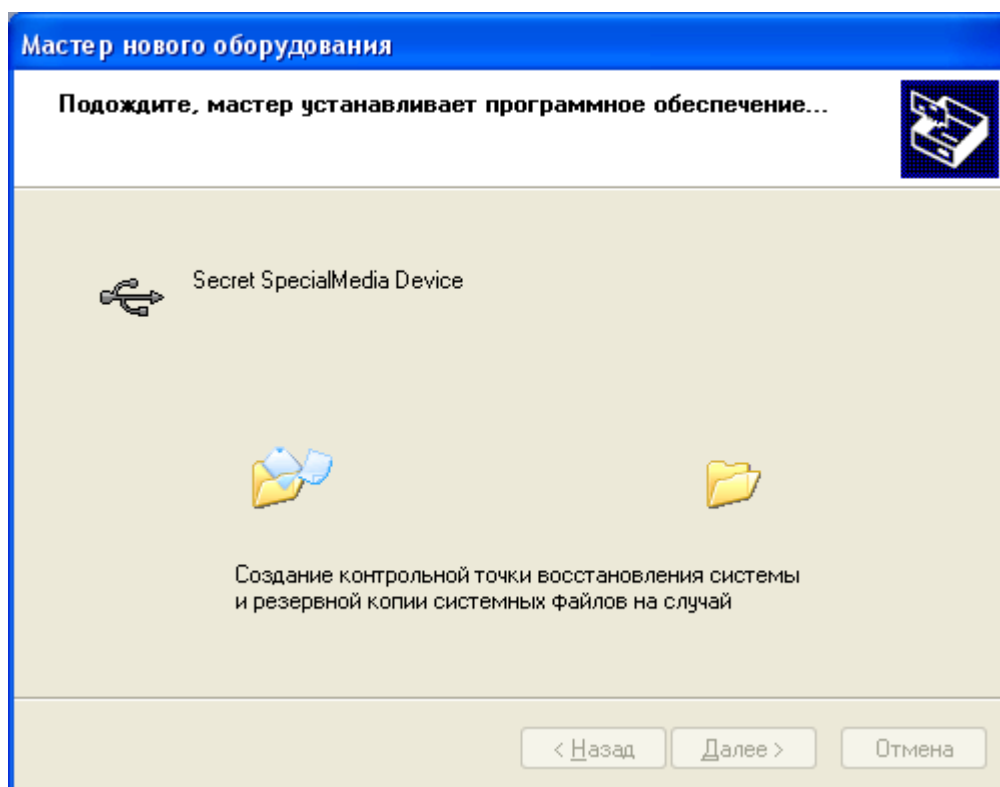


Рисунок 17 – Установка драйвера «Секрета»

При установке драйвера появится предупреждение (рисунок 18). Выбирайте пункт <Все равно продолжить>.

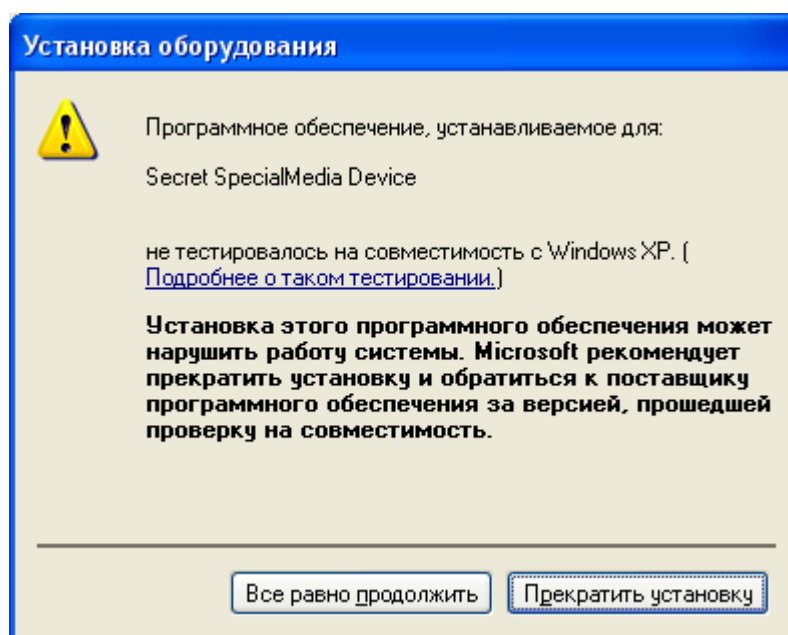


Рисунок 18 – Предупреждающее сообщение

После установки драйвера «Секрета» в ОС (он помещается в папку \Windows\System32\Drivers) появится окно завершения работы программы «Мастер нового оборудования» (рисунок 19).

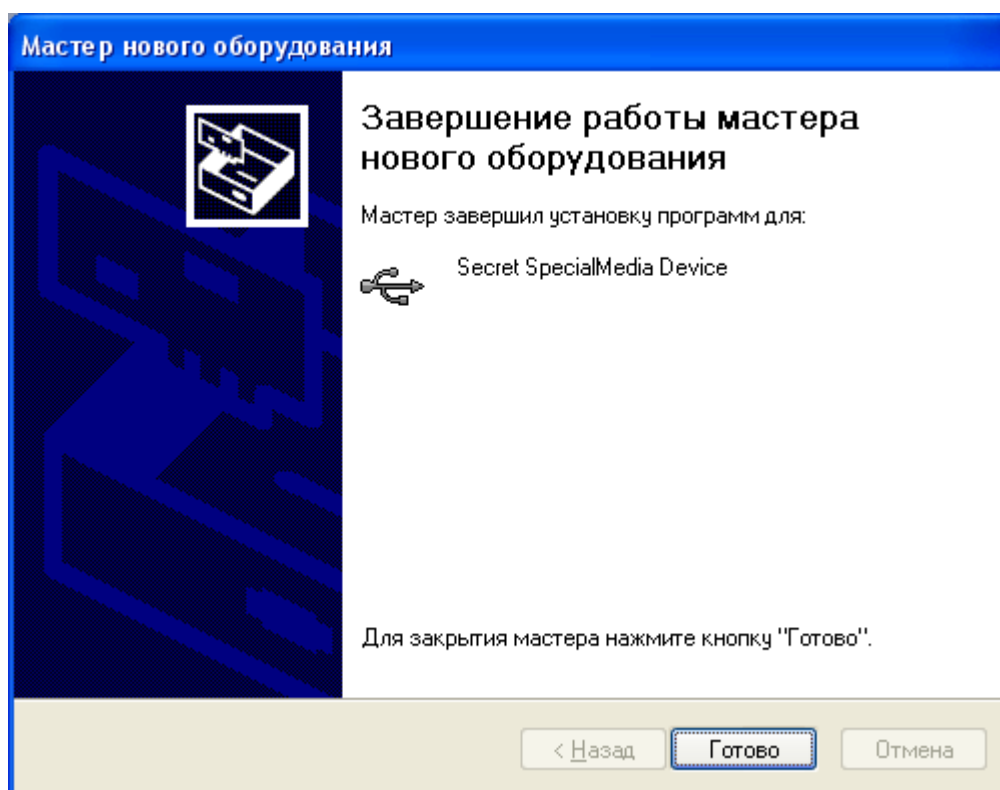


Рисунок 19 – Окно завершения работы Мастера нового оборудования

Нажмите <Готово>.

Процедура установки драйвера флешки СА аналогична процедуре установки драйвера «Секрета».

2.4. Начало работы

Итак, чтобы начать применять флешку «Секрет», нужно установить ПО «Секретный агент» на компьютер, и ПО «АРМ Администратора» на СА (см. подраздел 2.1), «Секрет» подключить к компьютеру, а флешку СА подключить к СА (см. подраздел 2.2), установить драйверы «Секрета Фирмы» и флешки СА (см. подраздел 2.3).

Следующий шаг – создание эталонной флешки СА (см. 3.1), которая в дальнейшем будет использоваться только для дублирования других флешек СА и создание рабочей флешки СА (см. 3.2), с помощью которой выполняются все действия, связанные с работой «Секрета Фирмы».

В результате выполнения этих процедур формируются PIN-коды и коды регистрации эталонной и рабочей флешек СА.

PIN-код эталонной СА необходим для выполнения следующих функций (управления эталонной флешкой СА): дублирование флешек СА, смена PIN-кода эталонной флешки СА. Если Вы потеряете PIN-кода эталонной флешки СА, то выполнение этих функций становится невозможным!

PIN-код рабочей флешки СА необходим для выполнения следующих функций: регистрация «Секрета Фирмы», подготовка «Секрета» к работе, смена PIN-кода «Секрета» и флешки СА, подготовка «Секрета» к повторной регистрации, повторная регистрация «Секрета», отмена регистрации «Секрета», разблокирование «Секрета». Если Вы потеряете PIN-кода рабочей флешки СА, то выполнение этих функций становится невозможным!

Если Вы потеряете коды регистрации эталонной (или рабочей) флешки СА, то станет невозможной процедура разблокирования эталонной (или рабочей) флешки СА.

Если сломалась (или потерялась) рабочая флешка СА – можно создать новую с помощью дублирования эталонной флешки (**но**, если потерялась эталонная флешка, то дублировать другие рабочие флешки СА будет нельзя).

ВНИМАНИЕ! Надежно сохраните в сейфе организации эталонную флешку (во избежание кражи или потери). При утрате эталонной флешки СА создание новых рабочих флешек станет невозможным!

Следующий шаг – процедура первичной регистрации «Секрета», в результате которой формируется PIN-код и код регистрации (подробнее об этом см. в подразделе 3.3).

PIN-код требуется для получения доступа к данным, хранящимся в «Секрете».

ВНИМАНИЕ! При утере PIN-кода «Секрета Фирмы» становится невозможным: получение доступа к данным, хранящимся в «Секрете», смена PIN-кода «Секрета».

Код регистрации необходим для управления «Секретом» (повторная регистрация, отмена регистрации, разблокирование. Подробнее см. соответствующие подразделы раздела 3).

Пользователю следует запомнить или надежно сохранить PIN-код и код регистрации «Секрета», а Администратору следует запомнить или надежно сохранить PIN-код и код регистрации флешки СА.

В случае необходимости (например, если есть подозрение, что PIN-код кто-то узнал) PIN-код можно сменить на новый. Для этого понадобится старый PIN-код. Как именно сменить PIN-код, написано в п. 3.9. Помните, что изменение кода регистрации «Секрета» приведет к полному обнулению устройства, возврату его к первоначальному состоянию (то есть исчезнут все данные о регистрации «Секрета», его PIN-коде, и доступ к записанным на нем данным станет невозможен).

До использования «Секрета» нужно:

- сразу после регистрации «Секрета» создать списки доступа (т.е. списки «своих» компьютеров) и параметры сетевого соединения (подробнее об этом см. 3.4);

- выполнить загрузку ключевой информации флешки СА в сервис сервера аутентификации (подробнее об этом см. в подразделе 3.5. Это необходимо для того, чтобы получить доступ к флешке «Секрет» как на сервере аутентификации, так и на компьютерах).

ВНИМАНИЕ! Если флешка СА была отключена от СА (или был выполнен выход из программы «АРМ Администратора»), то ключевая информация выгружается из сервиса СА. Поэтому, для того чтобы получить доступ к «Секрету», ключевую информацию флешки СА нужно загрузить в сервис СА после каждого подключения флешки СА к серверу аутентификации или перезапуска программы «АРМ Администратора».

После выполнения всех описанных выше операций доступ к данным «Секрета» (содержимому флешки) может быть получен на разрешенных компьютерах (т.е. «своих» компьютерах).

ВНИМАНИЕ! Доступ к флешке «Секрет» на компьютере может быть получен только в том случае, если рабочая флешка СА подключена к серверу аутентификации сети, в которой находится данный компьютер.

3. Управление «Секретом»

3.1. Создание эталонной флешки СА

ВНИМАНИЕ! Во время создания эталонной флешки СА не отключайте «Секрет» от компьютера, т.к. он может сломаться!

Для создания эталонной флешки СА необходимо:

- выполнить подключение флешки СА к серверу аутентификации (подробнее см. 2.2);
- запустить программу «АРМ Администратора», главное окно которой показано на рисунке 20. Чтобы запустить эту программу нужно выбрать пункт меню Пуск→Программы→Секрет Фирмы→Сервер Аутентификации→АРМ Администратора.

В данном окне выберите вкладку «Генерация». В ней будет отображаться список подключенных флешек СА с указанием их серийного номера. Выберите нужную флешку (нажмите на нее левой кнопкой мыши) и нажмите кнопку <Генерировать ключевую информацию...>.

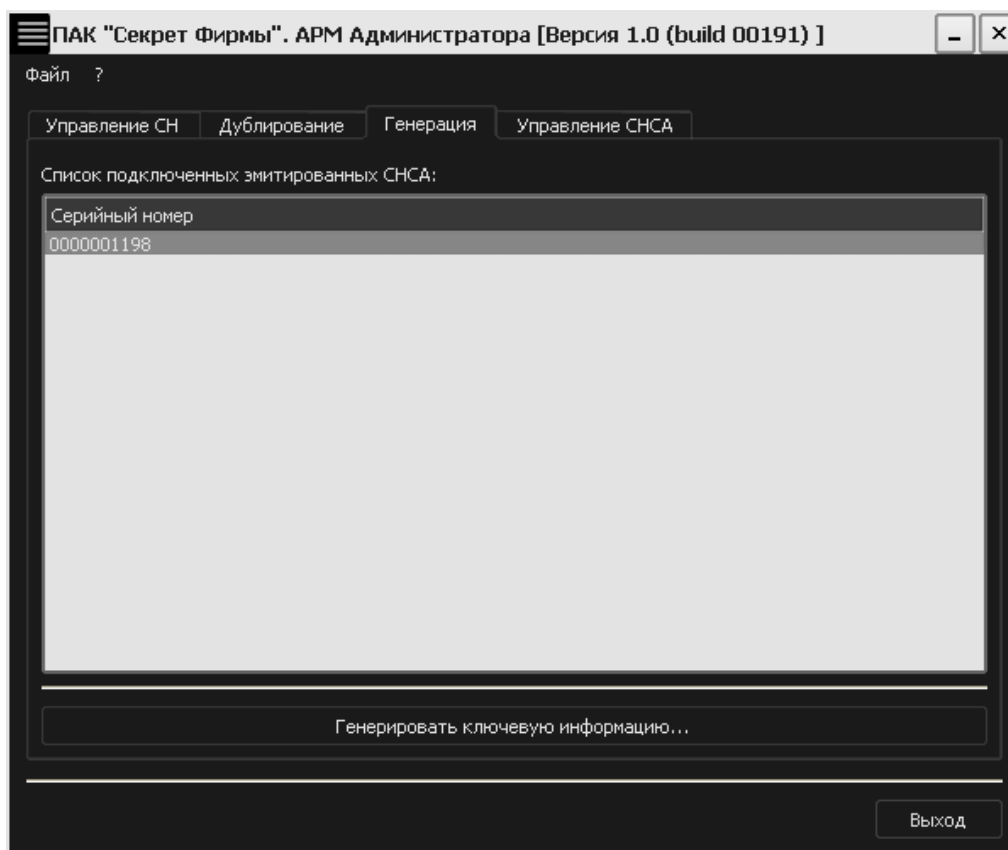


Рисунок 20 – Главное окно программы «АРМ Администратора». Вкладка «Генерация»

В следующем окне нужно задать имя регистрируемой флешки СА (рисунок 21). Имя флешки СА Вы задаете сами, его не нужно откуда-то брать. Оно должно быть не длиннее 27 символов, и может быть не одним словом, а каким-то словосочетанием или фразой – чтобы по ней Вы потом могли понять, о каком компьютере идет речь. Имя компьютера не связано с защитными функциями и задается только для удобства Пользователя, поэтому не нужно стремиться к тому, чтобы имя было сложным или чтобы о нем было трудно догадаться.

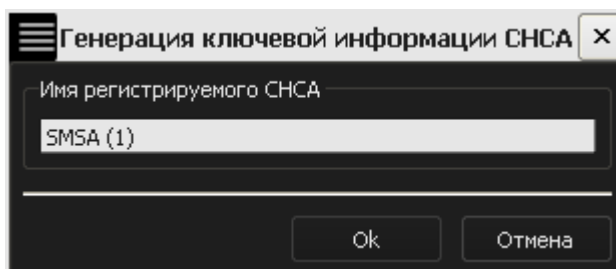


Рисунок 21 – Окно для ввода имени флешки СА

После этого на экране появляется окно, в нем нажмите кнопку <OK>:

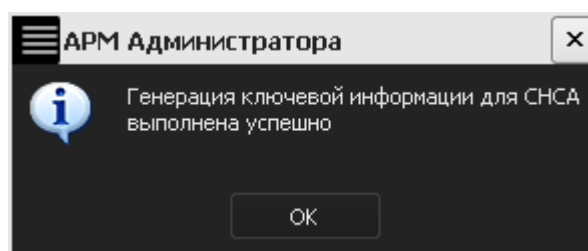


Рисунок 22 – Оповещение об успешной генерации КИ для флешки СА

Затем на экран выводится окно с основной информацией о флешке СА:

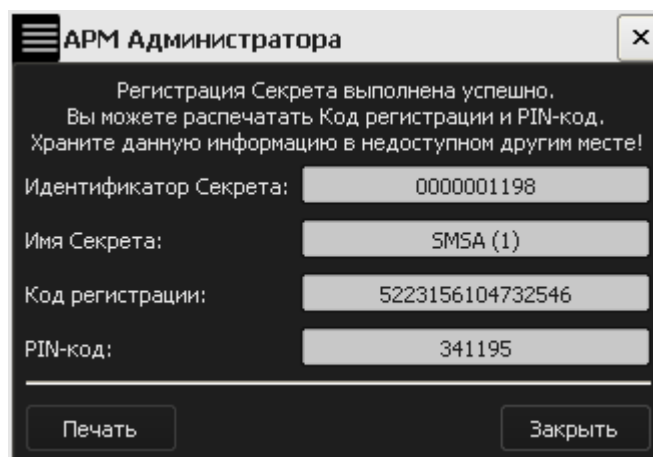


Рисунок 23 – Окно с основной ключевой информацией о флешке СА

ВНИМАНИЕ! Запомните или надежно сохраните PIN-код и код регистрации эталонной флешки СА. Помните о необходимости сохранения этих данных недоступными третьим лицам!

Можно распечатать код регистрации и PIN-код эталонной флешки СА (это делать необязательно). Для этого нажмите кнопку <Печать>. Если Вы нажали кнопку <Заккрыть>, не распечатывая код регистрации и PIN-код эталонной флешки СА, то на экране появляется окно:

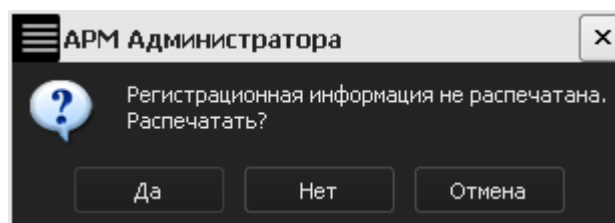


Рисунок 24 – Предупреждающее сообщение

Нажмите кнопку <Да>, если хотите распечатать эту информацию, или кнопку <Нет> в противном случае.

Далее во вкладке «Управление СНСА» появляется информация о только что зарегистрированной эталонной флешке СА (рисунок 25). При этом статус зарегистрированной флешки изменяется на «Снаряженный эталонный».

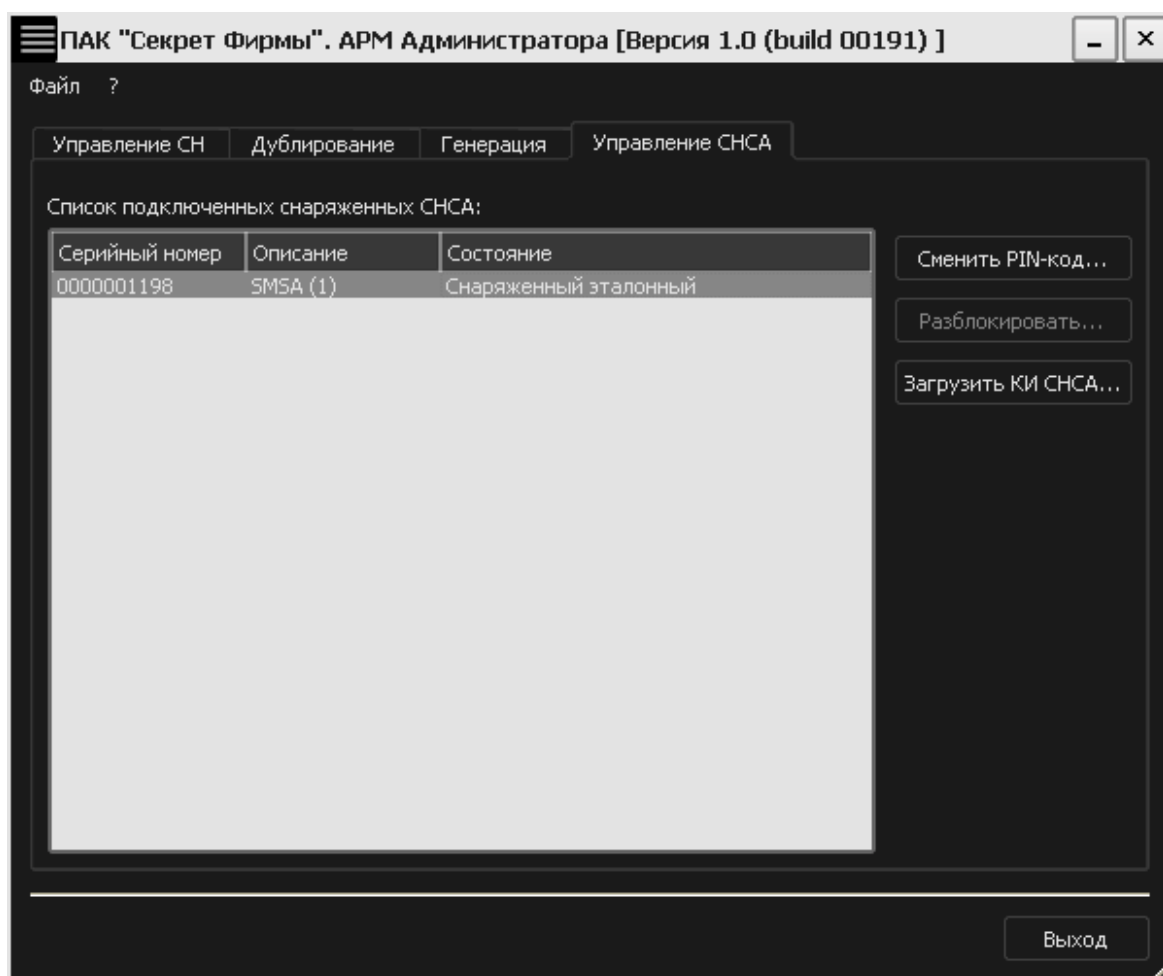


Рисунок 25 – Главное окно АРМ Администратора. Вкладка «Управление СНСА»

3.2. Дублирование флешек СА

Для дублирования нужно: подключить флешку СА к серверу аутентификации; эталонную флешку СА подключите во второй разъем СА (также допускается использование USB-хаба с собственным источником питания, см. 1.3).

Запустите программу «АРМ Администратора» и выберите вкладку «Дублирование» (см. рисунок 26). В ней будет отображаться список подключенных флешек СА с указанием их серийного номера;

ВНИМАНИЕ! Во время дублирования эталонной флешки СА не отключайте «Секрет» от компьютера, т.к он может сломаться!

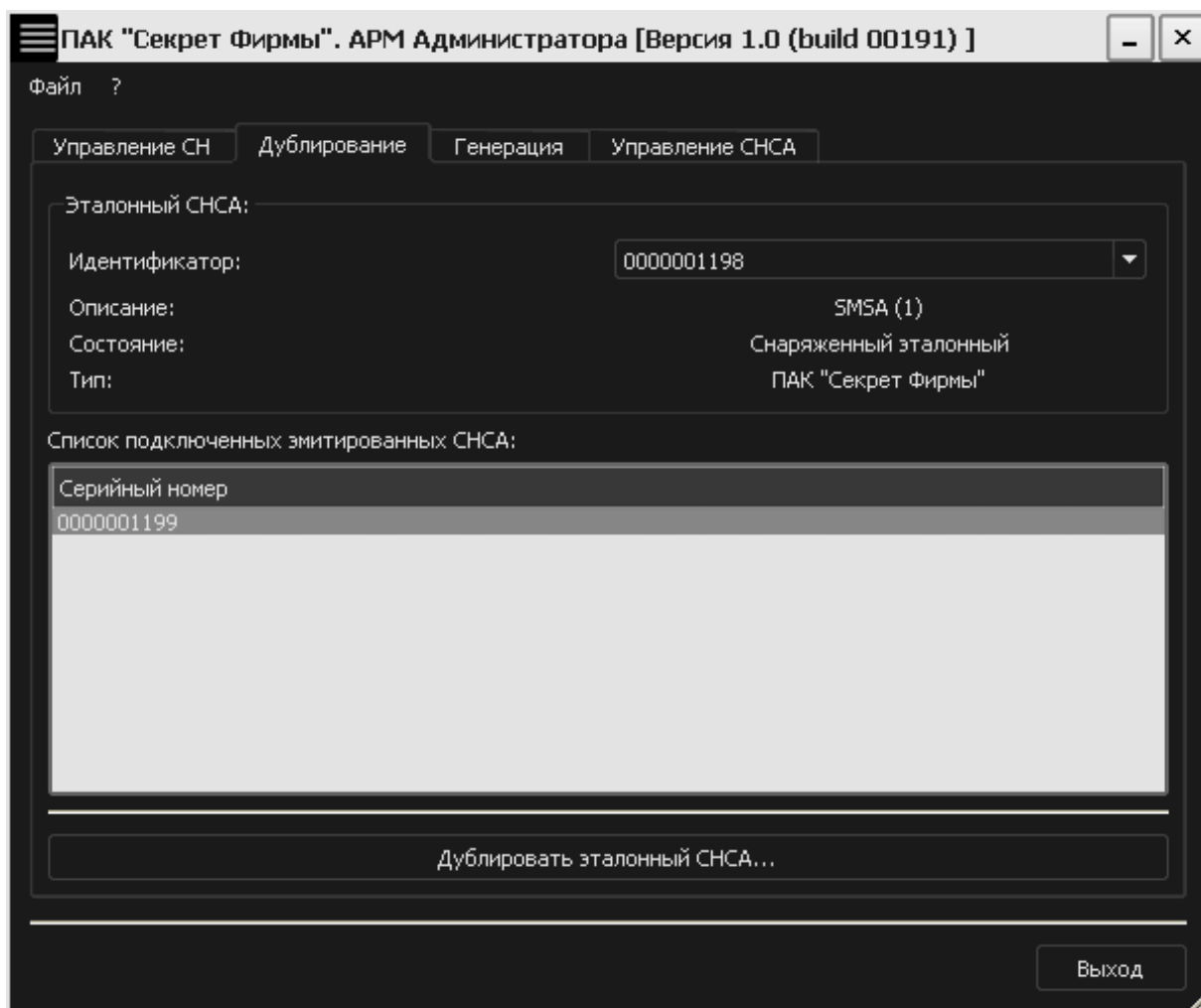


Рисунок 26 – Приложение АРМ Администратора. Вкладка «Дублирование»

В списке подключенных флешек СА выделите нужную флешку и нажмите кнопку <Дублировать эталонный СНСА...>.

В появившемся окне введите PIN-код эталонной флешки СА, полученный при ее создании (рисунок 27).

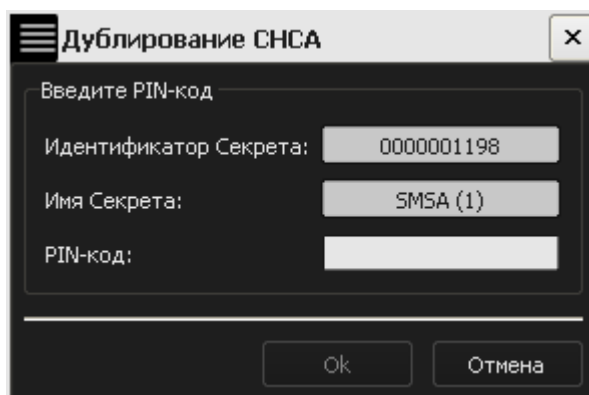


Рисунок 27 – Окно ввода PIN-кода эталонной флешки СА

При успешном выполнении дублирования флешки СА на экран выводится соответствующее оповещение (рисунок 28).

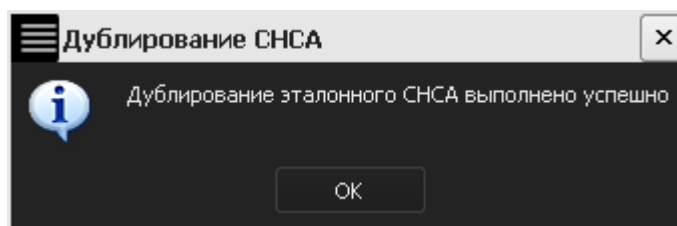


Рисунок 28 – Сообщение об успешном дублировании эталонной флешки СА

Далее на экран выводится окно с основной информацией о только что созданной рабочей флешке СА (рисунок 29).

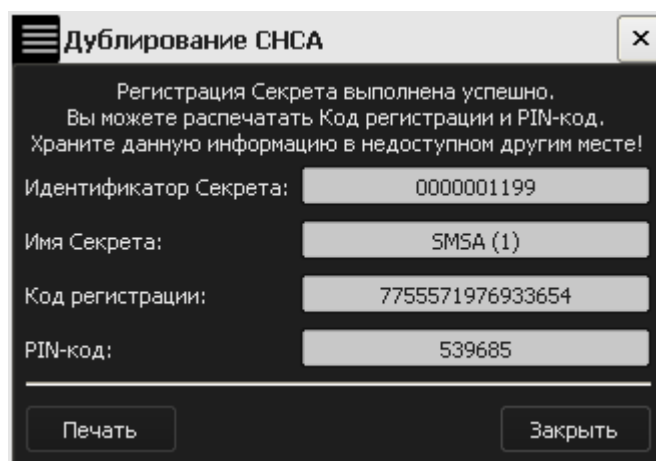


Рисунок 29 – Окно с регистрационными данными рабочей флешки СА

ВНИМАНИЕ! Запомните или надежно сохраните PIN-код и код регистрации рабочей СА.

PIN-код рабочей флешки СА позволяет получить доступ к следующим функциям «Секрета Фирмы»:

- регистрация «Секрета»;
- подготовка «Секрета» к возможности получения к нему доступа;
- подготовка «Секрета» к повторной регистрации;
- повторная регистрация «Секрета»;
- отмена регистрации «Секрета»;
- смена PIN-кода флешки СА;
- смена PIN-кода «Секрета»;
- разблокирование «Секрета».

Код регистрации флешки СА позволяет разблокировать флешку СА в случае ее блокирования.

Можно распечатать код регистрации и PIN-код (это делать необязательно). Для этого нажмите кнопку <Печать>. Если Вы нажали кнопку <Заккрыть>, не распечатывая код регистрации и PIN-код, то на экране появляется окно:

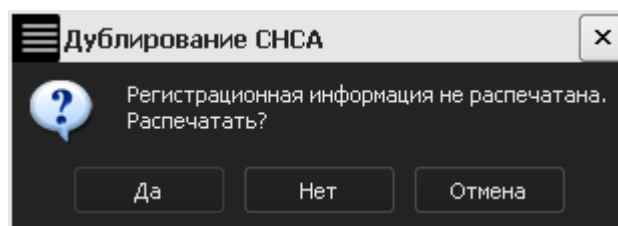


Рисунок 30 – Предупреждающее сообщение

Нажмите кнопку <Да>, если хотите распечатать эту информацию, или кнопку <Нет> в противном случае.

Далее во вкладке «Управление СНСА» появляется информация о только что созданной рабочей флешке СА (рисунок 31).

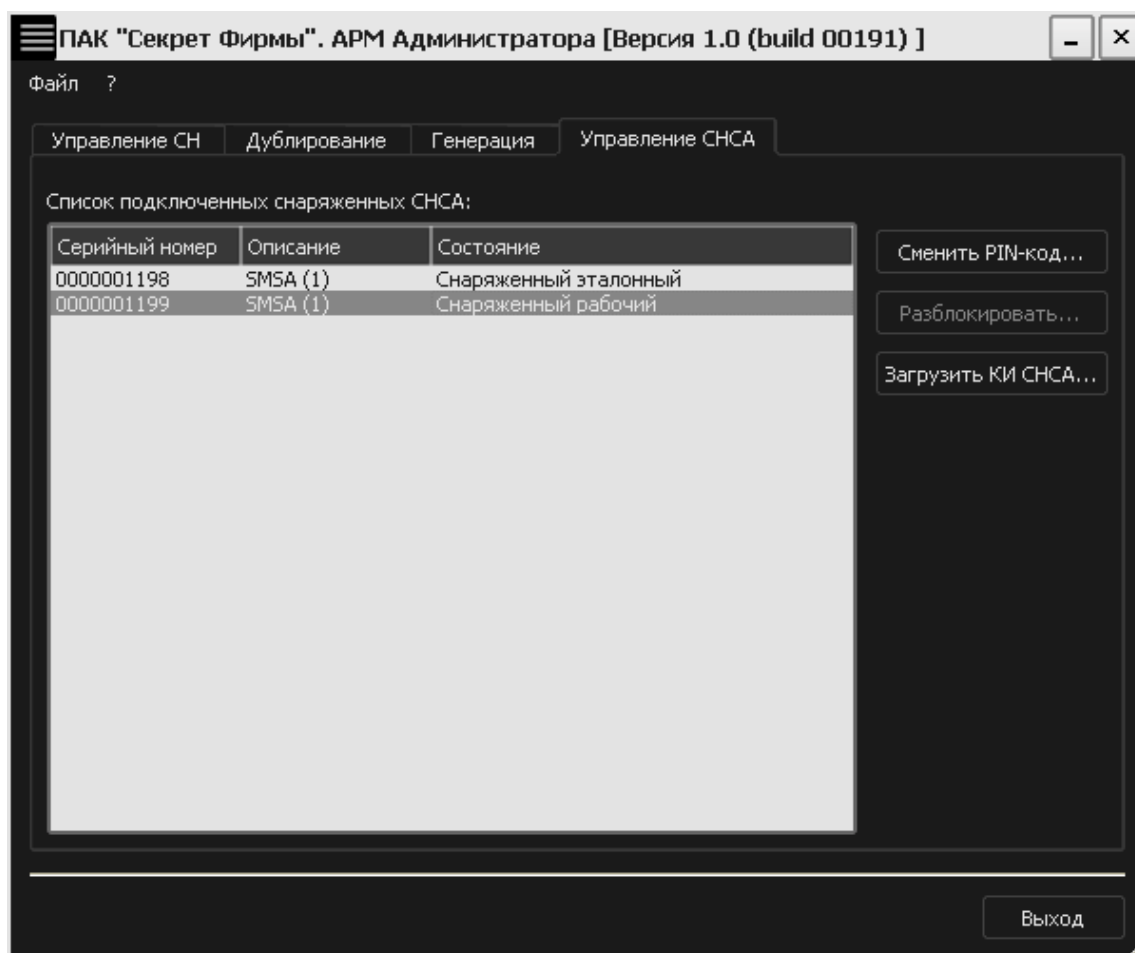


Рисунок 31 – АРМ Администратора. Вкладка «Управление СНСА»

Эталонную флешку СА отключите от СА и надежно сохраните в сейфе. Все дальнейшие действия, связанные с использованием «Секрета», должны выполняться с применением только рабочей флешки СА.

3.3. Регистрация «Секрета Фирмы»

Итак, ранее Вы установили на компьютер программу «Секретный агент» (см. 2), зарегистрировали рабочую флешку СА, с помощью которой можно настраивать «Секрет» (см. 3.2). Теперь можно перейти к регистрации «Секрета».

В ходе регистрации «Секрета» формируется PIN-код и код регистрации, которые потом понадобятся для работы с флешкой и для управления ею соответственно.

ВНИМАНИЕ! При регистрации «Секрета» не отключайте «Секрет» от компьютера. Он может сломаться!

Подключите «Секрет» и рабочую флешку СА к USB-портам сервера аутентификации (см. 2.2). При этом допускается использование USB-хаба с собственным источником питания (см. 1.3).

На экране появится сообщение о том, что подключенный «Секрет» не зарегистрирован (рисунок 32).

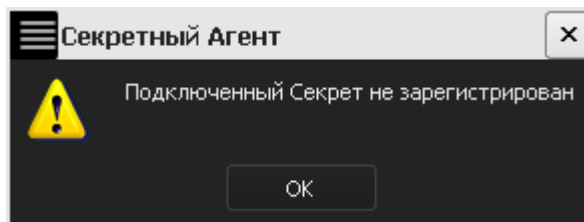


Рисунок 32 – Сообщение об отсутствии регистрации подключенного «Секрета»

Запустите программу «АРМ Администратора» (выберите Пуск → Программы → Секрет Фирмы → Сервер Аутентификации → АРМ Администратора), главное окно которой показано на рисунке 33.

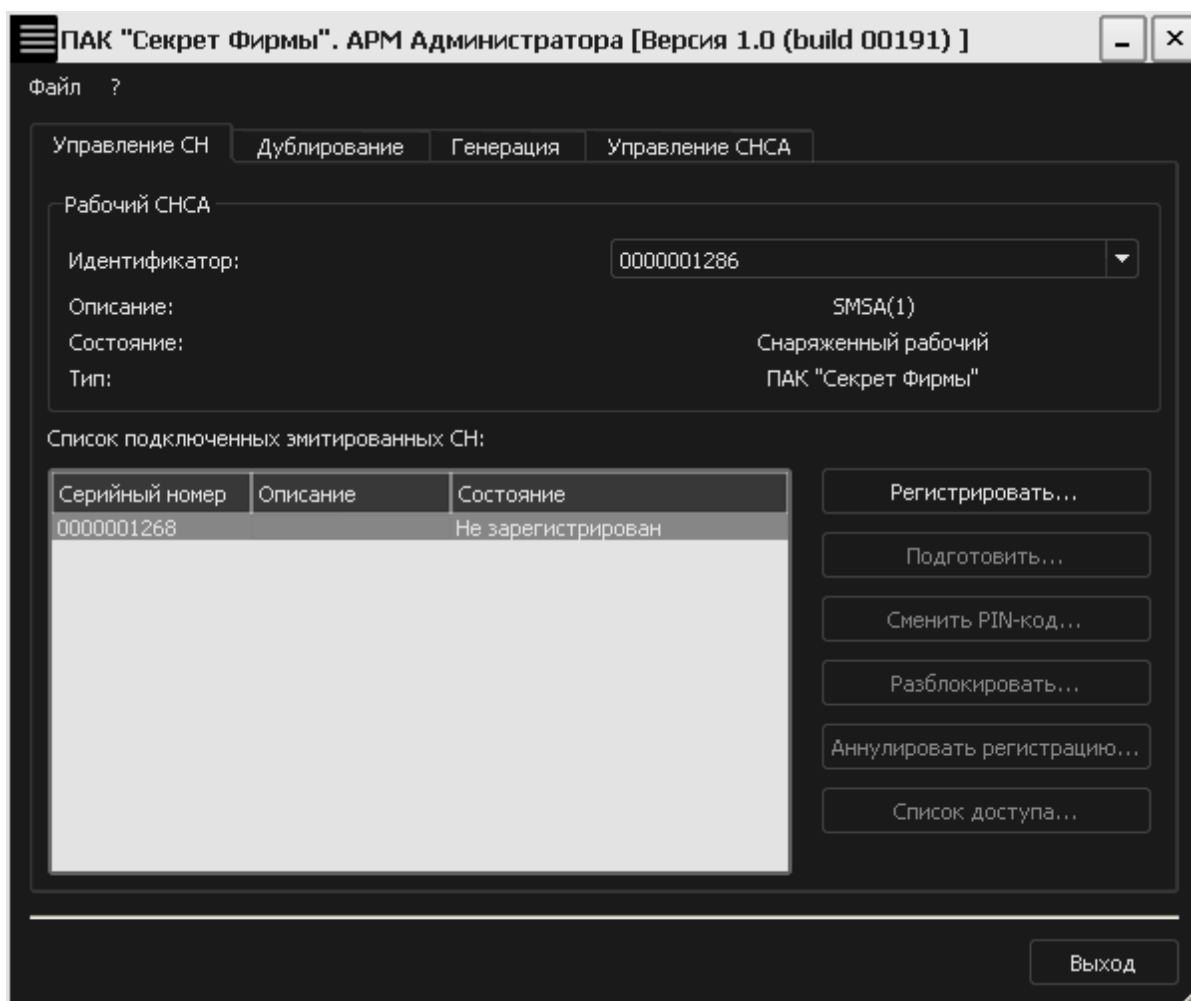


Рисунок 33 – Главное окно АРМ Администратора

Для регистрации нужного «Секрета» (флешка с состоянием <Не зарегистрирован>) выберите его из списка и нажмите кнопку <Регистрировать> (рисунок 33). Пока мы не выберем «Секрет», кнопка <Регистрировать> будет недоступна. Если к компьютеру подключен только один «Секрет», то и в списке он только один, не сомневайтесь.

После этого на экране появится окно, в нужно написать имя «Секрета» (рисунок 34).

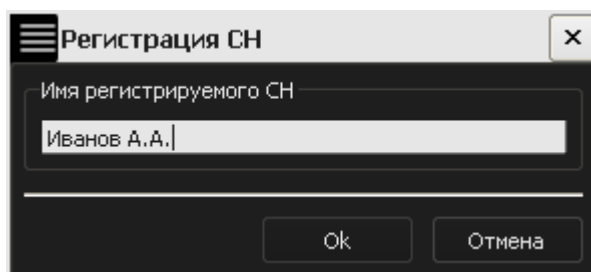


Рисунок 34 – Окно для задания имени регистрируемого «Секрета»

Имя «Секрета» задается обязательно. В нем может быть до 32 символов – и это может быть не обязательно одно слово, может быть фраза, из которой понятно, чей этот «Секрет», или для чего он (например, это удобно, если у Вас

несколько «Секретов» для разных задач. В этом случае их легко отличить друг от друга). Имя «Секрета» не связано с защитными функциями и задается только для удобства, поэтому не нужно стремиться к тому, чтобы имя было сложным или чтобы о нем было трудно догадаться. После того как имя задано, нажмите кнопку <OK> (она недоступна, если имя «Секрета» не задано).

В следующем окне введите PIN-код рабочей флешки CA (рисунок 35).

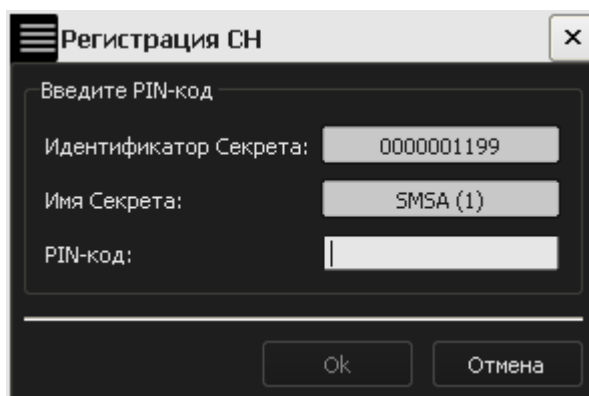


Рисунок 35 – Окно ввода PIN-кода для используемой флешки CA

Если Вы ввели неверный PIN-код (или произошла какая-либо другая ошибка), то на экране появится (рисунок 36).

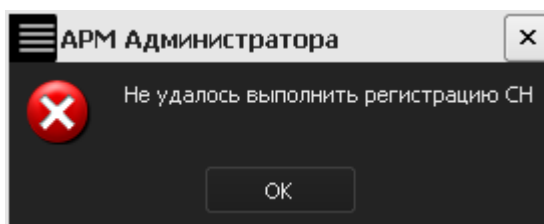


Рисунок 36 - Оповещение об ошибке в ходе регистрации

Если регистрация прошла без ошибок, то появится сообщение (рисунок 37).

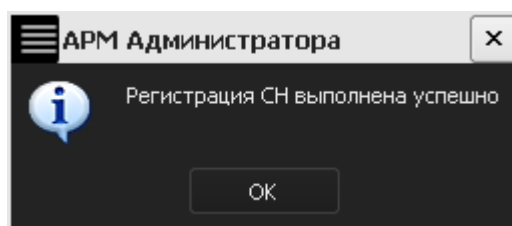


Рисунок 37 - Сообщение об успешной регистрации

Нажмите кнопку <OK>. После этого на экране появится окно с основной информацией о зарегистрированном «Секрете».

Администратор «Секрета» не должен знать PIN-код и код регистрации «Секрета». Их должен знать только Пользователь.

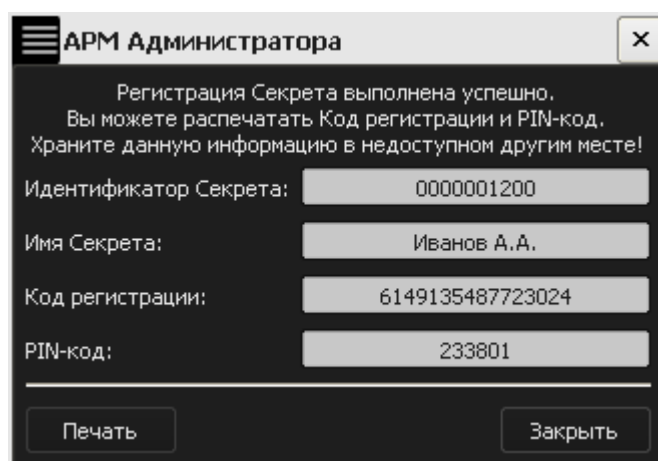


Рисунок 38 – Окно с информацией о зарегистрированном «Секрете»

ВНИМАНИЕ! Пользователь должен запомнить или надежно сохранить PIN-код и код регистрации «Секрета».

Код регистрации «Секрета Фирмы» используется для:

- регистрации «Секрета» на других компьютерах;
- отмены регистрации «Секрета»;
- разблокирования «Секрета».

PIN-код «Секрета» используется для получения доступа к данным, хранящимся на флешке «Секрет».

При желании можно распечатать код регистрации и PIN-код «Секрета» (этого делать необязательно). При этом для облегчения использования «Секрет Фирмы» код регистрации и PIN-код печатаются на разных листах (см. рисунок 39, рисунок 40).

Регистрационные данные Секрета

Имя Секрета: Иванов А.А.

Серийный номер Секрета: 0000001200

PIN-код: 233801

Дата регистрации: 21.06.2011

Рисунок 39 – Пример распечатанного PIN-кода

Регистрационные данные Секрета

Имя Секрета: Иванов А.А.

Серийный номер Секрета: 0000001200

Код регистрации : 2507953510697857

Дата регистрации: 21.06.2011

Рисунок 40 – Пример распечатанного кода регистрации

Для печати нажмите кнопку <Печать> (при условии наличия подключенного принтера). Если Вы не распечатали информацию, то на экране появляется сообщение (рисунок 41). Если Вы не хотите печатать эту информацию – нажмите кнопку <Нет>.

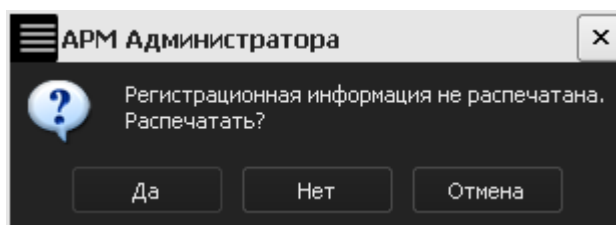


Рисунок 41 – Предупреждающее сообщение

После регистрации можно получить доступ к флешке «Секрет», сменить PIN-код, подготовить устройство к повторной регистрации, отменить регистрацию и настройку списка доступа (см. соответствующие подразделы 3).

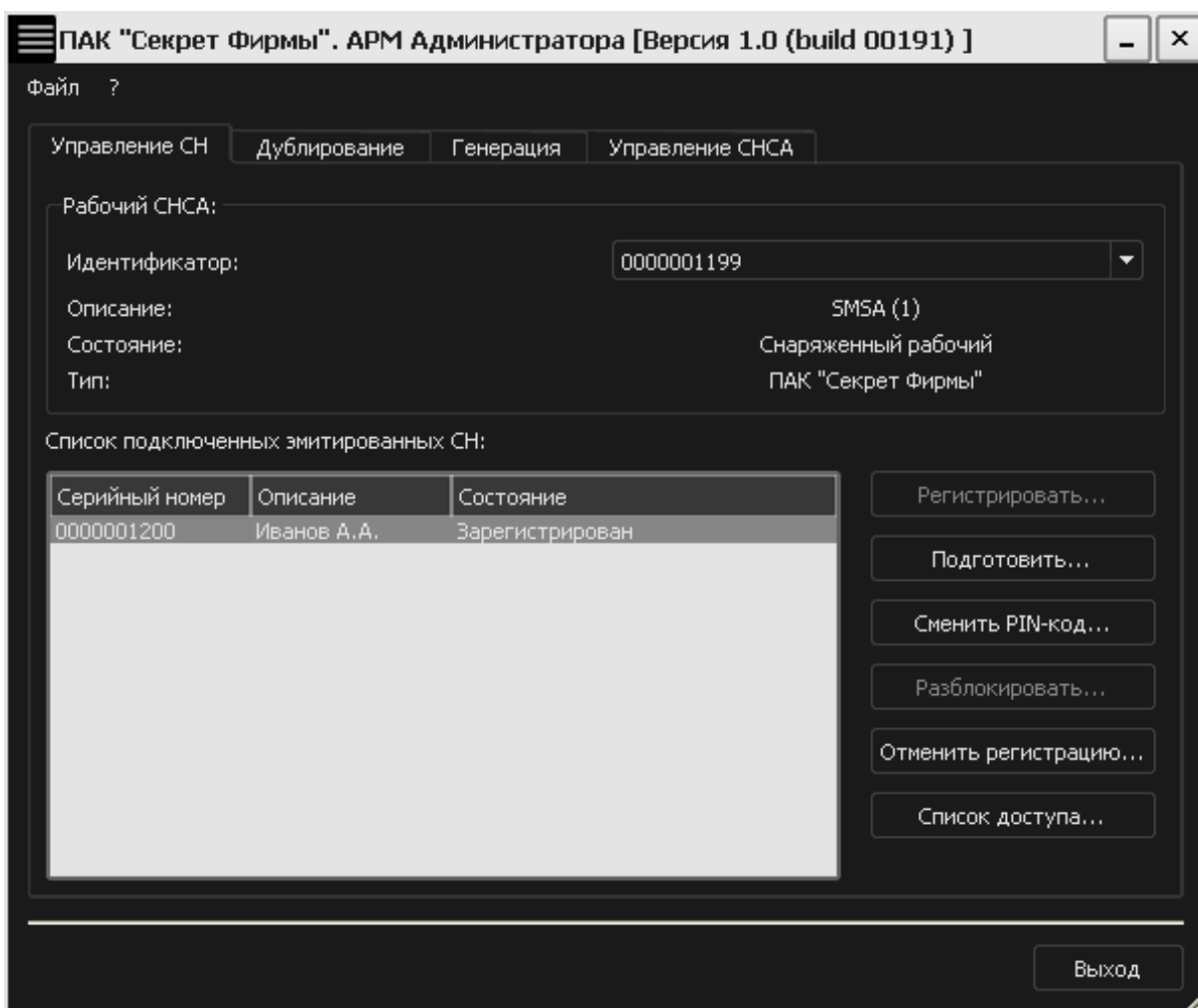


Рисунок 42 – АРМ Администратора. Вкладка «Управление СН»

Чтобы применять «Секрет» на других компьютерах, выполните на них повторную регистрацию «Секрета» (см. подраздел 3.6).

3.4. Подготовка «Секрета» к работе

После успешного выполнения регистрации «Секрета» необходимо выполнить подготовку «Секрет Фирмы» к дальнейшей работе:

- настроить списки доступа (см. 3.4.1);
- настроить сетевые параметры (см. 3.4.2).

ВНИМАНИЕ! Во время подготовки «Секрета» к работе, не отключайте его от компьютера! Он может сломаться!

3.4.1. Настройка списков доступа

До начала использования флешки «Секрет Фирмы» нужно настроить списки доступа (списки «своих» и запрещенных компьютеров):

- «белый» список доступа позволяет использовать «Секрет» только на «своих», т.е. разрешенных, компьютерах, имена которых указаны в списке. На остальных компьютерах применять «Секрет» нельзя;

- «черный» список запрещает использовать «Секрет» на компьютерах, имена которых указаны в списке. На остальных компьютерах применять «Секрет» можно.

Для настройки списков доступа во вкладке «Управление СН» программы «АРМ Администратора» выберите из списка необходимый «Секрет» и нажмите кнопку <Список доступа...> (рисунок 42).

В появившемся окне выберите вариант организации списка («белый» или «черный»). Вариант списка определяется в соответствии с принятой на работе политикой безопасности информации (рисунок 43).

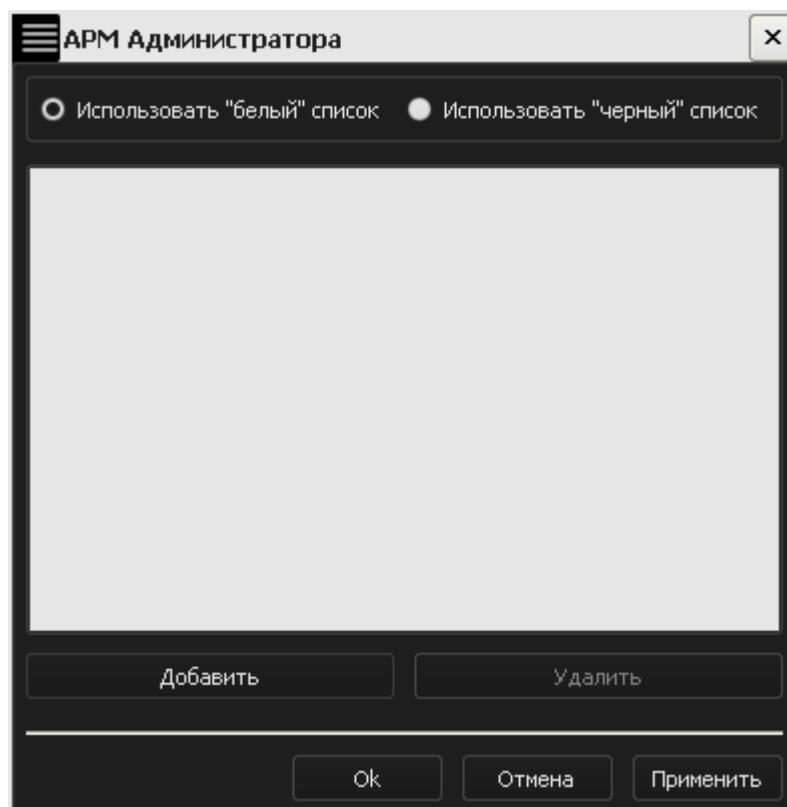


Рисунок 43 – Выбор списка доступа

Чтобы добавить компьютер в выбранный список, нажмите кнопку <Добавить>. Далее в появившемся окне введите сетевое имя нужного компьютера (Следует учитывать, что при добавлении в список доступа компьютеров, находящихся в домене, их имена могут содержать имя домена.) и нажмите кнопку <ОК> (рисунок 44).

ВНИМАНИЕ! Не вводите IP-адрес в поле «сетевое имя компьютера». Имя компьютера может содержать только латинские буквы (A-Z, a-z) и символы дефис (-) и точка (.).

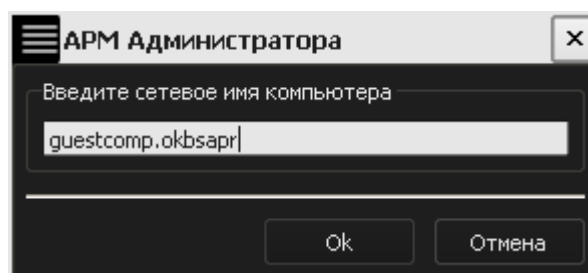


Рисунок 44 – Окно ввода сетевого имени компьютера

Сетевое имя компьютера будет добавлено в список доступа (рисунок 45). Чтобы добавить в список необходимое количество компьютеров, описанную выше процедуру столько раз, сколько компьютеров Вы планируете добавить в список.

Можно удалить компьютер из списка, выделив его и нажав кнопку <Удалить>.

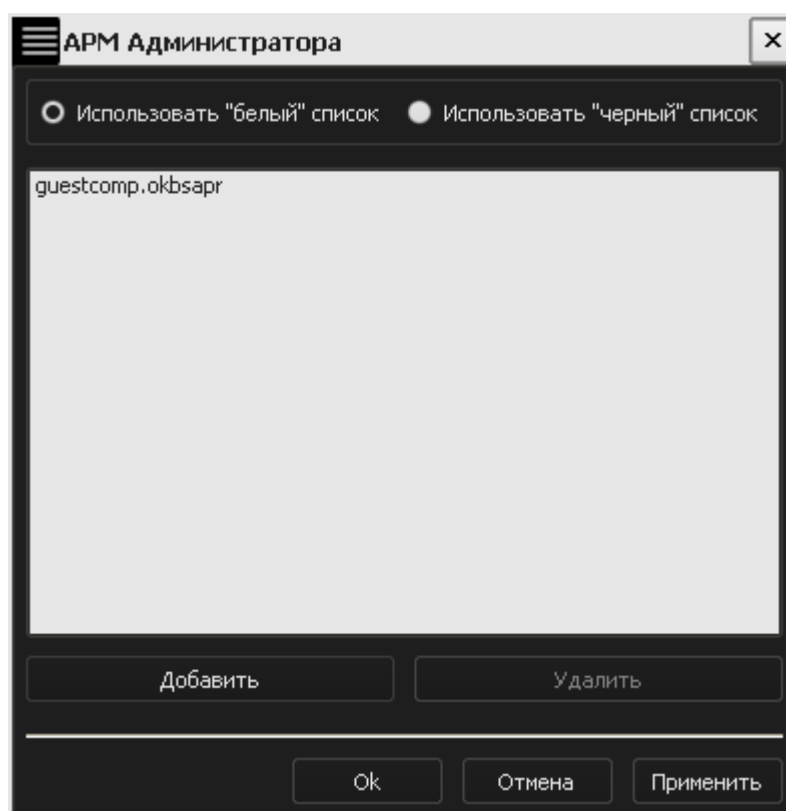


Рисунок 45 – Окно списка доступа

Далее нажмите кнопку <Применить>, затем – <ОК>.

ВНИМАНИЕ! Если Вы захотите изменить имя компьютера, который ранее уже был включен в «белый» список доступа во флешке «Секрет Фирмы», то измените также и «белый» список: удалите из списка запись со старым именем компьютера и добавьте запись, содержащую новое имя компьютера.

Если имя компьютера изменено, а «белый» список не скорректирован, Вы не сможете получить на данном компьютере доступ к «Секрету»!

3.4.2. Настройка сетевых параметров

После настройки списков доступа необходимо выполнить настройку сетевых параметров на компьютере. Для этого следует в трее (справа внизу экрана) щелкнуть правой кнопкой мыши на значке «Секретный Агент» (рисунок 46) и в меню выбрать пункт «Настройки».



Рисунок 46 – Значок приложения «Секретный Агент» в трее

В появившемся окне есть поля, которые необходимо заполнить:

- адрес сервера аутентификации (рисунок 47). В данную строку необходимо ввести адрес нужного СА и нажать кнопку <Применить>;
- порт для взаимодействия с сервером аутентификации;
- время ожидания отклика. Это время, в течение которого программа «Секретный Агент» ждет ответа от сервера аутентификации на отправленный им пакет данных.

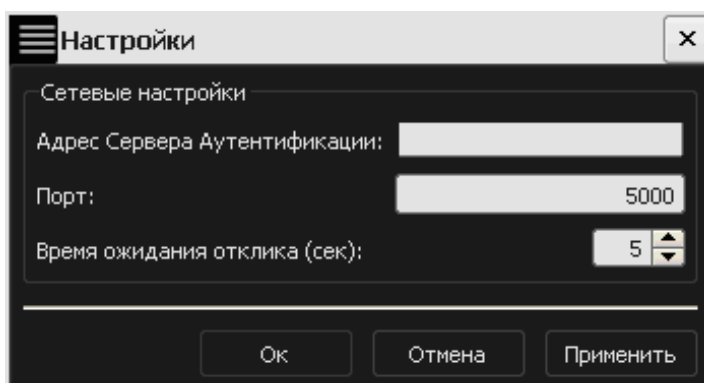


Рисунок 47 – Окно ввода адреса сервера аутентификации

После задания сетевых настроек нажмите кнопку <ОК>. После успешного выполнения описанной процедуры можно применять «Секрет» на компьютере, который «привязан» к указанному СА. При этом «Секрет» обнаруживается системой как обычная флешка.

3.5. Загрузка ключевой информации флешки СА в сервис СА

ВНИМАНИЕ! Если флешка СА была отключена от СА (или был выполнен выход из программы «АРМ Администратора»), то ключевая информация выгружается из сервиса СА. Чтобы получить доступ к данным «Секрета», ключевую информацию флешки СА необходимо загружать в сервис СА после каждого ее

подключения к серверу аутентификации или после каждого перезапуска программы «АРМ Администратора».

Подключите рабочую флешку СА к серверу аутентификации. Во вкладке «Управление СНСА» программы «АРМ Администратора» выберите нужную флешку СА и нажмите кнопку <Загрузить КИ СНСА...> (рисунок 48).

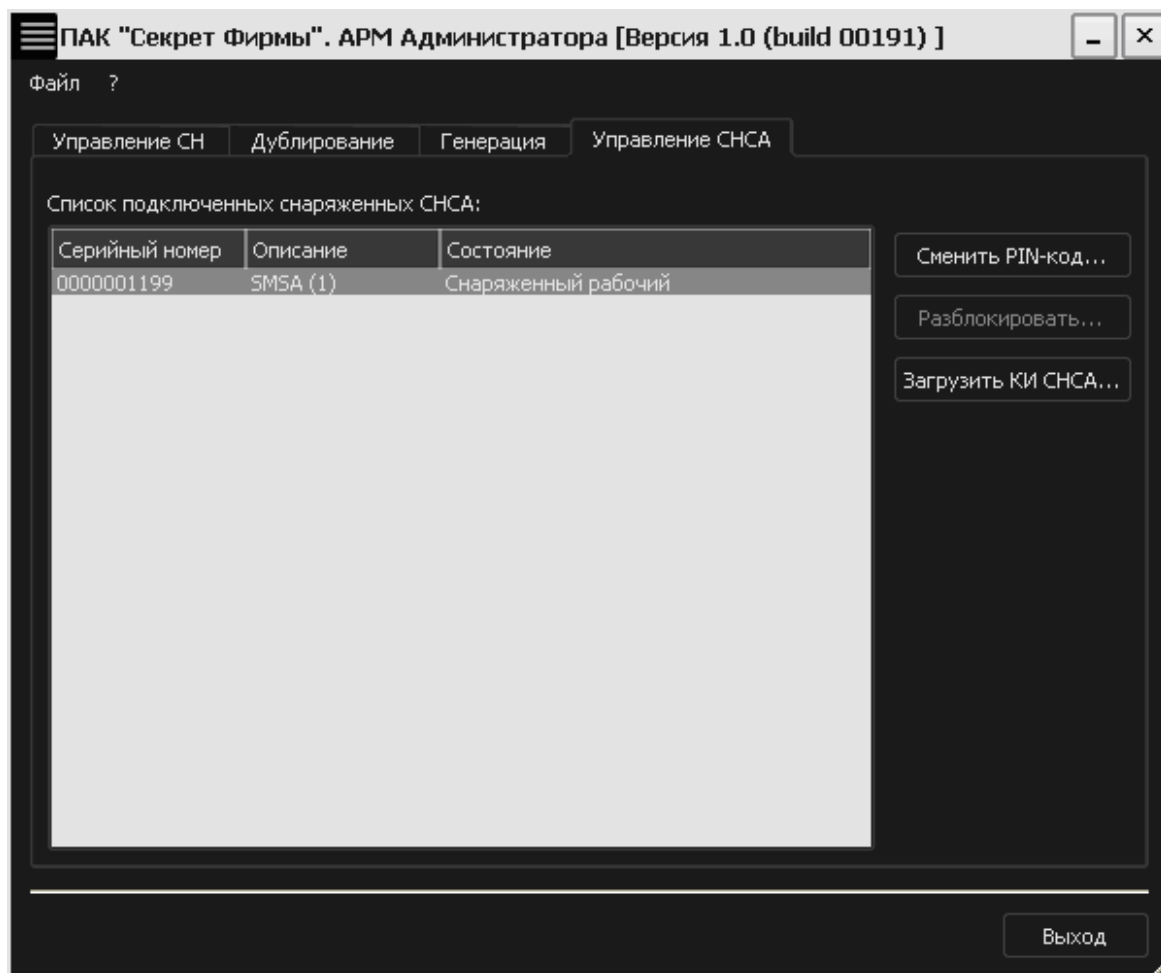


Рисунок 48 – АРМ Администратора. Вкладка «Управление СНСА»

В появившемся окне введите PIN-код флешки СА (рисунок 49).

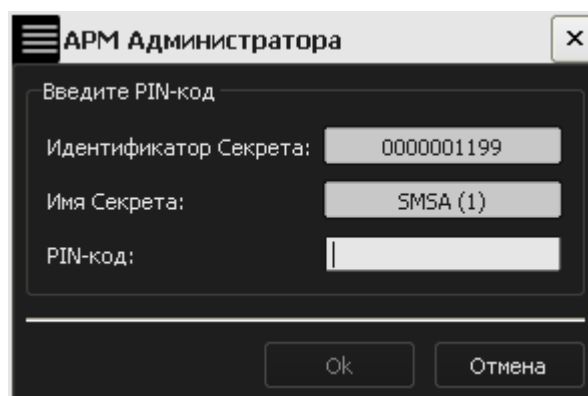


Рисунок 49 - Окно ввода PIN-кода для флешки СА

Если все выполнено успешно, Вы увидите на экране сообщение (рисунок 50).

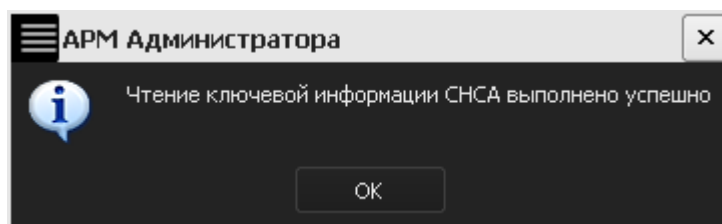


Рисунок 50 – Сообщение об успешном выполнении чтения КИ флешки СА

3.6. Регистрация «Секрета Фирмы» на другом компьютере

3.6.1. Подготовка «Секрета» к регистрации на другом компьютере (повторной регистрации)

Во вкладке «Управление СН» программы «АРМ Администратора» выберите из списка подключенных и зарегистрированных флешек «Секрет» нужную и нажмите кнопку <Подготовить...> (рисунок 51).

ВНИМАНИЕ! При подготовке к повторной регистрации «Секрета» не отключайте «Секрет» от компьютера! Он может сломаться!

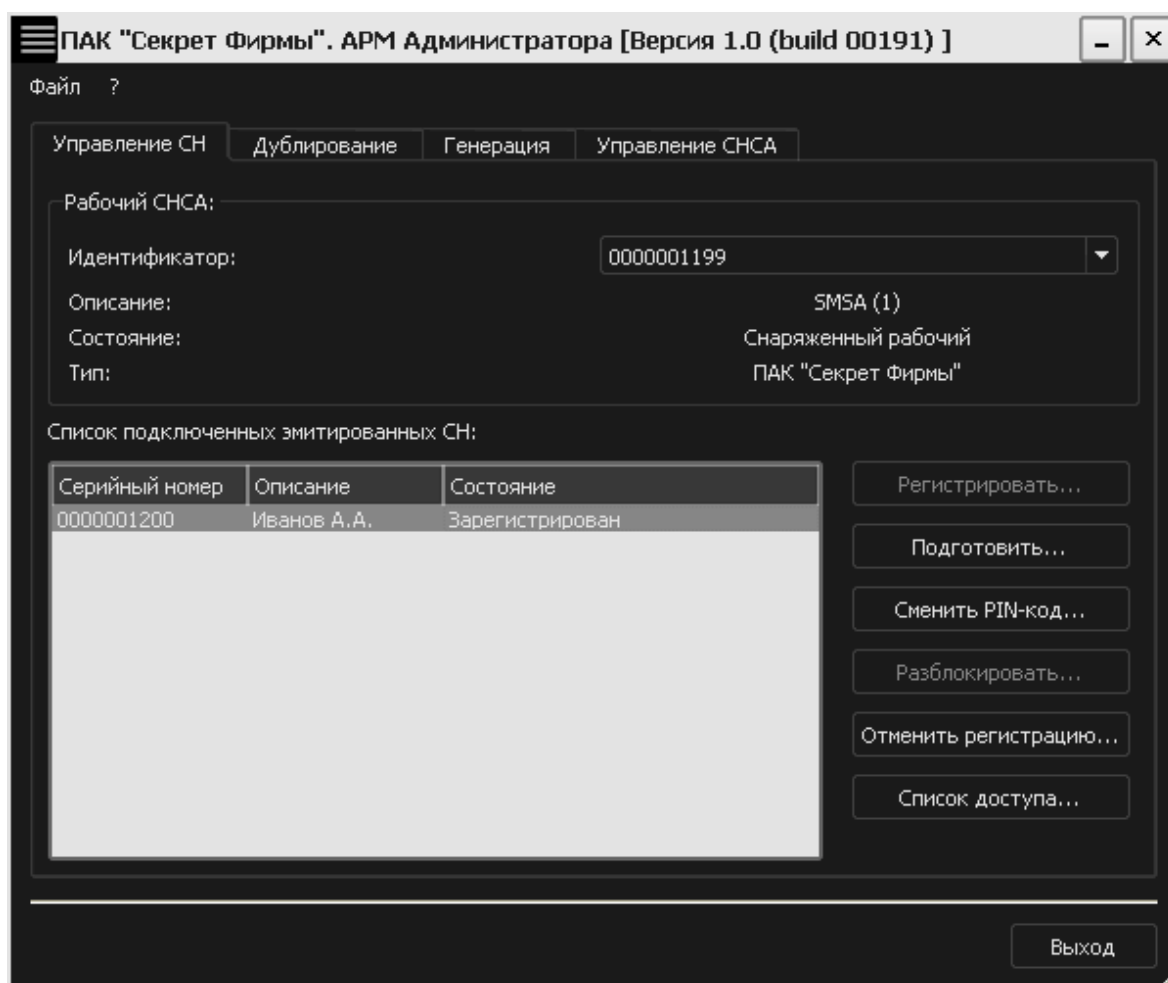


Рисунок 51 – АРМ Администратора. Вкладка «Управление СН»

В появившемся далее окне Пользователь должен ввести код регистрации данного «Секрета», полученный при его первичной регистрации, и нажать кнопку <OK> (рисунок 52).

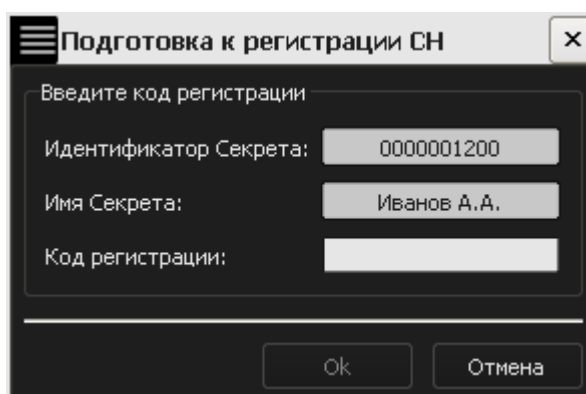


Рисунок 52 – Окно ввода кода регистрации для данного «Секрета»

Далее в появившемся окне введите PIN-код первичной флешки СА, на которой «Секрет» зарегистрирован в данный момент, и нажмите кнопку <OK> (рисунок 53).

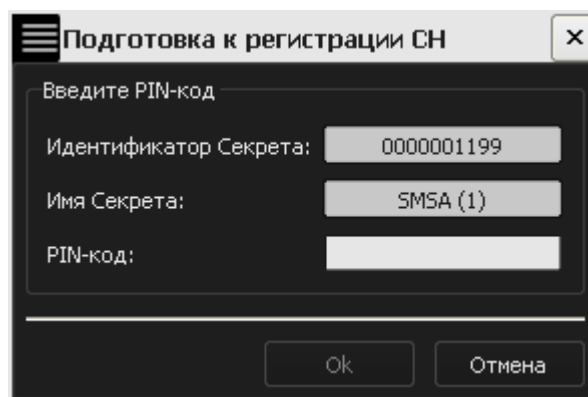


Рисунок 53 – Окно ввода PIN-кода старой флешки СА

В следующем окне нужно заполнить поля (рисунок 54):

- Идентификатор дружественной (той флешки, о которой точно известно, что ее можно использовать и что ее не будет использовать кто угодно) флешки СА. Это номер (новой) флешки СА, на которой планируется произвести повторную регистрацию.

- Дата окончания срока действия мандатов. Это дата, до которой (включительно) необходимо провести повторную регистрацию «Секрета»¹. По истечении действия мандата, регистрация на дружественной флешке СА становится невозможной². (Для того чтобы повторная регистрация вновь стала возможной, необходимо получить новый мандат регистрации. По умолчанию предлагается дата текущего дня. Дата, предлагаемая по умолчанию, может быть изменена посредством ручного редактирования или выбором из прилагаемого календаря).

- Каталог для сохранения мандата. По умолчанию сохранение мандата выполняется в каталог \Program Files\OKB SAPR JSC\Secret\Business\Server. Каталог, предлагаемый по умолчанию, можно изменить посредством ручного редактирования или задать с помощью кнопки <...>. Если указанный каталог не существует, он будет создан автоматически.

1) Дата окончания срока действия мандата регистрации не влияет на работу «Секрета» в рамках первичной регистрации.

2) Срок действия мандатов не ограничивает время использования СН в дружественном сегменте сети в случае успешного завершения процедуры повторной регистрации.

Рисунок 54 – Окно создания мандата регистрации

После заполнения всех полей нажмите кнопку <ОК>.

Если подготовка к повторной регистрации выполнена успешно, то на экране появится сообщение (в сообщении имеется имя мандата, рисунок 55).

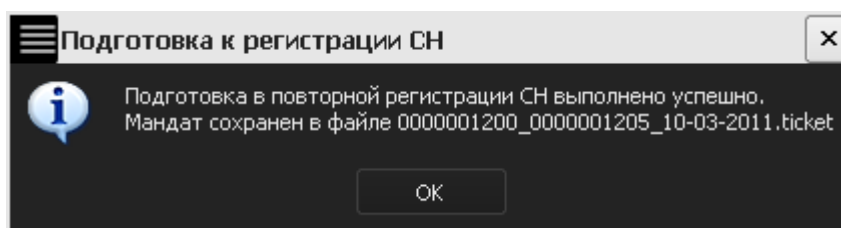


Рисунок 55 – Оповещающее сообщение

ВНИМАНИЕ! Повторную регистрацию нельзя провести при отсутствии файла с мандатом регистрации. Поэтому при выполнении повторной регистрации первичного СА нужно обеспечить доступ к данному файлу для дружественного СА (например, отправить по почте или скопировать на любой носитель информации и перенести на дружественный компьютер). При этом безопасность процедуры передачи мандата регистрации обеспечивается организацией, которая использует «Секрет».

После получения мандата регистрации дружественного СА можно провести регистрацию «Секрета» на дружественной флешке СА.

3.6.2. Повторная регистрация «Секрета»

Чтобы использовать «Секрет» не только на том компьютере, на котором Вы его первый раз зарегистрировали, нужно там его тоже зарегистрировать. Это будет не совсем такая же регистрация. Для повторной регистрации потребуется код регистрации. Это нужно для того, чтобы кто угодно не мог зарегистрировать Ваш «Секрет» на своем компьютере и открыть его.

Подключите флешку СА дружественного СА и «Секрет», который необходимо повторно зарегистрировать, к USB-портам дружественного сервера

аутентификации. При этом можно использовать USB-хаб с собственным источником питания (см. 1.3).

Запустите программу «АРМ Администратора» (Пуск → Программы → Секрет Фирмы **Ошибка! Источник ссылки не найден.** → Сервер Аутентификации → АРМ Администратора).

ВНИМАНИЕ! При повторной регистрации «Секрета» не отключайте «Секрет» от компьютера! Он может сломаться!

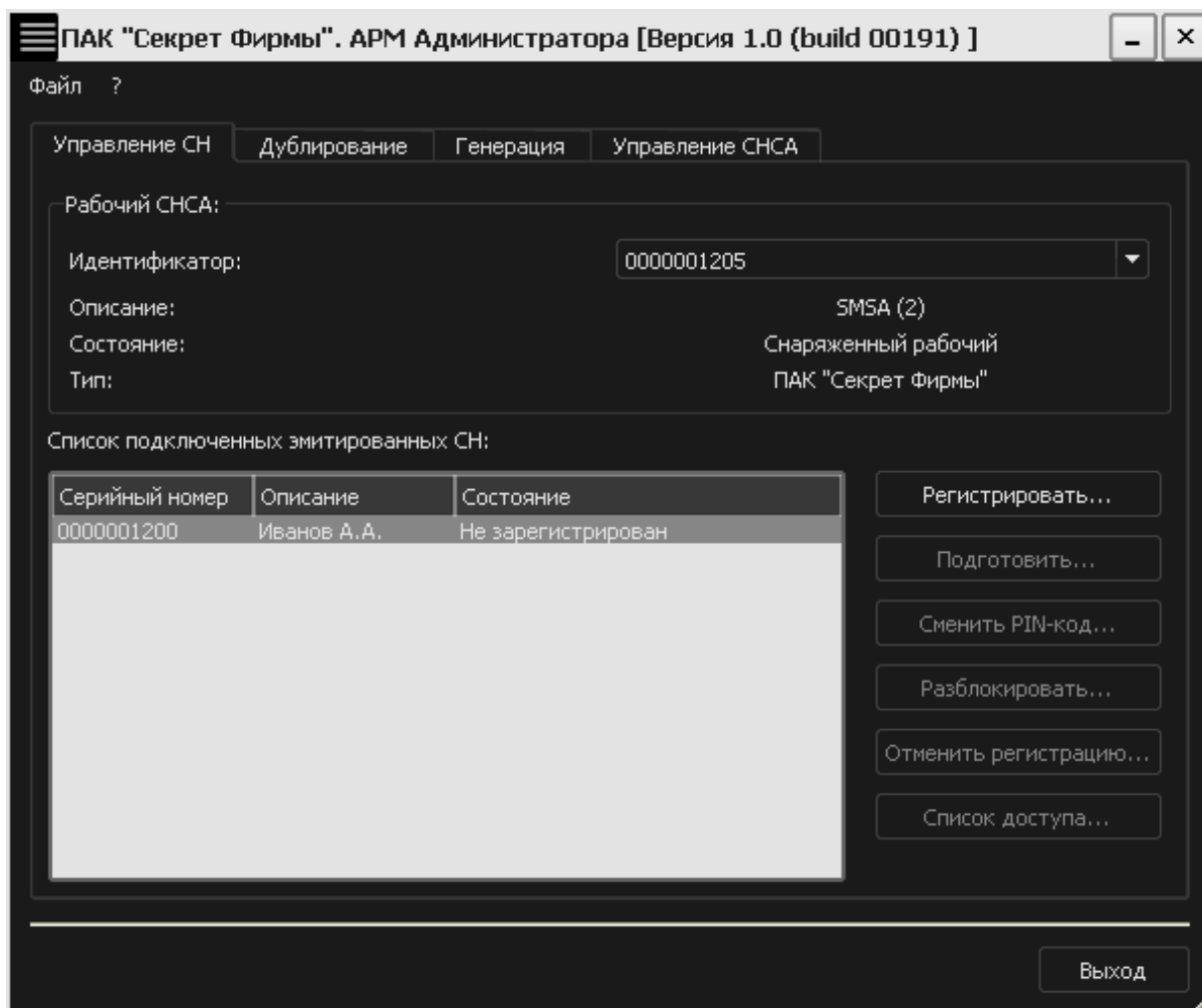


Рисунок 56 – АРМ Администратора. Вкладка «Управление СН»

Выберите «Секрет», который необходимо зарегистрировать, и нажмите кнопку <Регистрировать...> (рисунок 56).

В появившемся окне (рисунок 57) Пользователь должен ввести код регистрации данного «Секрета Фирмы», полученный при его первичной регистрации (см. 3.3).

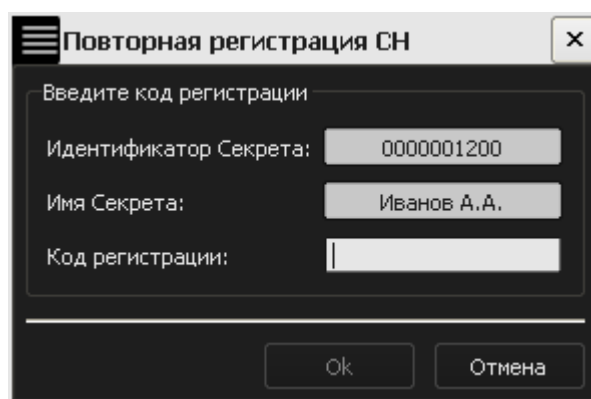


Рисунок 57 – Окно ввода кода регистрации для регистрируемого «Секрета»

В следующем окне введите PIN-код флешки СА, на которой производится процедура повторной регистрации (рисунок 58).

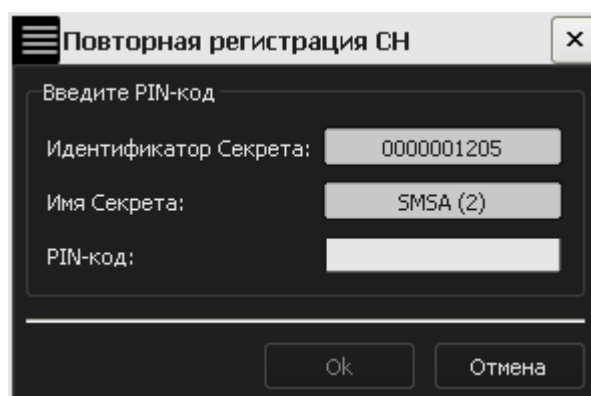


Рисунок 58 – Окно ввода PIN-кода дружественной флешки СА

Далее укажите путь к файлу с мандатом регистрации и нажмите кнопку <OK> (рисунок 59).

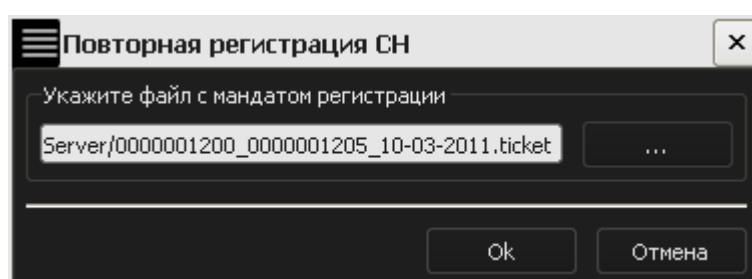


Рисунок 59 – Окно для указания файла с мандатом регистрации

Путь можно указан вручную или задать с помощью кнопки <...>.

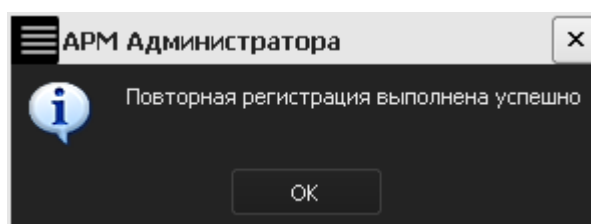


Рисунок 60 – Оповещение об успешной повторной регистрации

Если все хорошо, то на экране появится сообщение об успешной регистрации «Секрета» (рисунок 60)

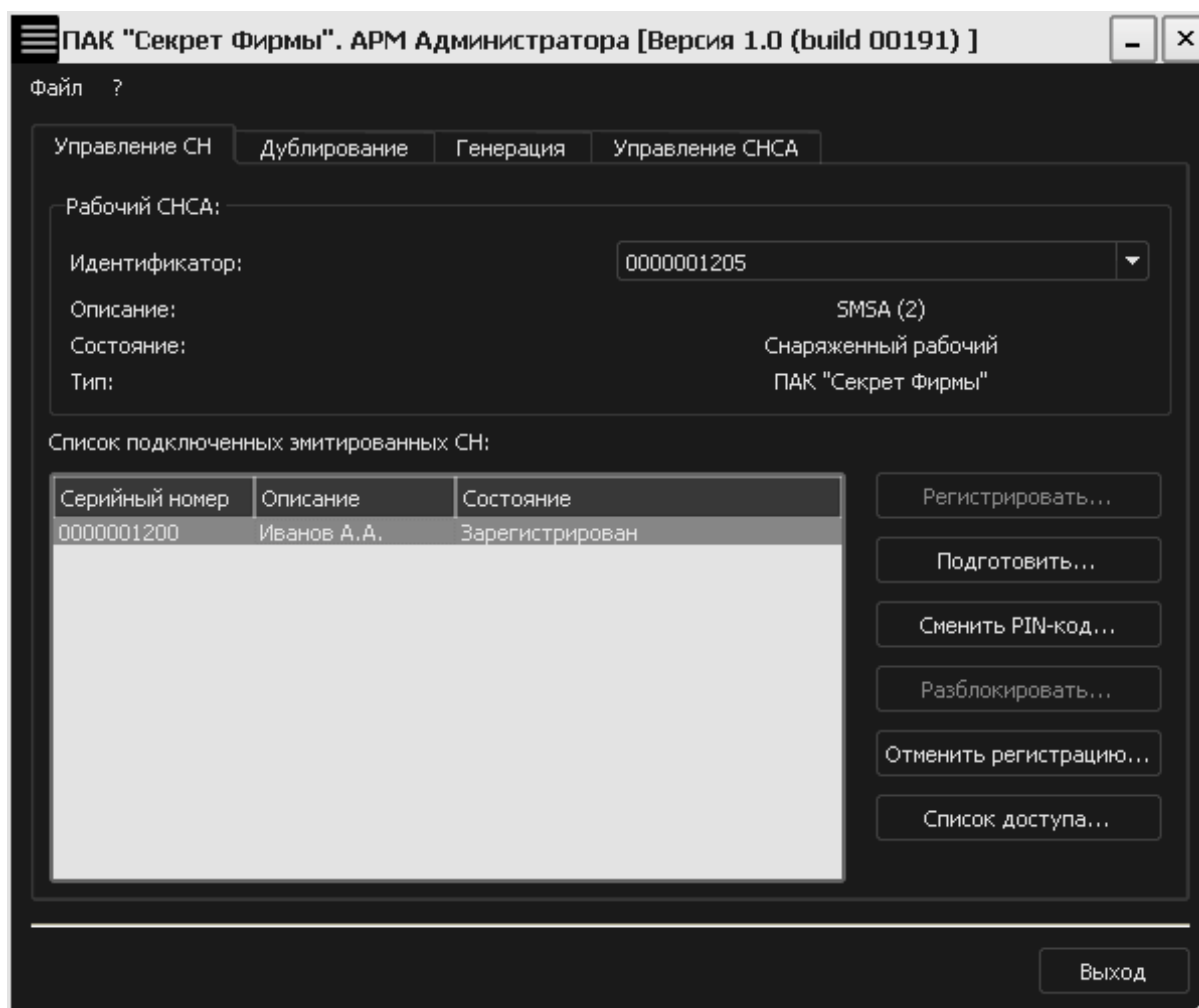


Рисунок 61 – АРМ Администратора. Вкладка «Управление СН»

После выполнения повторной регистрации «Секрета» его статус во вкладке «Управление СН» программы «АРМ Администратора» изменяется на «Зарегистрирован» (рисунок 61) и можно получить доступ к флешке «Секрет». При этом можно использовать «Секрет» на ранее зарегистрированном компьютере.

3.7. Отмена регистрации «Секрета Фирмы»

Если Вы поработали с «Секретом» на каком-то компьютере, а больше на нем Вам работать не надо, то нужно исключить его из «своих» компьютеров. Для этого нужно аннулировать регистрацию «Секрета» на нем и регистрацию его в «Секрете».

Лучше это обязательно делать, чтобы в списке «своих» всегда были только нужные компьютеры, а не все на которых когда-то понадобилось немножко поработать.

После отмены регистрации с этим «Секретом» на этом компьютере Вы не сможете уже работать – до того, как снова его зарегистрируете (можно сколько

угодно раз регистрировать и аннулировать регистрацию на одном и том же компьютере, хоть каждый день, если Вы чего-то опасаетесь).

Если Вы отмените регистрацию на одном дружественном компьютере, то на другом дружественном компьютере Вы сможете работать. Если Вы отмените регистрацию на первичном компьютере (т.е. на том компьютере, на котором Вы первый раз зарегистрировали «Секрет»), то на компьютерах, на которых «Секрет» регистрировался повторно, работать с флешкой будет нельзя.

Для отмены регистрации «Секрета» во вкладке «Управление СН» программы «АРМ Администратора» выберите нужный «Секрет» из списка зарегистрированных и нажмите кнопку <Отменить регистрацию> (рисунок 62).

ВНИМАНИЕ! Во время отмены регистрации «Секрета», не отключайте «Секрет» от компьютера. Он может сломаться!

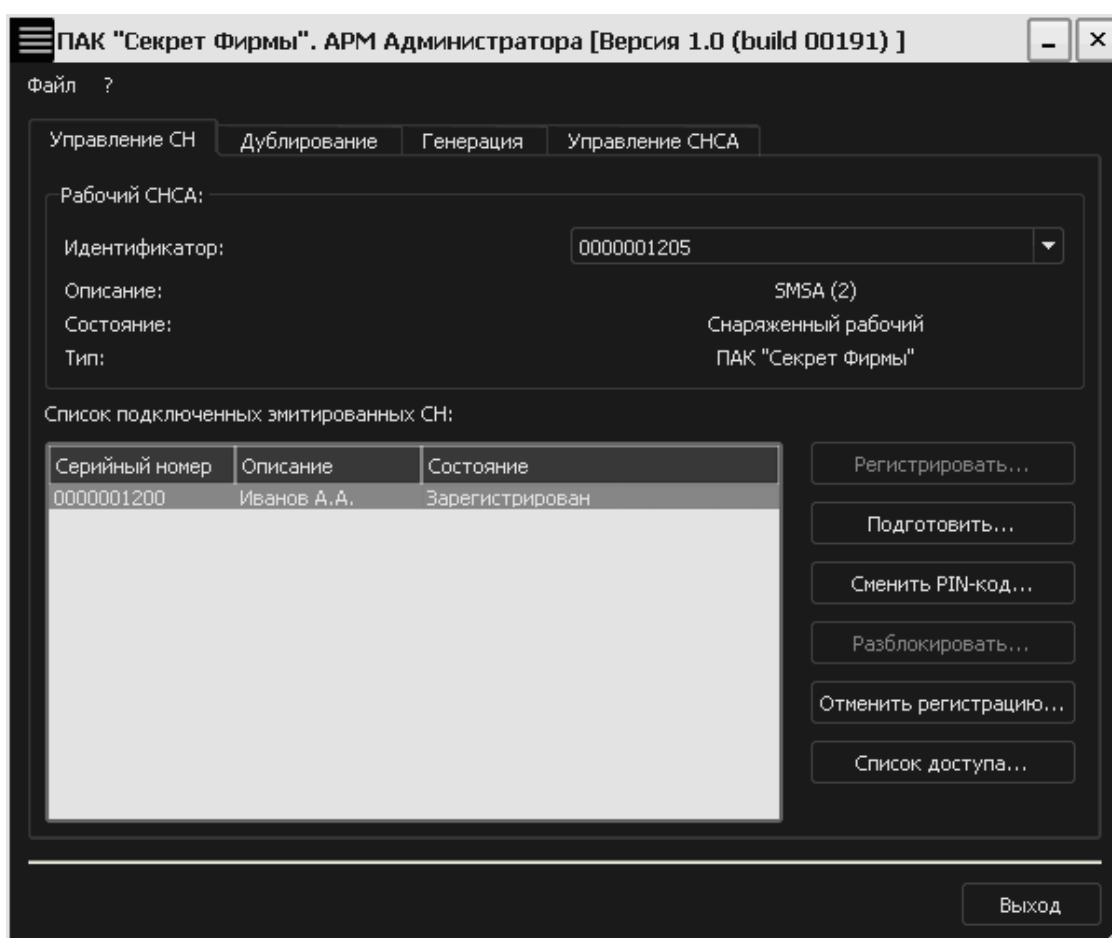


Рисунок 62 – Главное окно АРМ Администратора. Вкладка «Управление СН»

В появившемся окне Пользователю необходимо ввести код регистрации данного «Секрета» (рисунок 63). Нажмите кнопку <ОК>.

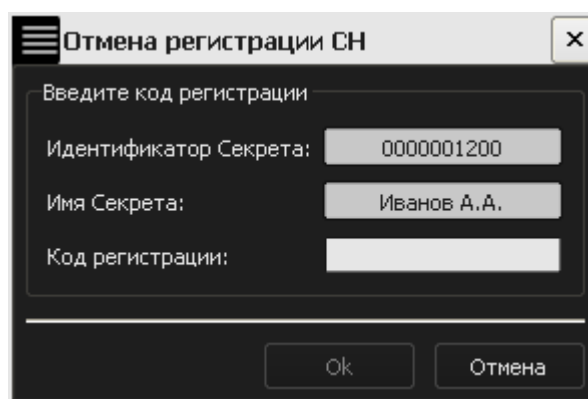


Рисунок 63 – Окно ввода кода регистрации

В следующем окне введите PIN-код соответствующей флешки СА (рисунок 64).

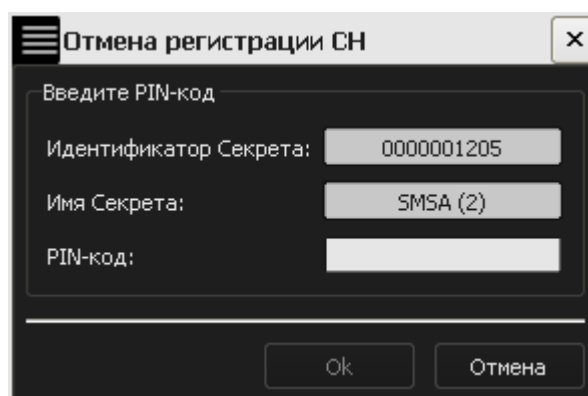


Рисунок 64 – Окно ввода PIN-кода для соответствующей флешки СА

Если Вы ввели неверный PIN-код, то на экран выводится оповещение об ошибке:

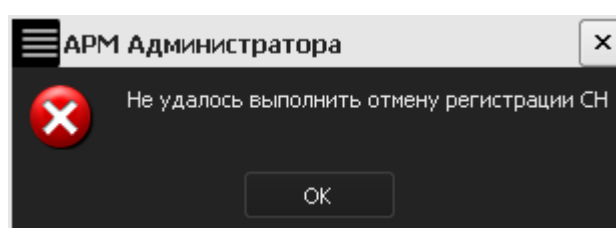


Рисунок 65 – Сообщение о сбое в ходе отмены регистрации

Если все выполнено правильно, то на экране появится сообщение (рисунок 66).

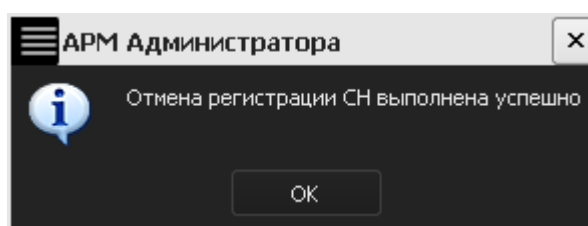


Рисунок 66 - Сообщение об успешной отмене регистрации

После отмены регистрации «Секрета» его статус в главном окне программы «АРМ Администратора» изменяется на «Не зарегистрирован» (рисунок 67).

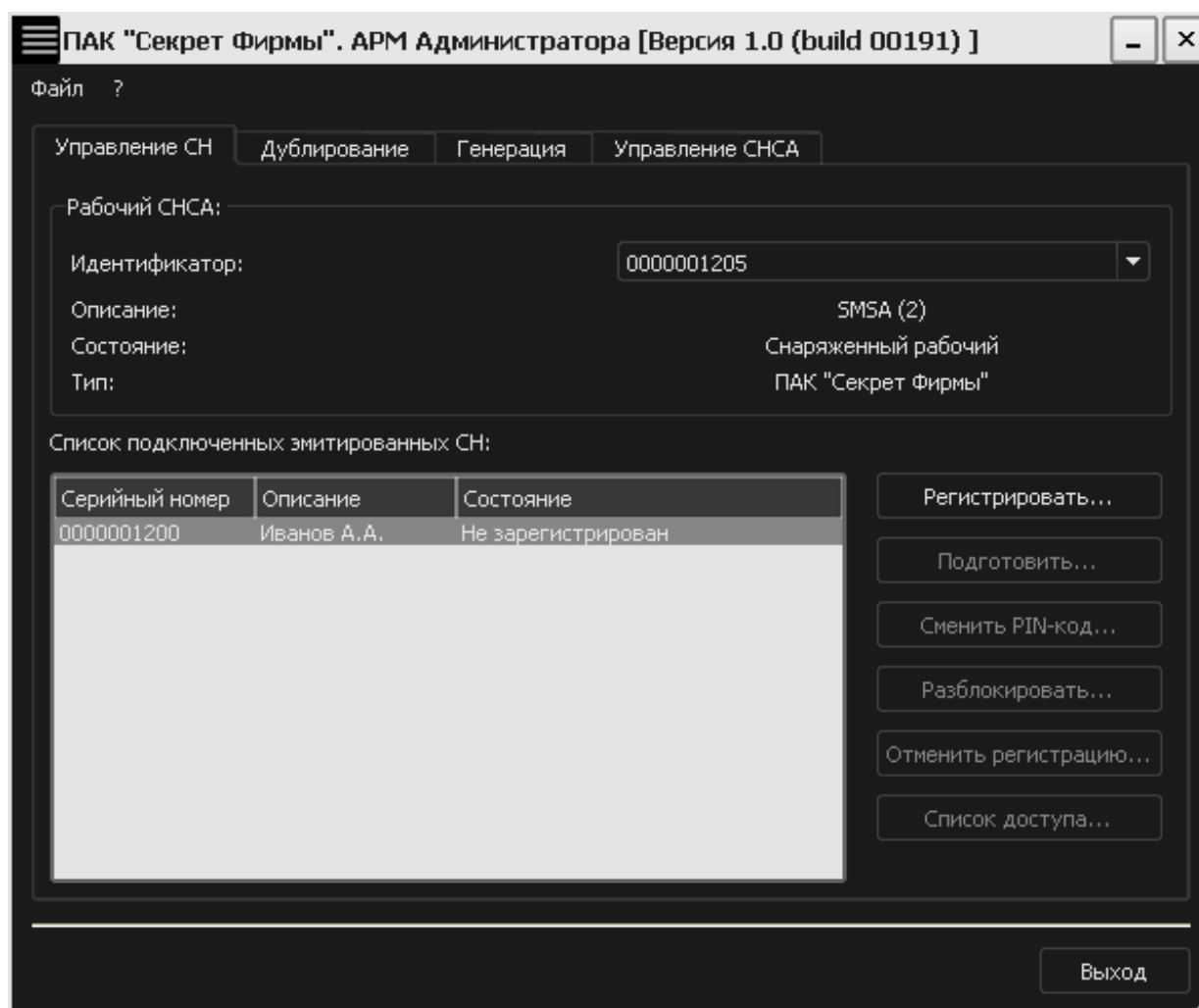


Рисунок 67 – Главное окно АРМ Администратора. Вкладка «Управление СН»

Теперь работать с «Секретом» невозможно.

3.8. Смена PIN-кода флешки СА

Если Вы считаете, что PIN-код флешки СА кто-то узнал, то смените его на новый.

Подключите флешку СА к СА. Во вкладке «Управление СНСА» программы «АРМ Администратора» выберите из списка нужную флешку СА и нажмите кнопку <Сменить PIN-код> (рисунок 68).

ВНИМАНИЕ! Во время смены PIN-кода флешки СА не отключайте «Секрет» от компьютера. Он может сломаться!

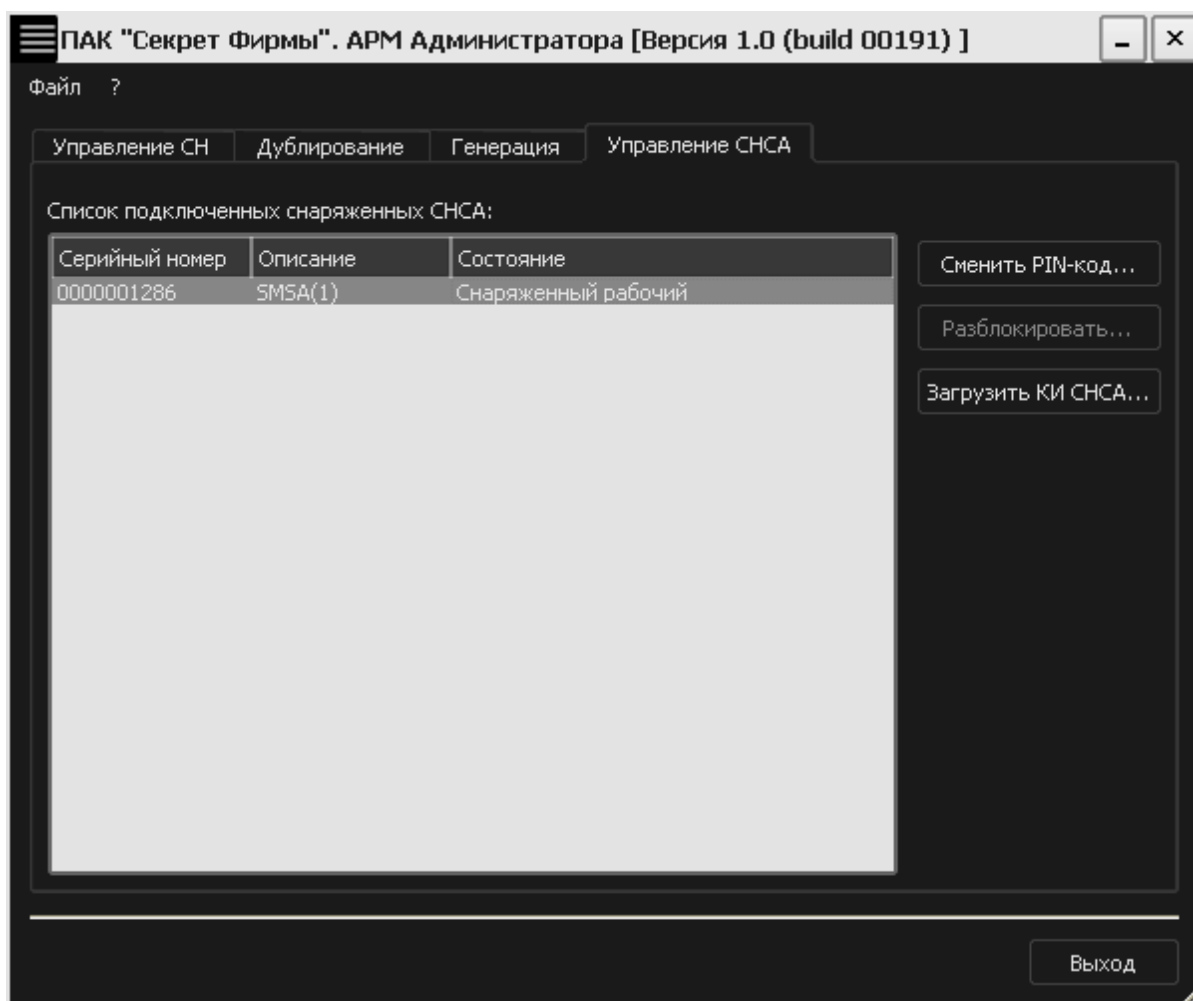


Рисунок 68 – Главное окно АРМ Администратора. Вкладка «Управление СНСА»

В следующем окне введите старый PIN-код данной флешки СА (рисунок 69).

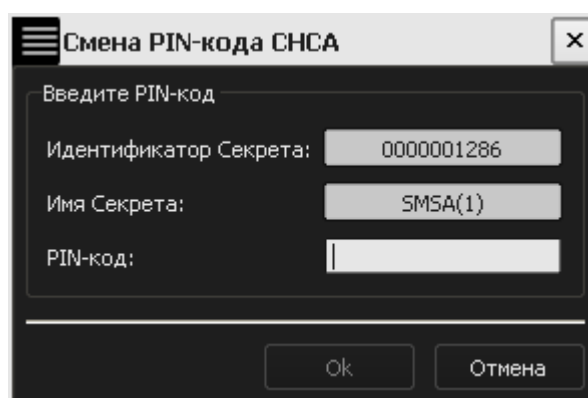


Рисунок 69 – Окно ввода PIN-кода для данной флешки СА

Если все выполнено правильно, то появится сообщение об успешной смене PIN-кода (рисунок 70), который генерируется автоматически. Нажмите кнопку <OK>.

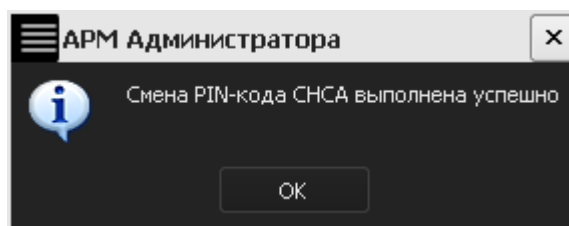


Рисунок 70 - Сообщение об успешной смене PIN-кода флешки СА

Следующее окно содержит новый PIN-код флешки СА, который необходимо запомнить или надежно сохранить (рисунок 71).

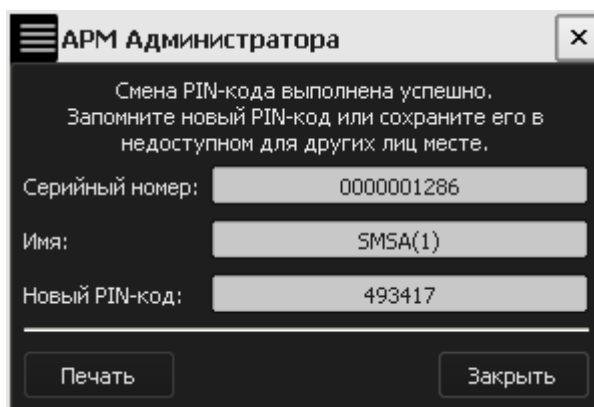


Рисунок 71 – Окно с новым PIN-кодом для флешки СА

Можно распечатать новый PIN-код. Для этого нужно нажать кнопку <Печать>, а затем кнопку <Да>.

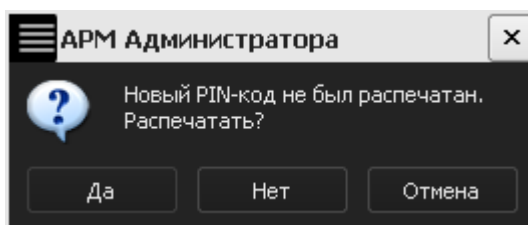


Рисунок 72 – Предупреждающее сообщение

Если Вы не распечатали новый PIN-код, на экран выводится сообщение (рисунок 72). Если Вы не хотите печатать новый PIN-код, нажмите кнопку <Нет>.

3.9. Смена PIN-кода флешки «Секрет»

Если Вы думаете, что PIN-код кто-то узнал, то нужно сменить его на новый.

Подключите «Секрет» к серверу аутентификации. Если флешек «Секрет» несколько, то допускается использование USB-хаба с собственным источником питания (см. 1.3).

Во вкладке «Управление СН» программы «АРМ Администратора» выберите из списка нужный «Секрет» и нажмите кнопку <Сменить PIN-код> (рисунок 73).

ВНИМАНИЕ! Во время смены PIN-кода «Секрета» не отключайте его от компьютера. Он может сломаться!

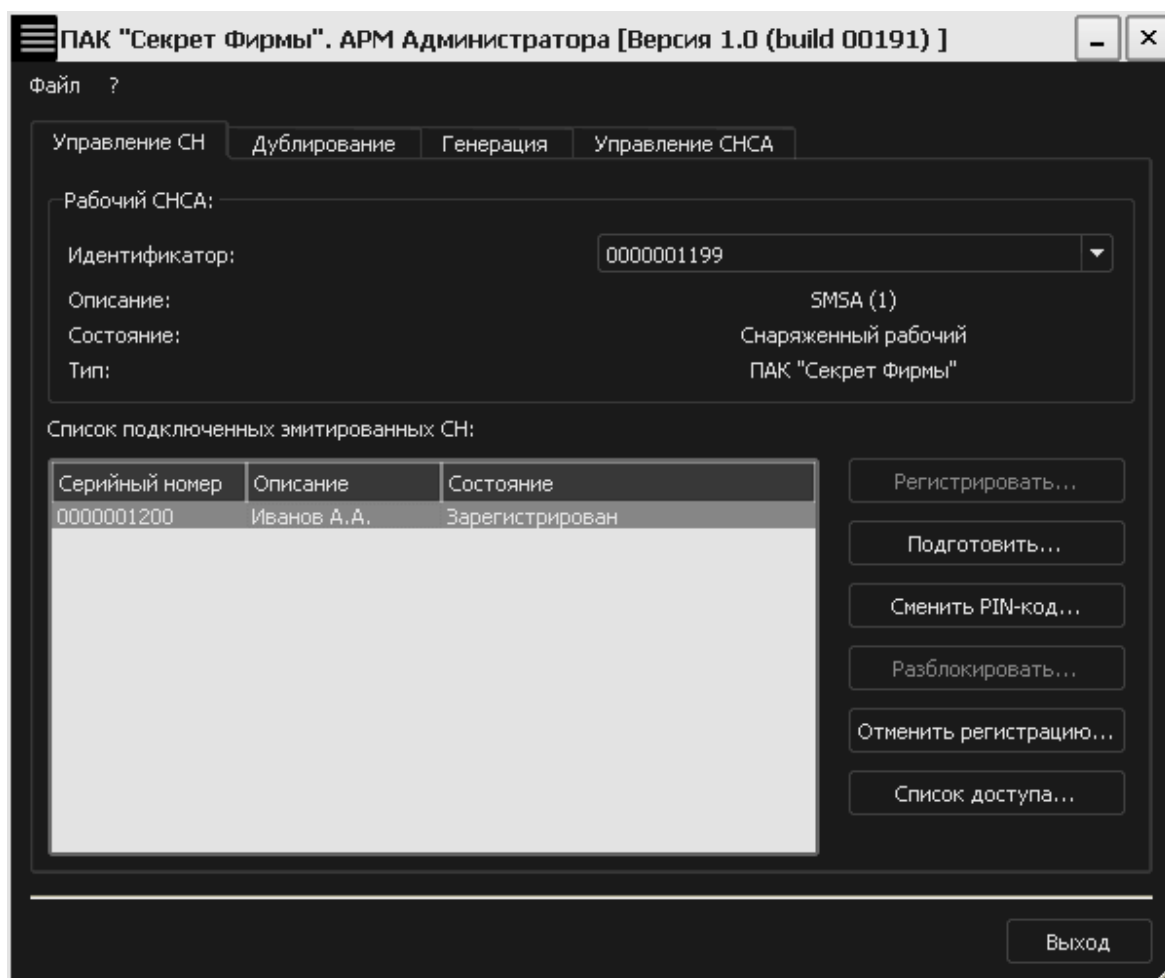


Рисунок 73 – Главное окно АРМ Администратора. Вкладка «Управление СН»

В появившемся окне Пользователь должен ввести старый PIN-код данного «Секрета», указать новый PIN-код, а также подтвердить ввод нового PIN-кода (написать новый PIN-код еще раз в поле «Подтвердите PIN-код») (рисунок 74).

Рисунок 74 – Окно смены PIN-кода на желаемый Пользователем

Можно задать новый PIN-код самостоятельно (как описано выше) или сгенерировать его автоматически с помощью установки галочки «Генерировать автоматически» (рисунок 75).

Рисунок 75 - Окно смены PIN-кода на сгенерированный автоматически

В появившемся окне введите PIN-код флешки СА, к которой относится данный «Секрет» (рисунок 76).

Рисунок 76 – Окно ввода PIN-кода для соответствующей флешки СА

В случае ошибки на экране появится сообщение (рисунок 77).

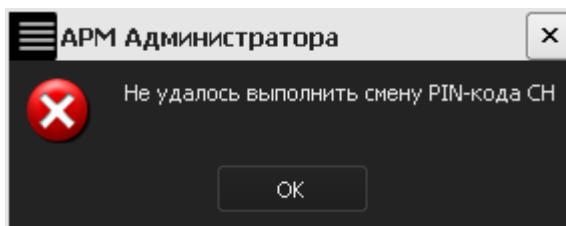


Рисунок 77 - Сообщение об ошибке в ходе смены PIN-кода

Если все выполнено правильно, то появится сообщение (рисунок 78).

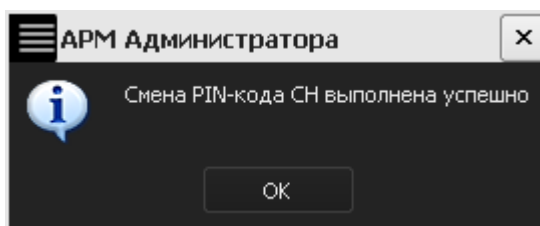


Рисунок 78 - Сообщение об успешной смене PIN-кода

Следующее окно содержит новый PIN-код, который необходимо запомнить или надежно сохранить (рисунок 79). Можно распечатать новый PIN-код. Для этого нажмите кнопку <Печать>, затем в следующем окне – кнопку <Да>.

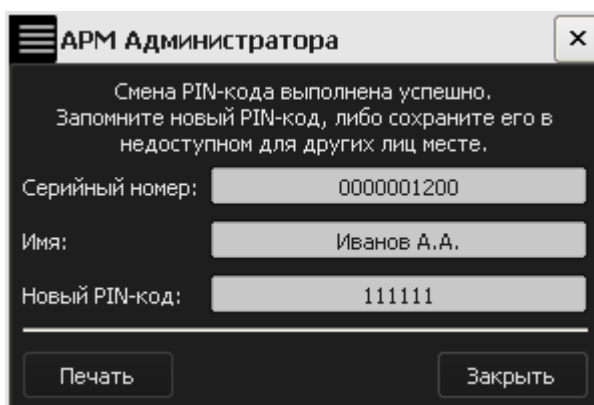


Рисунок 79 – Окно с новым PIN-кодом

Если Вы не хотите печатать PIN-код, нажмите кнопку <Нет> (рисунок 80).

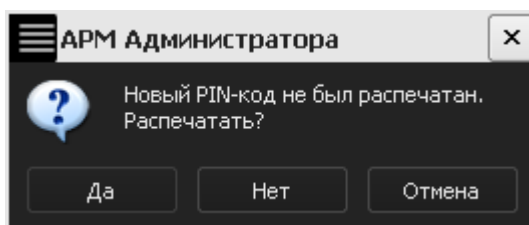


Рисунок 80 – Предупреждающее сообщение

3.10. Разблокирование «Секрета»

Если три раза подряд неправильно ввести PIN-код, «Секрет» заблокируется и на экране появится сообщение (рисунок 81).

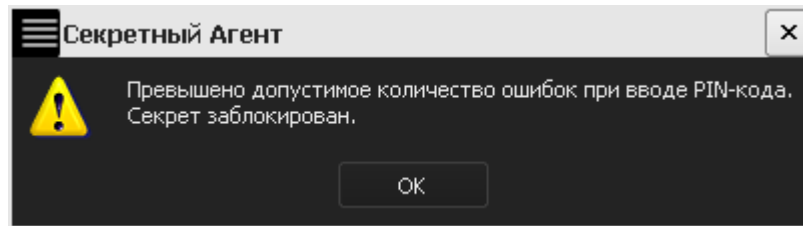


Рисунок 81 – Оповещение о блокировке

Если подключить заблокированный «Секрет» к компьютеру, на экране появляется следующее окно:

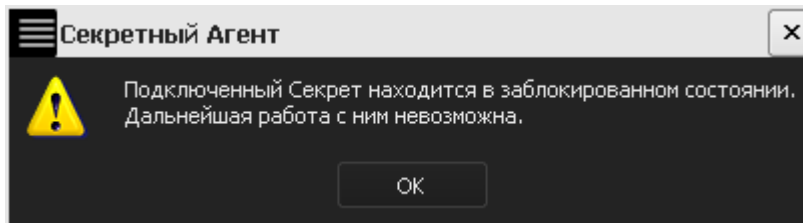


Рисунок 82 – Оповещение при подключении к USB-порту компьютера о блокировке

При этом в главном окне программы «АРМ Администратора» про этот «Секрет» будет написано не «Зарегистрирован», а «Заблокирован» и единственной доступной операцией становится <Разблокировать> (рисунок 83).

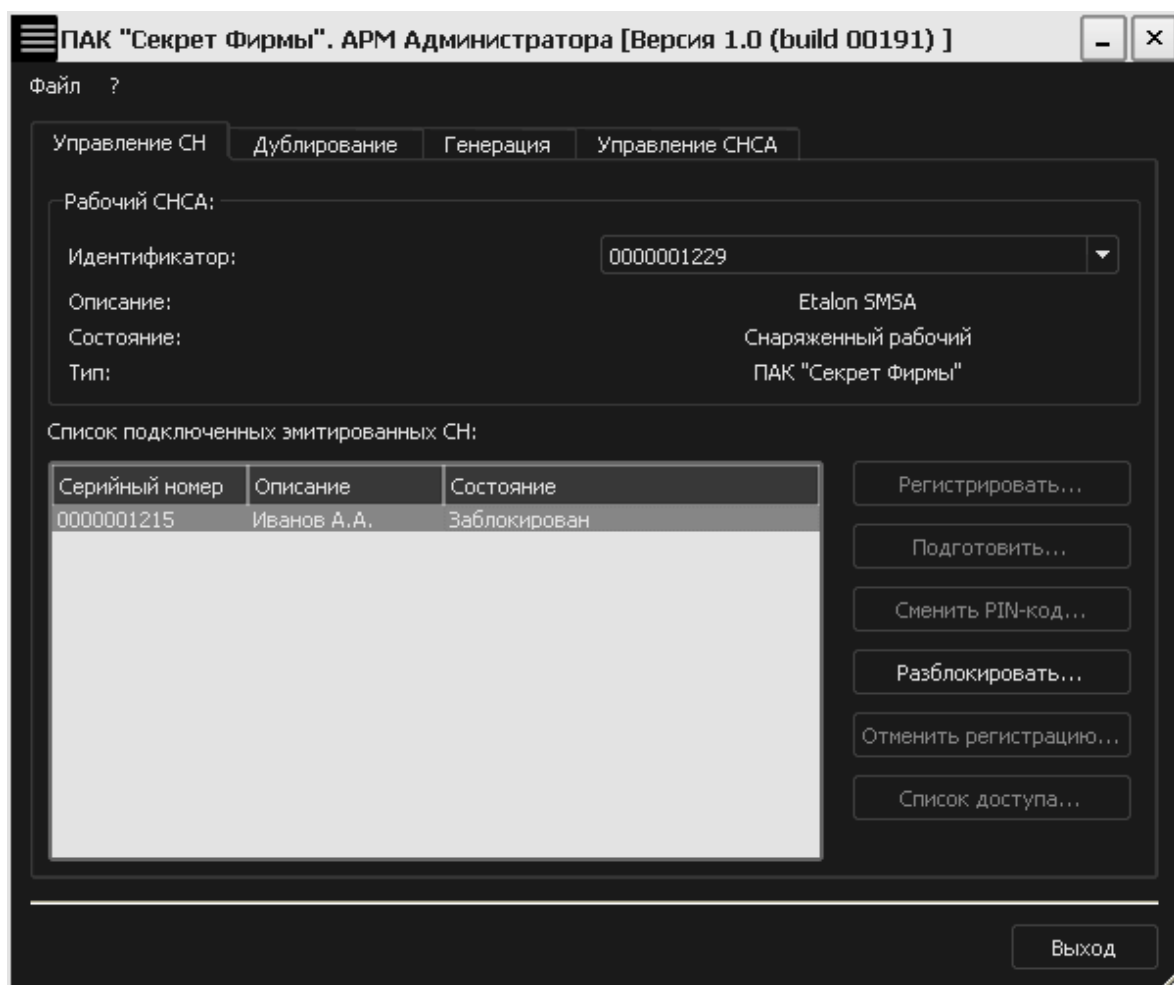


Рисунок 83 – Вкладка «Управление СН» АРМ Администратора

Подключите заблокированный «Секрет» и рабочую флешку СА к серверу аутентификации. Выберите свой «Секрет» в списке и нажмите <Разблокировать>. В появившемся окне нужно ввести код регистрации и новое значение PIN-кода (рисунок 38), . При этом можно использовать USB-хаб с собственным источником питания (см. 1.3).

ВНИМАНИЕ! Во время разблокирования «Секрета» не отключайте его от компьютера. Он может сломаться!

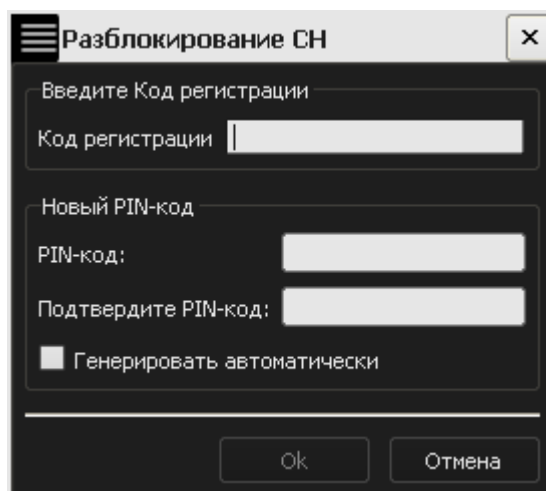


Рисунок 84 – Разблокирование «Секрета»

Пользователь может задать новый PIN-код самостоятельно или сгенерировать его автоматически с помощью установки галочки «Генерировать автоматически» (рисунок 84).

Нажмите кнопку <ОК>. В появившемся далее окне введите PIN-код рабочей флешки СА, к которой относится данный «Секрет» (рисунок 85).

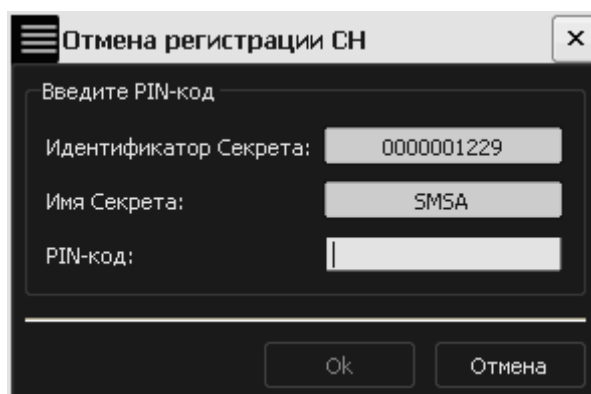


Рисунок 85 – Окно ввода PIN-кода флешки СА

Если все выполнено правильно, на экране появится окно (рисунок 86). Нажмите кнопку <ОК>.

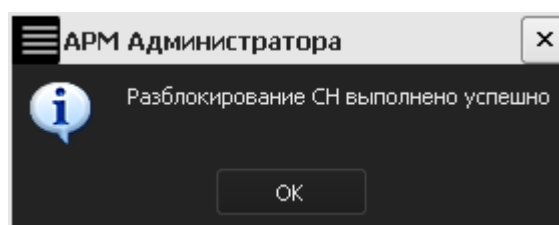


Рисунок 86 – Оповещение об успешной разблокировке

Появляется окно с новым PIN-кодом, который необходимо запомнить или надежно сохранить (рисунок 87). Можно распечатать новый PIN-код. Для этого нажмите кнопку <Печать>, затем в следующем окне – кнопку <Да>.

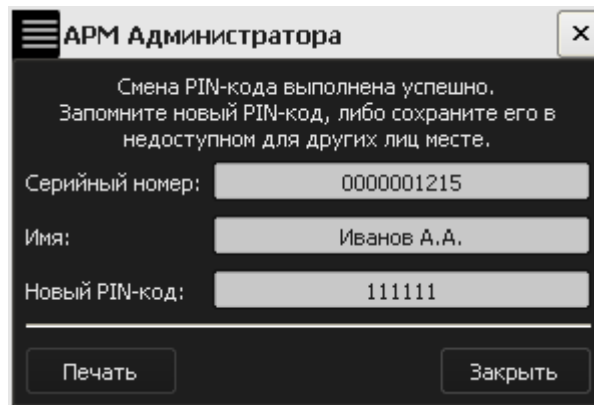


Рисунок 87 – Новый PIN-код разблокированного «Секрета»

Если Вы не распечатали новый PIN-код, на экран выводится сообщение (рисунок 88). Если Вы не хотите печатать новый PIN-код, нажмите кнопку <Нет>.

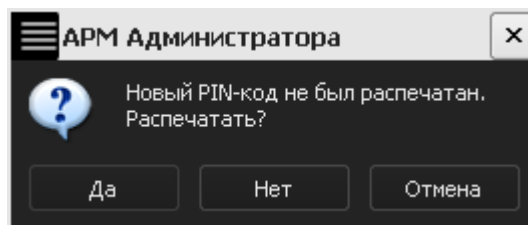


Рисунок 88 – Предупреждающее сообщение

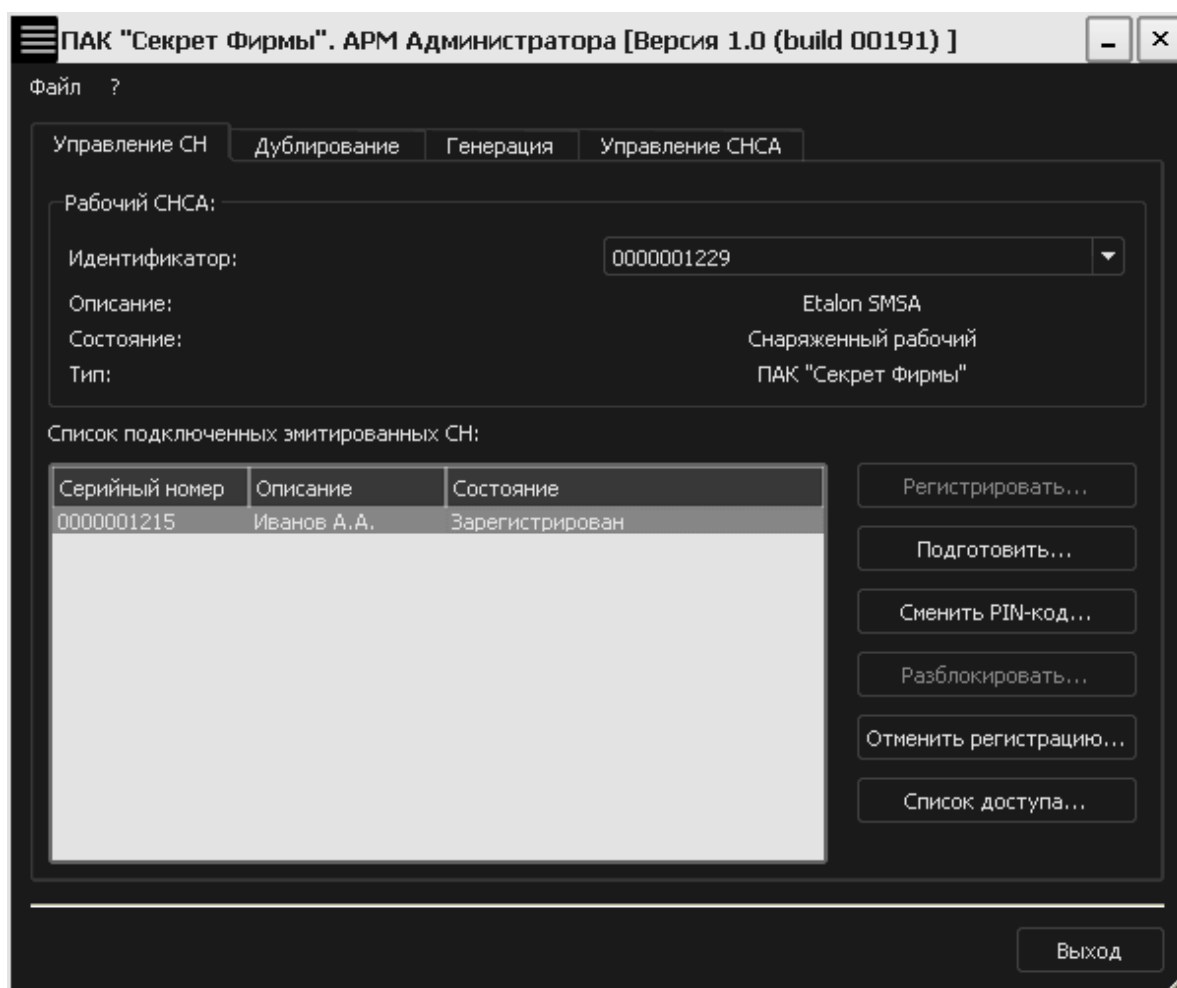


Рисунок 89 – Вкладка «Управление СН» АРМ Администратора

После успешного разблокирования работа с «Секретом» может быть продолжена (рисунок 89).

3.11. Разблокирование флешки СА

Если три раза подряд неправильно ввести PIN-код, флешка СА заблокируется и на экране появится сообщение (рисунок 90).

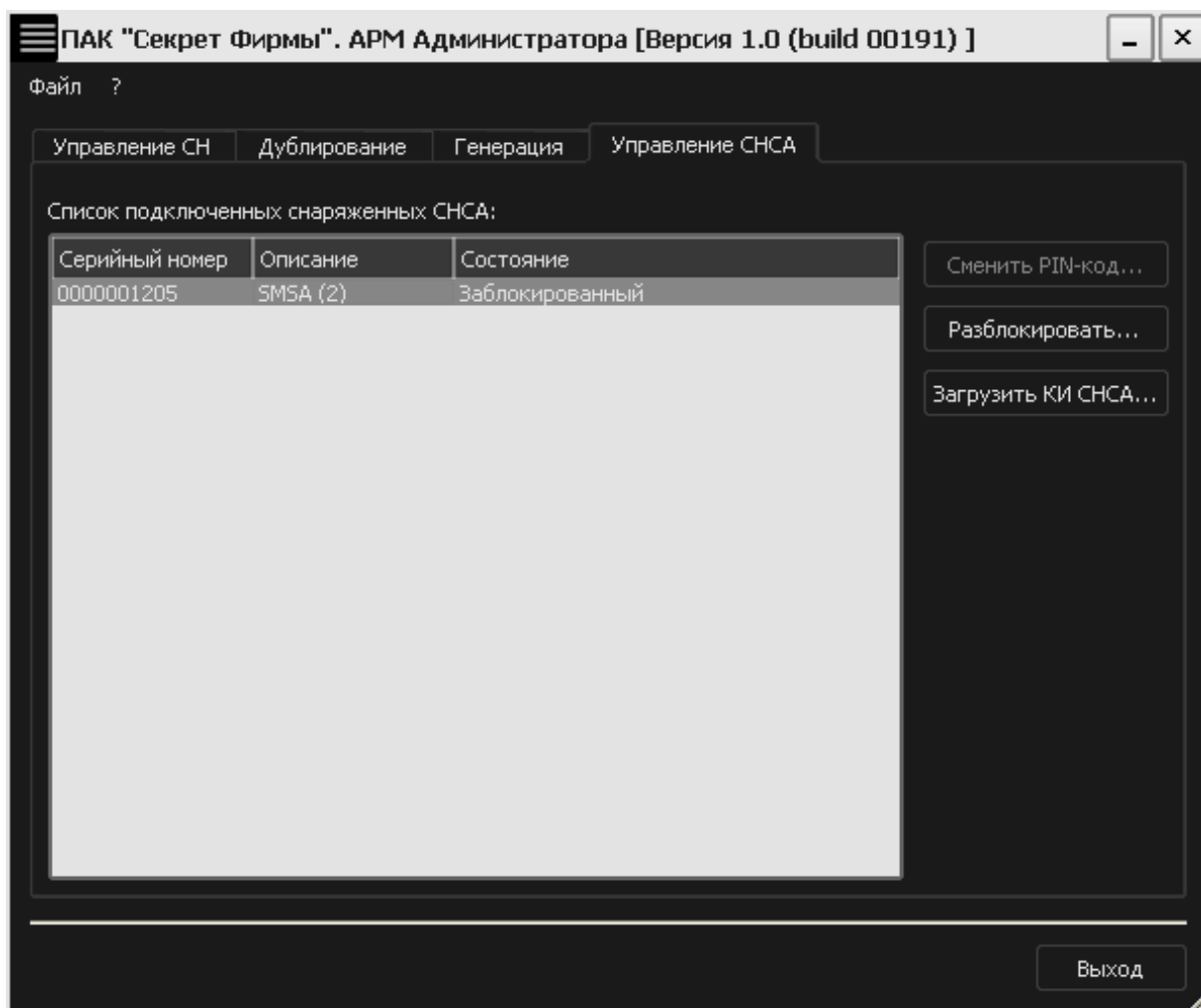


Рисунок 90 - Вкладка «Управление СНСА» АРМ Администратора

Для разблокирования флешки СА выберите из списка нужную флешку и нажмите кнопку <Разблокировать>.

ВНИМАНИЕ! Во время разблокирования флешки СА не отключайте ее от компьютера. Она может сломаться!

В появившемся окне введите код регистрации флешки СА, которую необходимо разблокировать (рисунок 91).

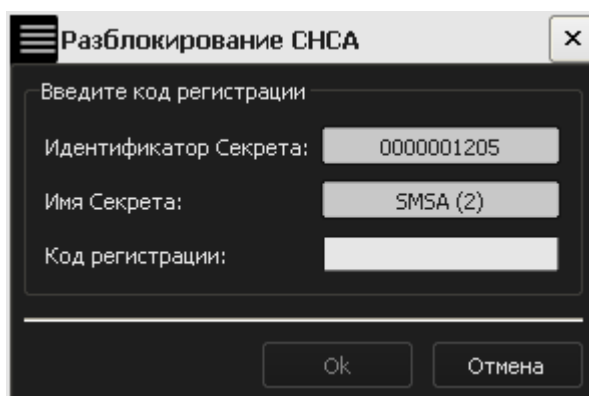


Рисунок 91 – Окно ввода кода регистрации флешки СА, которую необходимо разблокировать

Если все выполнено правильно, на экране появится окно (рисунок 92).

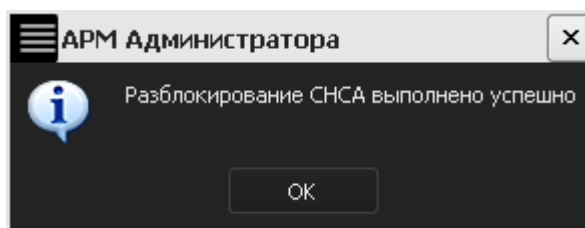


Рисунок 92 – Оповещение о разблокировке

Информацию о новом PIN-коде флешки СА можно распечатать, нажав кнопку <Печать> (рисунок 93).

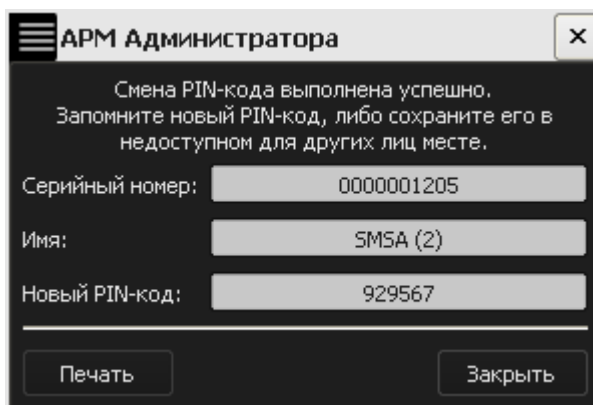


Рисунок 93 – Новый PIN-код разблокированной флешки СА

Если PIN-код не был распечатан, то по нажатии кнопки <Заккрыть> на экран выводится сообщение (рисунок 94).

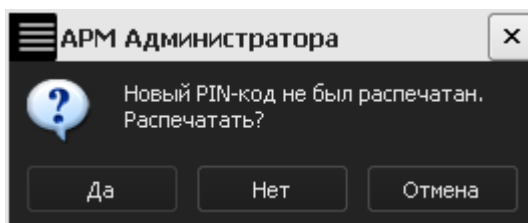


Рисунок 94 – Предупреждающее сообщение

В случае, если Вы не хотите печатать PIN-код, то нажмите кнопку <Нет>.

После успешного разблокирования работа с флешкой СА может быть продолжена.

4. Журнал регистрации событий

Все действия с «Секретом», зарегистрированным на данном компьютере, записываются в журнал регистрации событий (рисунок 95).

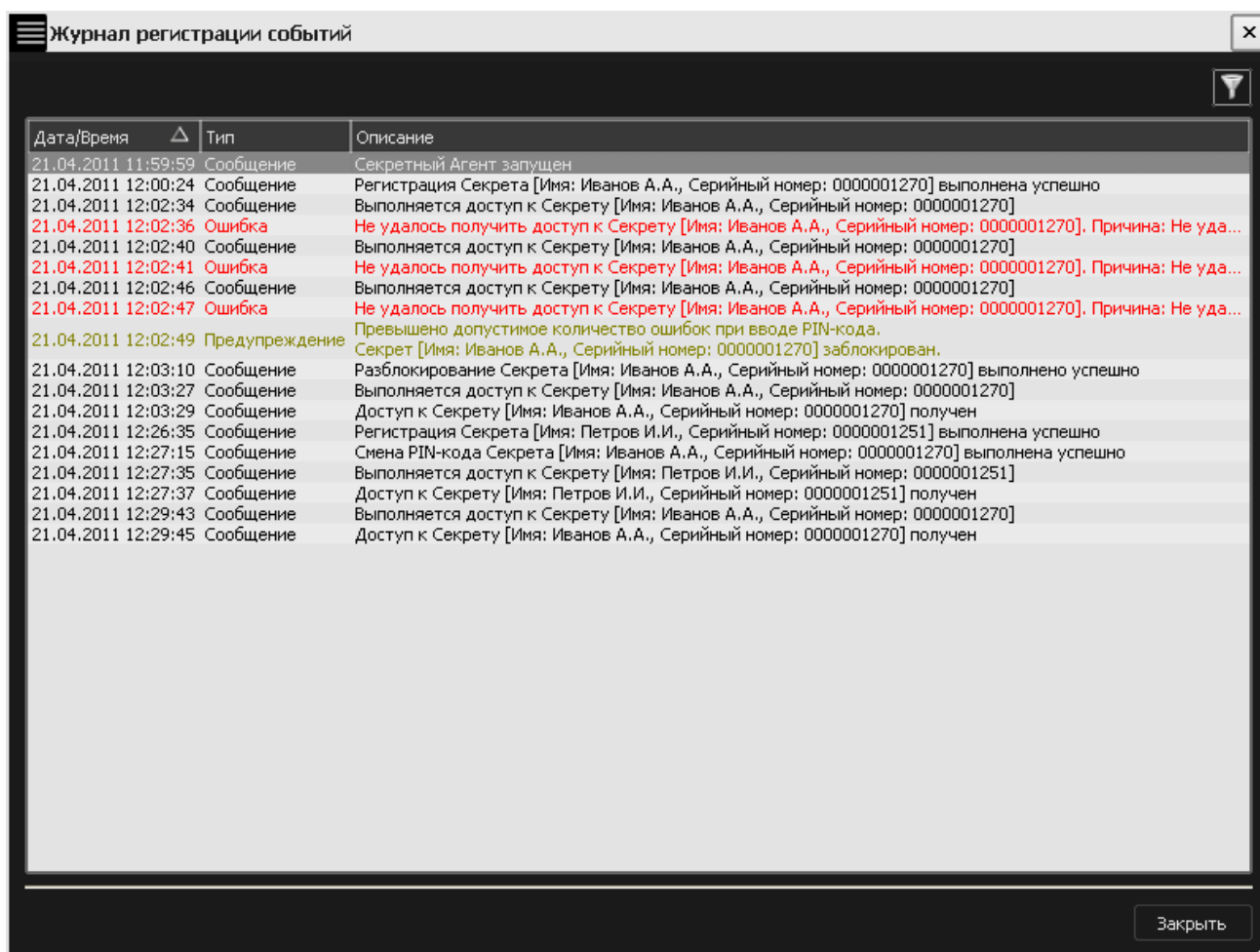


Рисунок 95 – Окно просмотра журнала регистрации событий

Чтобы посмотреть журнал событий «Секрета», необходимо правой кнопкой мыши нажать на значок «Секретного Агента» в трее (справа внизу на панели, где часы) и выбрать пункт «Журнал работы» (рисунок 96).

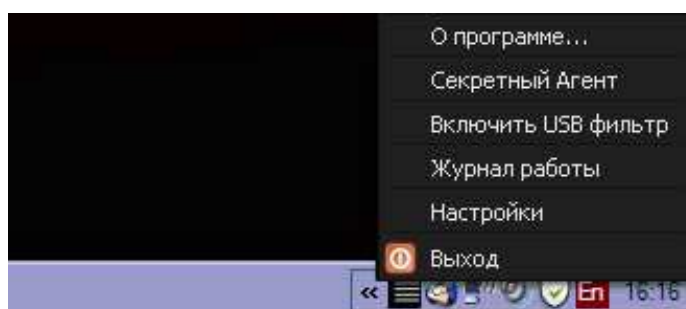


Рисунок 96 - Контекстное меню приложения «Секретный Агент»

Окно просмотра журнала регистрации событий содержит информацию о событиях, зафиксированных при работе Пользователя с «Секретом» на данном компьютере.

Можно отфильтровать события (для упрощения поиска), для этого нажмите кнопку <Фильтр> (рисунок 97).

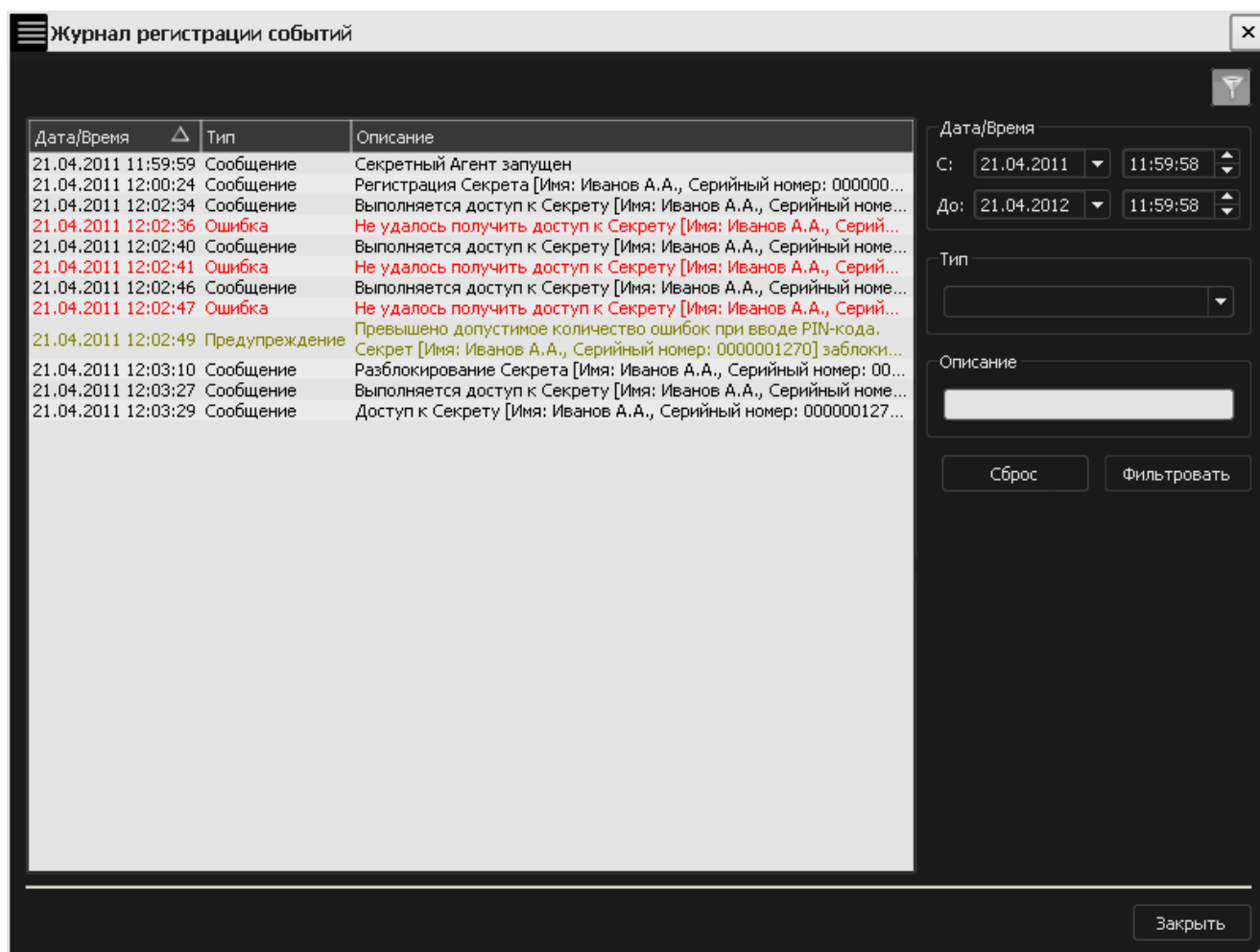


Рисунок 97 – Окно просмотра журнала регистрации событий с панелью для задания параметров фильтрации

В появившемся окне можно задать (для фильтрации событий):

4) «Дата/Время» – поле для выбора временного интервала фильтрации. По умолчанию временной интервал фильтрации установлен с момента старта последней сессии программы «Секретный Агент». При изменении начальных и (или) конечных значений даты и (или) времени в окне журнала появляются все события, зафиксированные при работе с «Секретом» в указанный временной интервал;

5) «Тип» – поле для выбора типа событий, зафиксированных при работе с «Секретом». Фиксируемые события могут принадлежать одной из следующих категорий: сообщение, ошибка, предупреждение. Для нахождения всех событий, принадлежащих одной из трех описанных категорий и зафиксированных в журнале в определенный промежуток времени, следует заполнить необходимый временной интервал, выбрать тип события и нажать кнопку «Фильтровать». В окне просмотра журнала работы появится информация о событиях, удовлетворяющих заданным параметрам фильтрации (рисунок 98). Для того чтобы вернуться к полному списку событий, следует нажать кнопку «Сброс»;

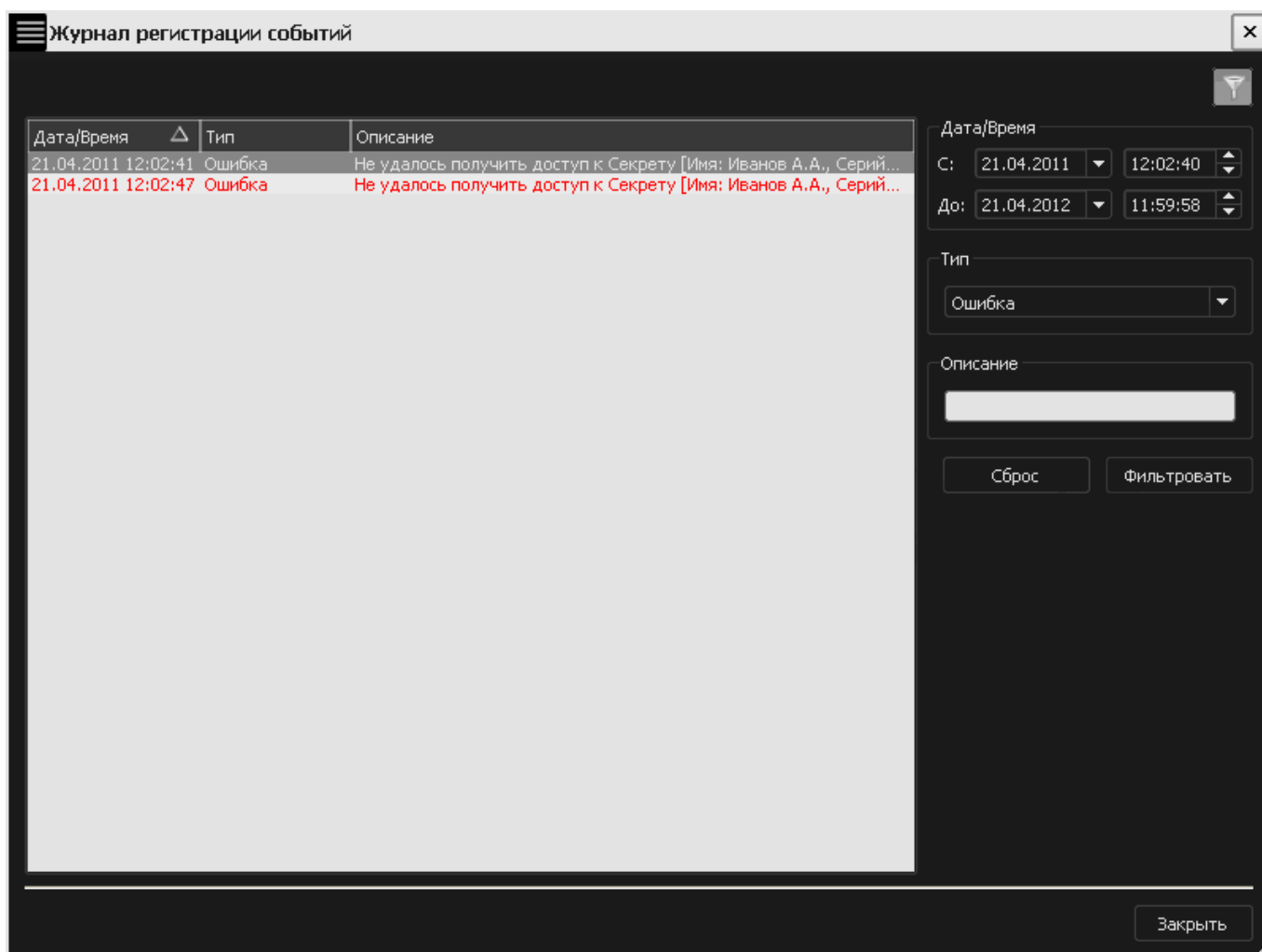


Рисунок 98 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по типу

6) «Описание» – в данное поле вводится фраза или часть фразы описания события, которое необходимо найти. Для нахождения всех событий, содержащих указанную фразу (или часть фразы) и зафиксированных в журнале в определенный промежуток времени, заполните поля «Дата/Время» и «Описание» и нажмите кнопку <Фильтровать>. В окне просмотра журнала регистрации событий появится информация о событиях, удовлетворяющих заданным параметрам фильтрации (рисунок 99).

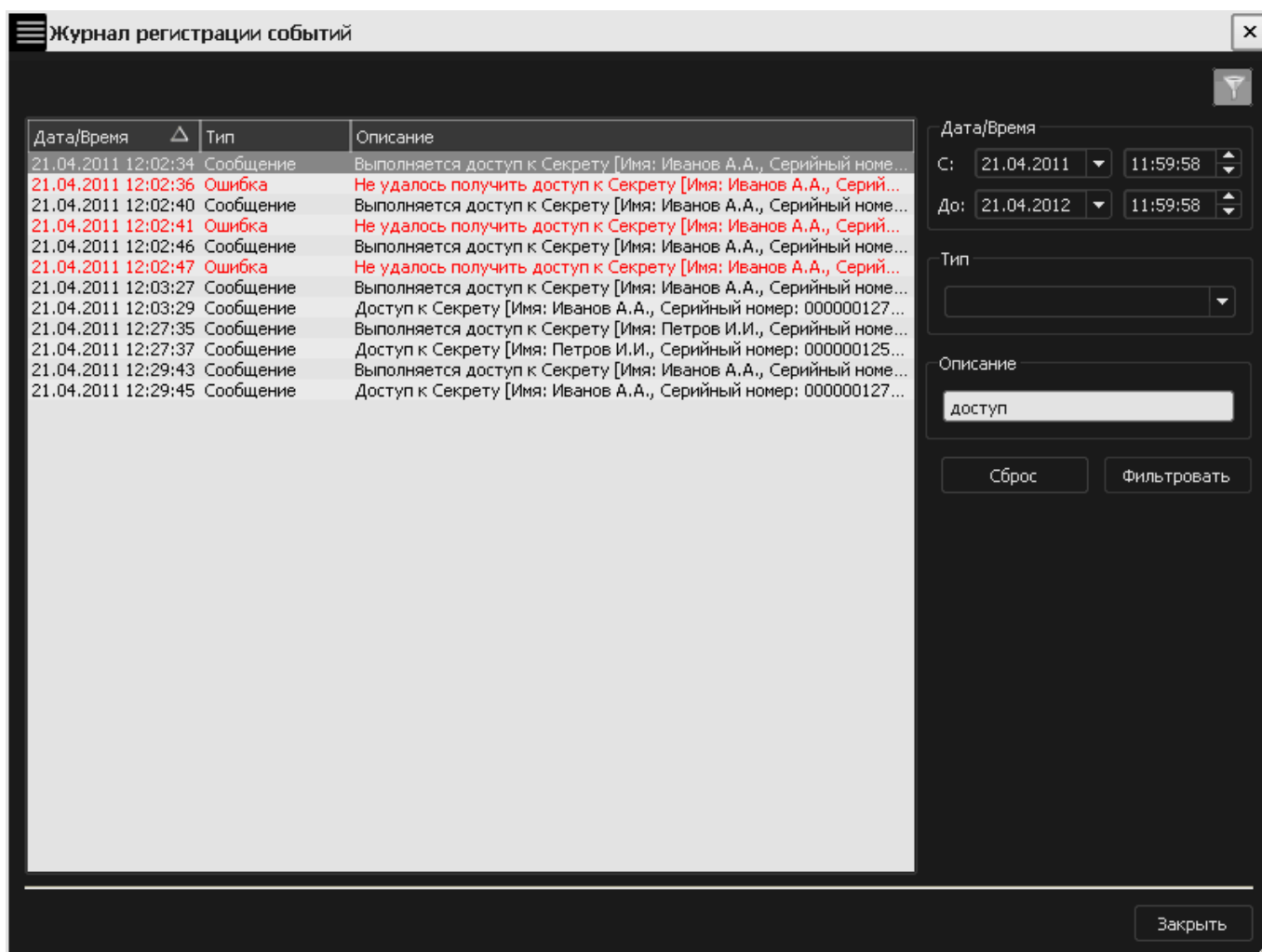


Рисунок 99 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по описанию

Если на данном компьютере используется несколько зарегистрированных «Секретов» (рисунок 95), то с помощью фильтрации по описанию можно легко найти все события, зафиксированные в журнале при работе с конкретным «Секретом», введя в поле «Описание» имя или серийный номер нужного «Секрета» (рисунок 100).

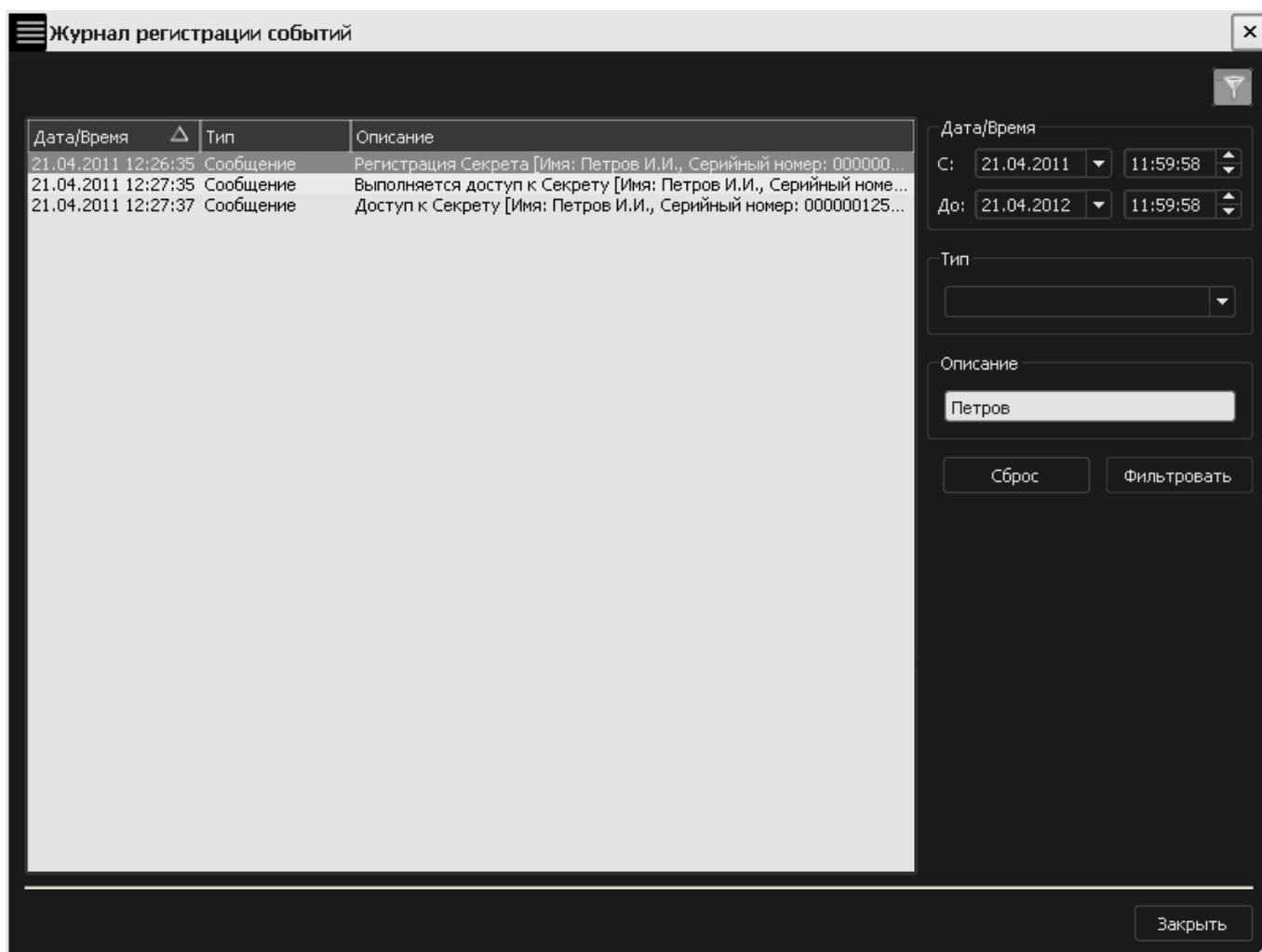


Рисунок 100 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по имени «Секрета»

5. Как применять «Секрет Фирмы» безопасным образом

5.1. Общие сведения

Необходимо помнить, что прежде чем встать из-за компьютера, нужно обязательно заблокировать экран (например, нажатием комбинации клавиш <Win>+<L>).

Это позволит защитить данные Пользователя от посторонних лиц, когда Пользователь отсутствует на рабочем месте, работа с флешкой «Секрет» еще не завершена.

Чтобы подстраховать Пользователя, Администратору рекомендуется:

- устанавливать вход Пользователя в систему с обязательным вводом пароля;
- настраивать автоматическую блокировку экрана компьютера.

5.2. Вход в систему с обязательным вводом пароля

Чтобы установить вход Пользователя в систему с обязательным вводом пароля, необходимо:

1) через меню Пуск->Выполнить запустить команду «control userpasswords2» и в появившемся далее окне «Учетные записи пользователей» поставить галочку «Требовать ввод имени Пользователя и пароля» (рисунок 101). Это можно сделать для компьютеров, не включенных в домен.

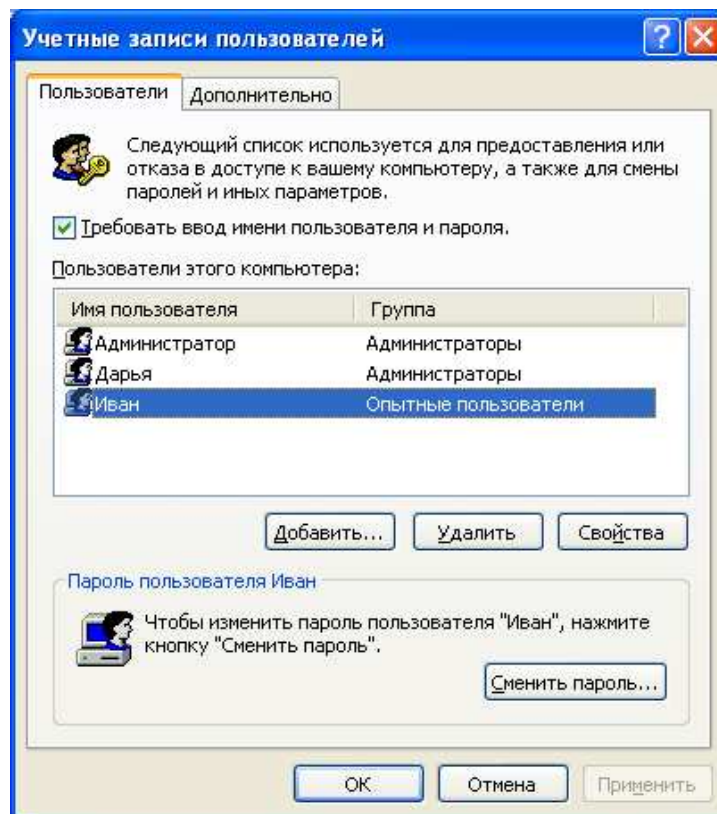


Рисунок 101 – Окно настроек учетных записей Пользователей

2)если выбранному Пользователю еще не задан пароль для входа в систему, следует нажать кнопку <Сменить пароль...> и в появившемся далее окне смены пароля задать и подтвердить новый пароль (рисунок 102).

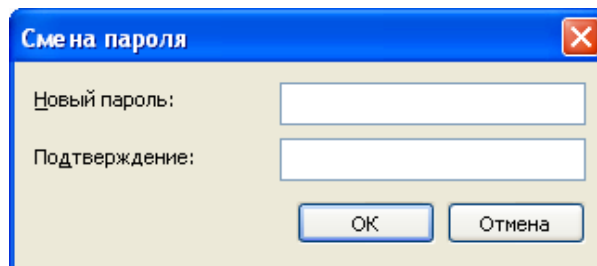


Рисунок 102 – Окно смены пароля Пользователя для входа в ОС

5.3. Включение режима автоматической блокировки экрана

Для включения режима автоматической блокировки следует:

- при работе в Windows XP: в меню Пуск->Панель управления-> Экран->Заставка установить галочку «Начинать с экрана приветствия» и выставить необходимый срок неактивности (рисунок 103).

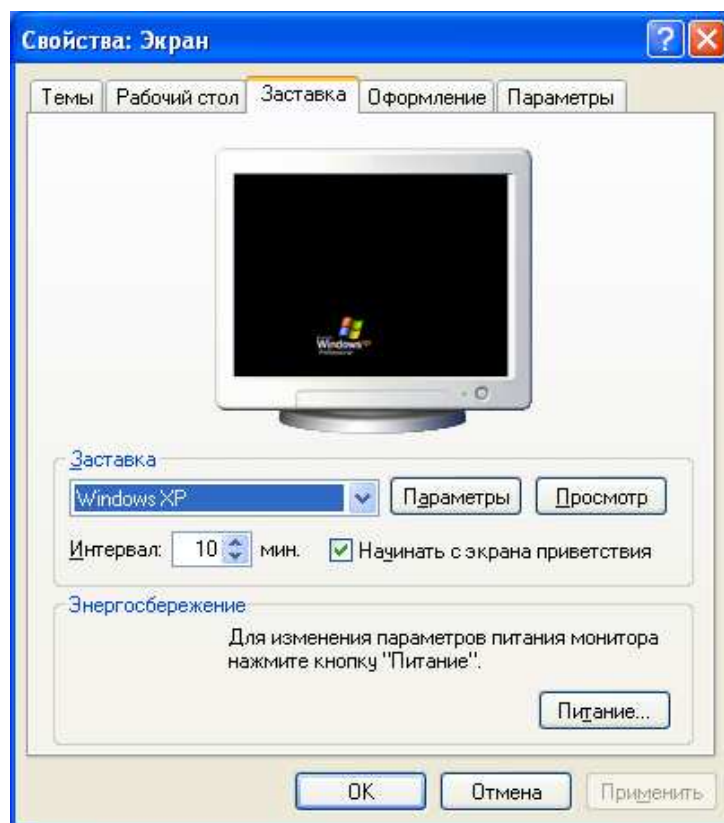


Рисунок 103 – Окно настройки заставки экрана в ОС Windows XP

•при работе в Windows 7: в меню Пуск->Панель управления->Персонализация->Заставка установить галочку «Начинать с экрана входа в систему» и выставить необходимый срок неактивности (рисунок 104).

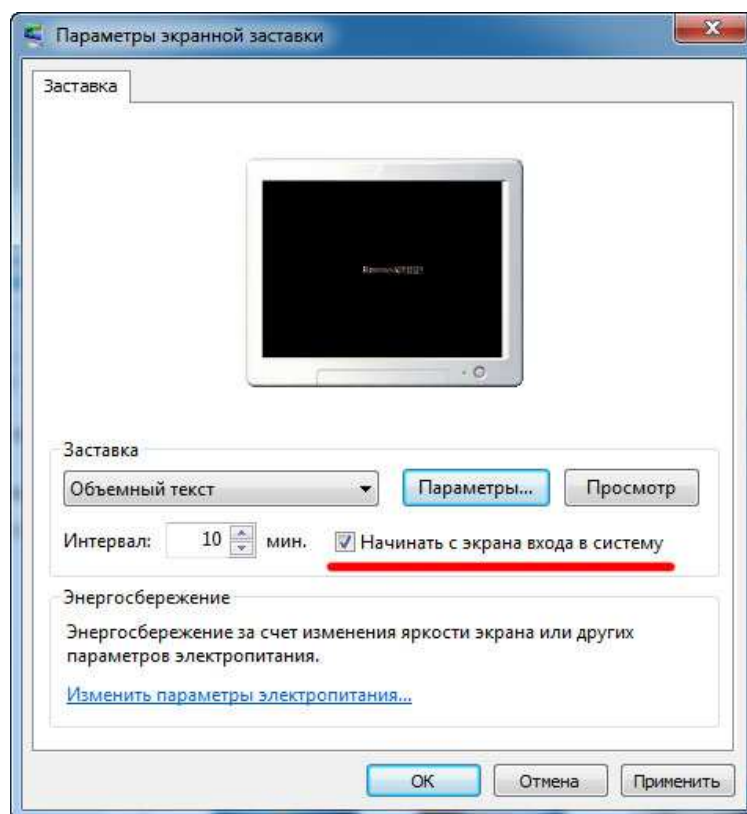


Рисунок 104 - Окно настройки заставки экрана в ОС Windows 7

6. Перечень принятых сокращений и обозначений

АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СН	Специальный носитель
СНСА	Специальный носитель сервера аутентификации
СНЭ	Специальный носитель эмитента

7. Возможные сообщения в журнале событий «Секрета Фирмы»

Виды возможных сообщений «Секрета Фирмы» и их описание приведены в таблице 1.

Таблица 1 - Возможные неполадки в работе «Секрета Фирмы» и порядок действий Администратора по их устранению

Описание неполадки	Возможные причины возникновения неполадки	Порядок действий по устранению
	1. Сообщения об ошибках	
	1.1. Сообщения об ошибках на СА	
«Не удалось выполнить генерацию ключевой информации для СНСА»	Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить дублирование СНСА»	Неверно введен PIN-код флешки СА Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить регистрацию СН»	Неверно введен PIN-код флешки СА Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить отмену регистрации СН»	Неверно введен PIN-код флешки СА Неверно введен код регистрации СН Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА и код регистрации «Секрета» введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить смену PIN-кода СН»	Неверно введен PIN-код флешки СА Неверно введен PIN-код «Секрета» Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА и PIN-код «Секрета» введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить разблокирование СН»	Неверно введен PIN-код флешки СА Неверно введен код регистрации СН Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА и код регистрации «Секрета» введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить смену PIN-кода СНСА»	Неверно введен PIN-код флешки СА Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки

Описание неполадки	Возможные причины возникновения неполадки	Порядок действий по устранению
«Не удалось выполнить разблокирование CHCA»	Неверно введен код регистрации флешки СА Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если код регистрации флешки СА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить чтение ключевой информации CHCA»	Неверно введен PIN-код флешки СА Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить подготовку к повторной регистрации СН»	Неверно введен PIN-код флешки СА Неверно введен код регистрации «Секрета» Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА и код регистрации «Секрета» введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить повторную регистрацию СН»	Неверно введен PIN-код флешки СА Неверно введен код регистрации СН Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код флешки СА и код регистрации «Секрета» введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить подготовку к повторной регистрации СН. Не удалось сохранить подготовленный мандат в указанном каталоге»	Возникла ошибка при записи мандата в файл (например, если нет достаточного места на диске, недостаточно прав для выполнения операции и т.п. системные проблемы)	Найти причину возникновения ошибки при записи мандата в файл и повторить операцию
«Не удалось выполнить повторную регистрацию СН. Не удалось прочитать мандат из указанного файла»	Возникла ошибка чтения мандата из файла (например, файл меньшей длины, недостаточно прав для выполнения операции и т.п. системные проблемы)	Найти причину возникновения ошибки чтения мандата из файла и повторить операцию
1.2. Сообщения об ошибках на компьютерах		
«Не удалось выполнить аутентификацию Секрета [Имя: %1]»	Неверно введен PIN-код «Секрета» Неисправность устройства Программная ошибка в процессе выполнения операции	Повторить операцию. В случае если PIN-код «Секрета» введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить подключение к Серверу Аутентификации»	Может возникнуть при физической невозможности установить соединение с СА в рамках отведенного времени	1) Проверить, запущен ли СА (компьютер, на котором установлено ПО СА). 2) Проверить наличие сетевого соединения между

Описание неполадки	Возможные причины возникновения неполадки	Порядок действий по устранению
«Соединение с Сервером Аутентификации прервано»	Истекло установленное время ожидания ответа от СА	компьютером и СА. Повторить операцию
«Доступ к Секрету на данном компьютере запрещен»	Хост, с которого выполняется доступ к «Секрету», находится в черном списке на СА Хост, с которого выполняется доступ к Секрету, отсутствует в белом списке на СА	Удалить данный хост из черного списка на СА Добавить данный хост в белый список на СА
«Сервер Аутентификации в данное время не готов к приему данных»	На СА не выполнена процедура загрузки КИ флешки СА флешка СА отключена от СА Закрыто приложение «АРМ Администратора»	Выполнить загрузку КИ флешки СА в СА 1) Выполнить подключение флешки СА к СА. 2) Выполнить загрузку КИ флешки СА в СА. 1) Запустить приложение «АРМ Администратора». 2) Выполнить загрузку КИ флешки СА в СА.
«Секрет не зарегистрирован на Сервере Аутентификации»	Данный «Секрет» отсутствует в базе зарегистрированных	Зарегистрировать «Секрет» на данном СА
«Прервана передача данных на Сервер Аутентификации»	Соединение было разорвано	Устранить причину разрыва соединения
«Невозможно выполнить доступ к Секрету. Служба доступа к Серверу Аутентификации не установлена»	Некорректно установлено ПО РС (ПО компьютера)	Выполнить переустановку ПО РС (ПО компьютера)
«Невозможно выполнить доступ к Секрету. Служба доступа к Серверу Аутентификации не запускается»	Некорректно установлено ПО РС (ПО компьютера)	Выполнить переустановку ПО РС (ПО компьютера)
2. Прочие неполадки		
Приложение «АРМ Администратора» не отвечает	Данная неполадка может возникать при работе в ОС Windows 7 без установленного обновления SP1.	Проверить наличие установленного обновления SP1 для ОС Windows 7. В случае отсутствия обновления SP1 установить его.