ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс защищенного хранения информации «Секрет Фирмы»

Руководство администратора

11443195.4012.032-90

Листов 75

Москва
2012

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса «Секрет Фирмы» (далее по тексту – ПАК «Секрет Фирмы», либо «Секрет Фирмы»), предназначенного для защищенного хранения данных на отчуждаемом USB-носителе и предоставляющего возможность применения этого носителя исключительно в выделенных сегментах сети, разрешенных владельцем.

ПАК «Секрет Фирмы» предназначен для корпоративного использования. В этом случае непосредственный пользователь специального носителя «Секрет Фирмы» является исключительно оператором «Секрета». Функции администратора ПАК «Секрет» должны выполняться специально назначенным должностным лицом, имеющим необходимые знания и полномочия.

В документе приведены основные функции, особенности установки и эксплуатации ПАК «Секрет Фирмы».

Перед установкой и эксплуатацией ПАК «Секрет Фирмы» рекомендуется внимательно ознакомиться с настоящим руководством.

Применение ПАК «Секрет Фирмы» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ (PC).

СОДЕРЖАНИЕ

АННОТАЦИЯ **2**
1 Общие сведения **5**
1.1 Состав ПАК «Секрет Фирмы» 5
1.1.1 Аппаратные средства 5
1.1.2 Программные средства 5
1.2 Назначение ПАК «Секрет Фирмы» 6
1.3 Технические условия применения комплекса 6
2 Установка и настройка ПАК «Секрет Фирмы» **7**
2.1 Установка ПО ПАК «Секрет Фирмы» 7
2.1.1 Установка ПО Сервера Аутентификации 7
2.1.2 Установка ПО Рабочей станции 13
2.2 Подключение СН и СНСА 17
2.3 Установка системного драйвера СН и СНСА 17
2.4 Порядок работы 21
3 Управление ПАК «Секрет Фирмы» **23**
3.1 Создание эталонного СНСА 23
3.2 Дублирование СНСА 26
3.3 Регистрация СН 30
3.4 Подготовка СН к работе 35
3.4.1 Настройка списков доступа 36
3.4.2 Настройка сетевых параметров 38
3.5 Загрузка ключевой информации СНСА в сервис СА 38
3.6 Регистрация СН в другом сегменте сети 40
3.6.1 Подготовка СН к процедуре повторной регистрации 40
3.6.2 Повторная регистрация СН 43
3.7 Отмена регистрации СН 47
3.8 Смена PIN-кода СНСА 50
3.9 Смена PIN-кода СН 52
3.10 Разблокирование СН 56
3.11 Разблокирование СНСА 60
4 Журнал регистрации событий **63**
5 Рекомендации по организации безопасного применения ПАК «Секрет Фирмы» **69**
5.1 Общие сведения 69
5.2 Установка входа пользователя в систему с обязательным вводом пароля 69
5.3 Включение режима автоматической блокировки экрана 70

6 Перечень принятых сокращений и обозначений 72
7 Методы устранения неполадок в работе ПАК «Секрет Фирмы» 72

1 Общие сведения

1.1 Состав ПАК «Секрет Фирмы»

ПАК «Секрет Фирмы» представляет собой комплекс программных и аппаратных средств, который предназначен для применения на ПЭВМ типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP/Vista/7 SP1 (x32 или x64), с целью обеспечения защищенного хранения данных на отчуждаемом USB-носителе и предоставления возможности применения этого носителя исключительно в выделенных сегментах сети, разрешенных владельцем.

ПАК «Секрет Фирмы» состоит из аппаратных и программных средств.

1.1.1 Аппаратные средства

Минимальный состав аппаратных средств ПАК «Секрет Фирмы»:

- специальный носитель «Секрет Фирмы» (далее – СН);
- 2 специальных носителя сервера аутентификации (СНСА) – эталонный и рабочий;
- 2 специальных носителя эмитента (СНЭ) – эталонный и рабочий.

СН представляет собой аппаратный модуль, выполненный в форм-факторе флеш-диска с интерфейсом USB, предназначенный для защищенного хранения информации пользователя.

СНСА – носитель ключевой информации сервера аутентификации.

СНЭ – носитель ключевой информации эмитента, которая позволяет различать СН, эмитированные различными организациями-эмитентами.

СНСА и СНЭ по конструкции аналогичны СН.

1.1.2 Программные средства

Программные средства ПАК «Секрет Фирмы»:

1) программное обеспечение (ПО) рабочей станции (РС) в составе:
   - драйвер USB-устройства для работы в составе операционной системы (ОС);
   - ПО сервиса РС;
   - ПО фильтра USB-носителей;
2) ПО Сервера Аутентификации (СА) в составе:
   - драйвер USB-устройства;
   - ПО сервиса СА;
   - ПО «АРМ Администратора»;
3) ПО эмиссии в составе:

- драйвер USB-устройства;
- ПО «АРМ Эмиссии».

ВНИМАНИЕ! ПО эмиссии и ПО Сервера Аутентификации поставляются в сборе, предустановленными на ПЭВМ, спецификация которых оговаривается при заказе!

ПО РС предназначено для обнаружения СН, аутентификации (опознавания) СН с участием СА, получения доступа к внутренней памяти флеш-диска со стороны РС и блокирования использования других USB-носителей информации.

ПО СА исполняется на выделенном компьютере сегмента локальной сети. Оно предназначено для выполнения операций удаленной аутентификации СН на РС и администрирования СН. В качестве носителя собственной ключевой информации ПО СА использует СНСА, аналогичный по конструкции СН.

Процедура эмиссии используется для защиты сети организации от использования СН «Секрет Фирмы» других организаций. Для этого все СН и СНСА его сети проходят процедуру эмиссии. В качестве носителя собственной ключевой информации ПО эмиссии использует СНЭ, аналогичный по конструкции СН.

1.2 Назначение ПАК «Секрет Фирмы»

«Секрет фирмы» предназначен для использования на служебных компьютерах, объединенных в корпоративную сеть.

ПАК «Секрет Фирмы» используется в целях:

1)защиты корпоративной конфиденциальной информации, находящейся на USB-носителях, от получения доступа со стороны посторонних лиц в случае кражи и потери;

2)защиты корпоративной конфиденциальной информации, находящейся на USB-носителях, от получения доступа в случае выноса за пределы организации.

1.3 Технические условия применения комплекса

К техническим и программным средствам компьютерной системы, на которой используется Секрет Фирмы, предъявляются следующие минимальные требования:

3)для рабочей станции:

- IBM PC совместимая ПЭВМ, работающая под управлением операционной системы Microsoft Windows XP/Vista/7 SP1 (x32 или x64);
- свободный разъем USB;

– объем дискового пространства для размещения программного обеспечения на жестком диске ПЭВМ – примерно 20 Мбайт;

– связь с сервером аутентификации с использованием протоколов TCP/IP;

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

– IBM PC совместимая ПЭВМ, работающая под управлением операционной системы 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;

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

– IBM PC совместимая ПЭВМ, работающая под управлением операционной системы 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.

ВНИМАНИЕ! Для подключения к ПЭВМ двух или более специальных носителей (СН, СНСА, СНЭ) может использоваться USB-хаб. В этом случае USB-хаб должен быть оснащен собственным источником питания.

2 Установка и настройка ПАК «Секрет Фирмы»

2.1 Установка ПО ПАК «Секрет Фирмы»

До начала использования ПАК «Секрет Фирмы» на жесткие диски СА и РС следует установить комплект необходимого программного обеспечения: ПО Сервера Аутентификации «АРМ Администратора» и ПО Рабочей станции «Секретный Агент» соответственно.

ВНИМАНИЕ! Если у Вас установлено ПО ПАК «Секрет Фирмы» предыдущей версии, то перед установкой нового ПО обязательно выполните удаление ПО старой версии и перезагрузите компьютер!

2.1.1 Установка ПО Сервера Аутентификации

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

Для управления ПАК «Секрет Фирмы» необходимо установить на жесткий диск сервера аутентификации ПО сервера аутентификации.

Для этого следует запустить с прилагаемого CD исполняемый файл SetupSecretBusinessServer_v1.0.exe[1]. В настоящий момент поддерживается вариант установки (и дальнейшей работы всех программных компонентов) на русском языке. После запуска исполняемого файла выполняется процедура подготовки к установке и на экран выводится стартовое окно с общей информацией (рисунок 1).

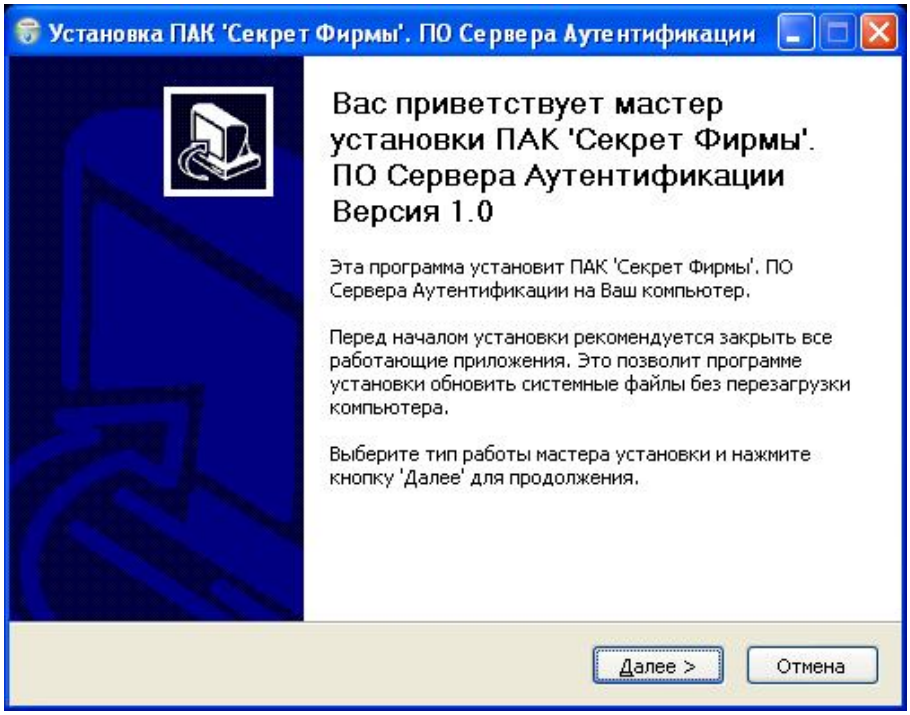

Рисунок 1 - Стартовое окно процедуры установки ПО СА

Для продолжения процедуры необходимо нажать кнопку <Далее>. Для прекращения процесса установки следует нажать кнопку <Отмена>.

В следующем окне следует выбрать компоненты ПО, которые необходимо установить (рисунок 2).

[1)] Для ОС x64 исполняемый файл имеет название SetupSecretBusinessServer_v1.0_x64.exe

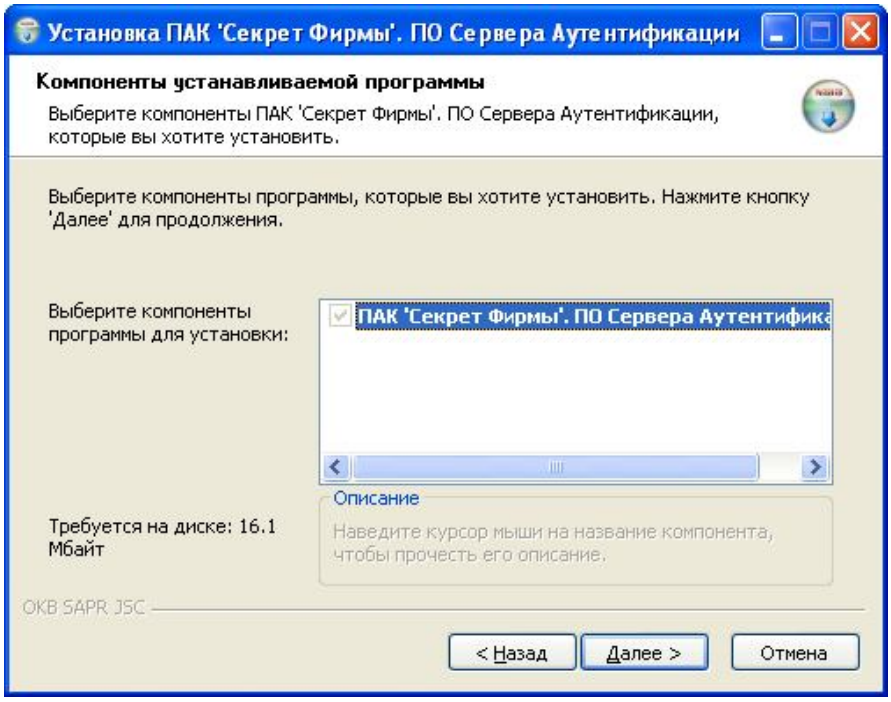

Рисунок 2 – Окно выбора компонентов устанавливаемого ПО СА

В следующем окне необходимо указать путь к каталогу установки (рисунок 3). По умолчанию установка всех программных компонентов выполняется в каталог \Program Files\OKB SAPR JSC\Secret\Business\Server. Каталог, предлагаемый по умолчанию, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <Обзор…>. Если указанный каталог не существует, он будет создан программой установки автоматически.

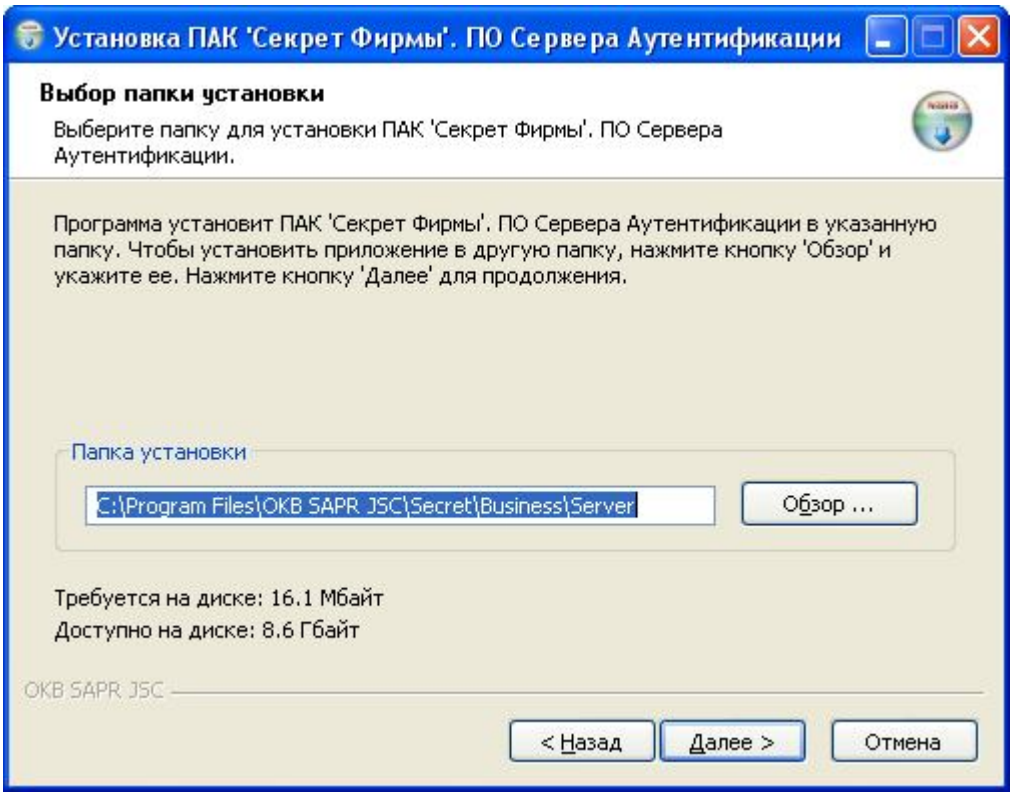

Рисунок 3 - Выбор каталога установки ПО СА

После выбора каталога установки следует нажать кнопку <Далее>, в появившемся далее окне выбрать место размещения ярлыков программы в меню «Пуск» (папка, предлагаемая по умолчанию, может быть изменена посредством ручного редактирования) и нажать кнопку <Установить>. Далее начинается процесс копирования файлов на жесткий диск (рисунок 4). В число устанавливаемых компонентов ПО сервера аутентификации входят: драйвер USB-устройств, ПО «АРМ Администратора», сервер аутентификации (служба Windows).

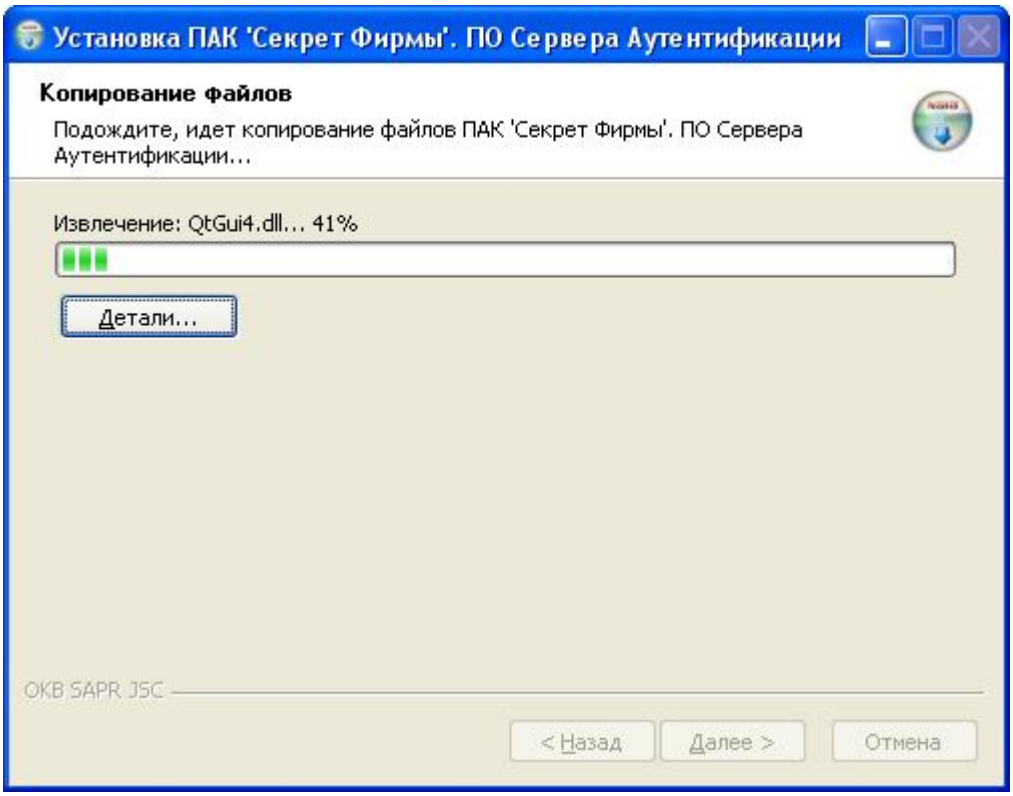

Рисунок 4 - Установка программных компонентов ПО СА

При установке программных компонентов ПО сервера аутентификации может выводиться сообщение об отсутствии теста на совместимость с ОС (рисунок 5). Необходимо выбрать пункт <Все равно продолжить>.

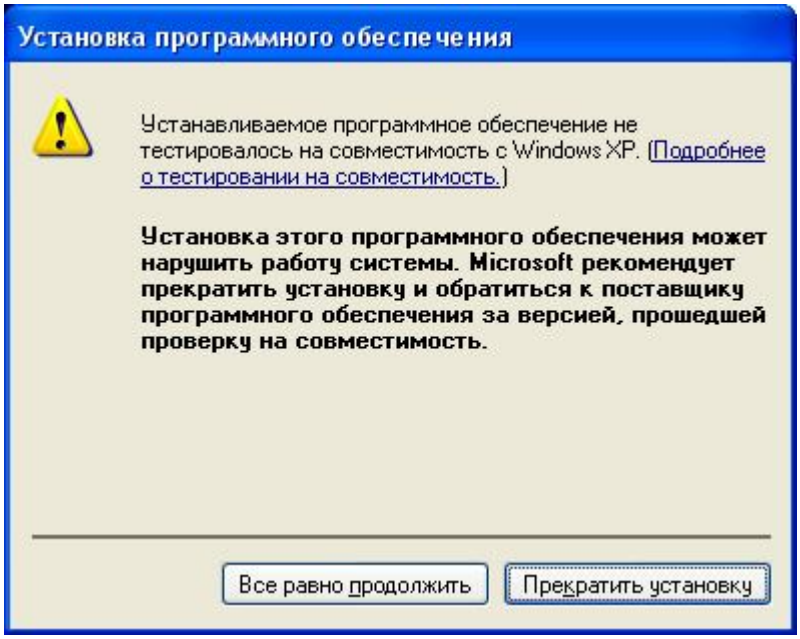

Рисунок 5 - Предупреждающее сообщение

По завершении процесса копирования файлов на экран выводится сообщение об окончании процесса установки (рисунок 6). Выход из программы установки выполняется по нажатии кнопки <Готово>.

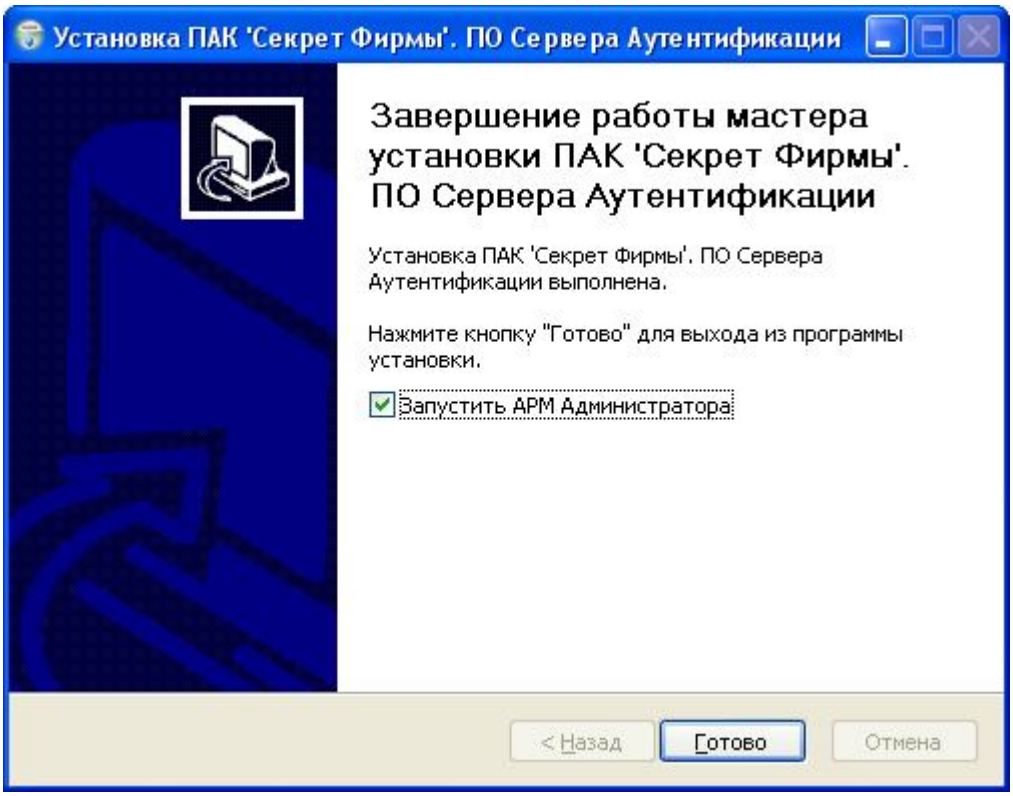

Рисунок 6 - Окно завершения установки ПО СА

После успешного завершения процесса установки можно начать администрирование «Секрета».

ВНИМАНИЕ! Для работы с ПО сервера аутентификации ПАК «Секрет Фирмы» на СА должна быть установлена плата «Аккорд»[1]. Это позволит защитить сеть от несанкционированного доступа.

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 предупреждающее сообщение (рисунок 7).

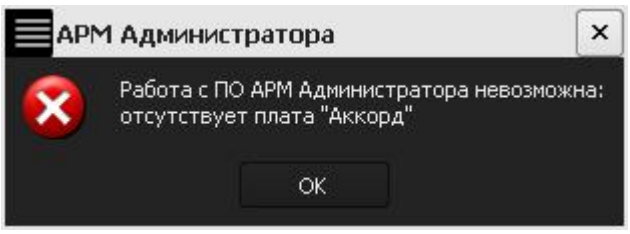

Рисунок 7 – Предупреждающее сообщение

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

2.1.2 Установка ПО Рабочей станции

До начала использования СН на жесткий диск РС должно быть установлено ПО рабочей станции. Для этого следует запустить с прилагаемого CD исполняемый файл SetupSecretBusinessWorkStation__v1.0.exe[1] . В настоящий момент поддерживается вариант установки (и дальнейшей работы всех программных компонентов) на русском языке. После запуска исполняемого файла выполняется процедура подготовки к установке и на экран выводится стартовое окно с общей информацией (рисунок 8).

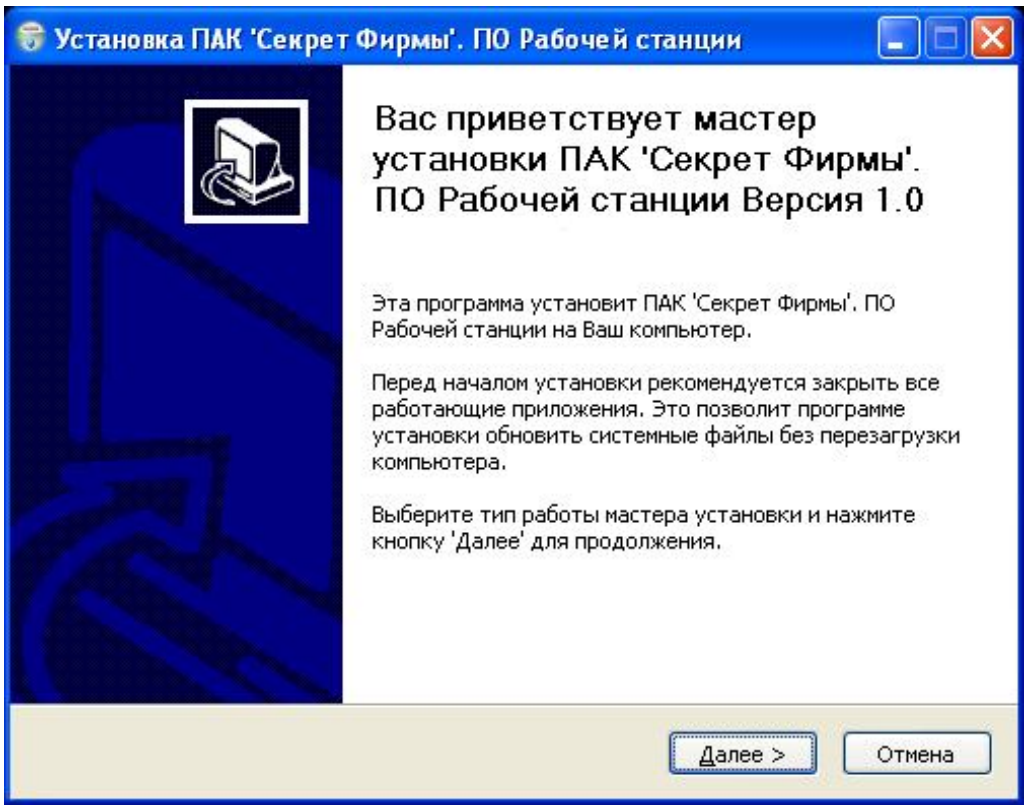

Рисунок 8 – Стартовое окно процедуры установки ПО РС

Для продолжения процедуры необходимо нажать кнопку <Далее>. Для прекращения процесса установки следует нажать кнопку <Отмена>.

В следующем окне следует выбрать компоненты ПО, которые необходимо установить (рисунок 9). При желании можно установить Фильтр USB-устройств, который запретит на данной РС использование сторонних USB-устройств, кроме устройств ПАК «Секрет Фирмы».

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

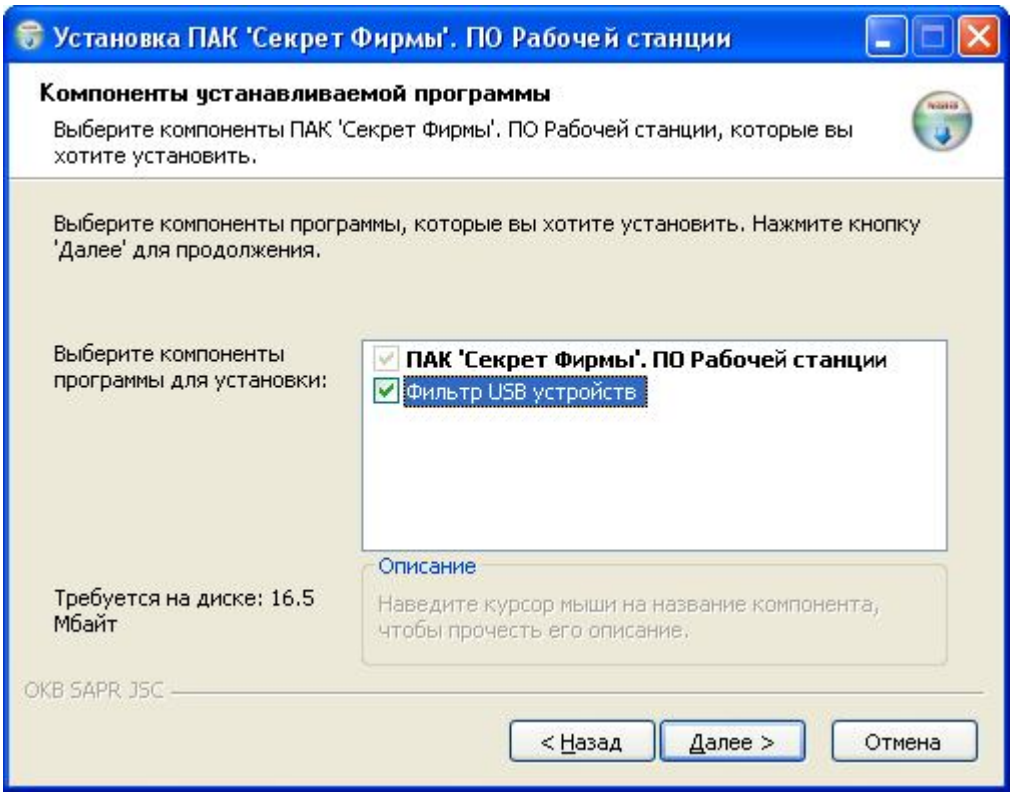

Рисунок 9 – Окно выбора компонентов устанавливаемого ПО РС

В следующем окне необходимо указать путь к каталогу установки (рисунок 10). По умолчанию установка всех программных компонентов выполняется в каталог \Program Files\OKB SAPR JSC\Secret\Business\WorkStation. Каталог, предлагаемый по умолчанию, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <Обзор…>. Если указанный каталог не существует, он будет создан программой установки автоматически.

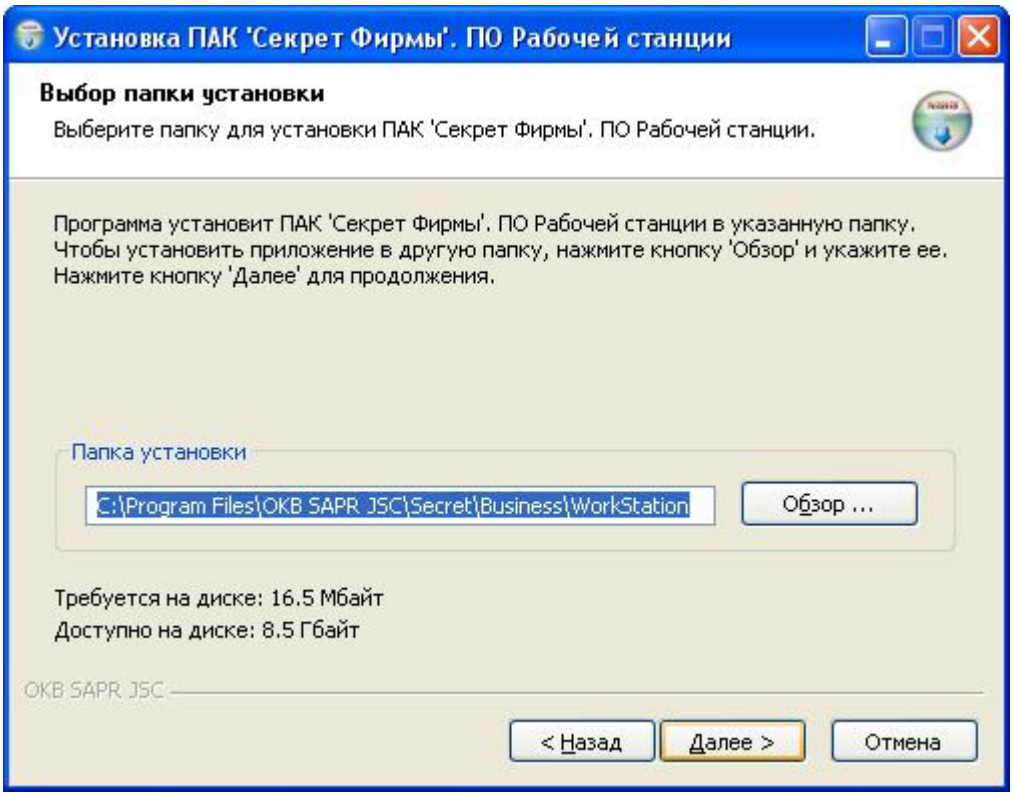

Рисунок 10 - Выбор каталога установки ПО РС

После выбора каталога установки следует нажать кнопку <Далее>, в появившемся далее окне выбрать место размещения ярлыков программы в меню «Пуск» (папка, предлагаемая по умолчанию, может быть изменена посредством ручного редактирования) и нажать кнопку <Установить>. Далее начинается процесс копирования файлов на жесткий диск (рисунок 11). В число устанавливаемых компонентов ПО рабочей станции входят: драйвер USB-устройств, драйвер-фильтр USB-устройств, ПО «Секретный Агент», вспомогательный сервис.

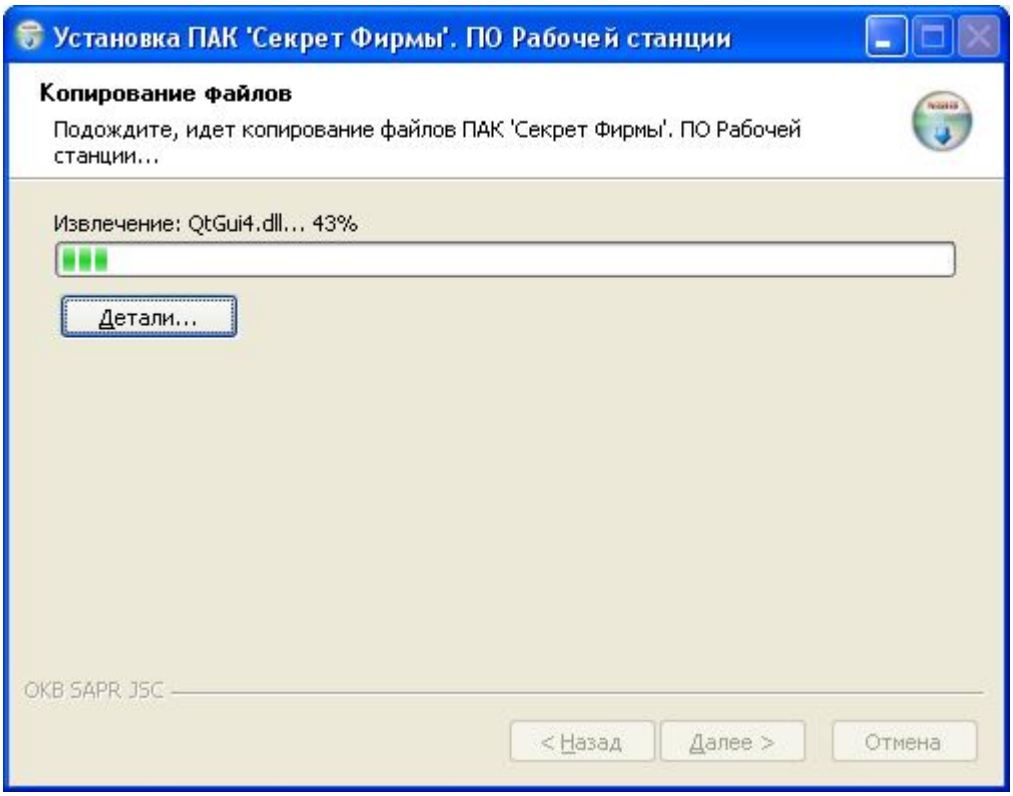

Рисунок 11 - Установка программных компонентов ПО РС

При установке программных компонентов ПО «Секретный Агент» может выводиться сообщение об отсутствии теста на совместимость с ОС (рисунок 12). Необходимо выбрать пункт <Все равно продолжить>.

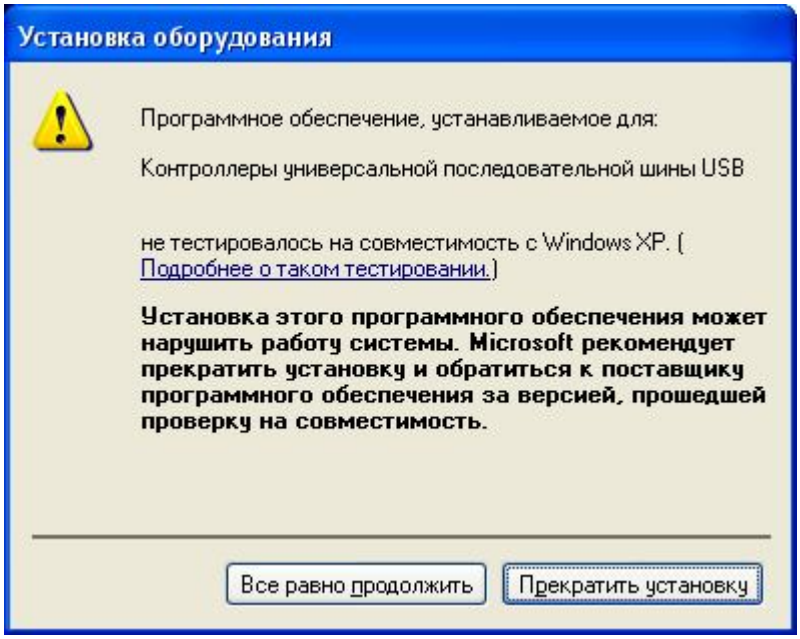

Рисунок 12 - Предупреждающее сообщение

По завершении процесса копирования файлов на экран выводится сообщение об окончании процесса установки (рисунок 13). Выход из программы установки выполняется по нажатии кнопки <Готово>.

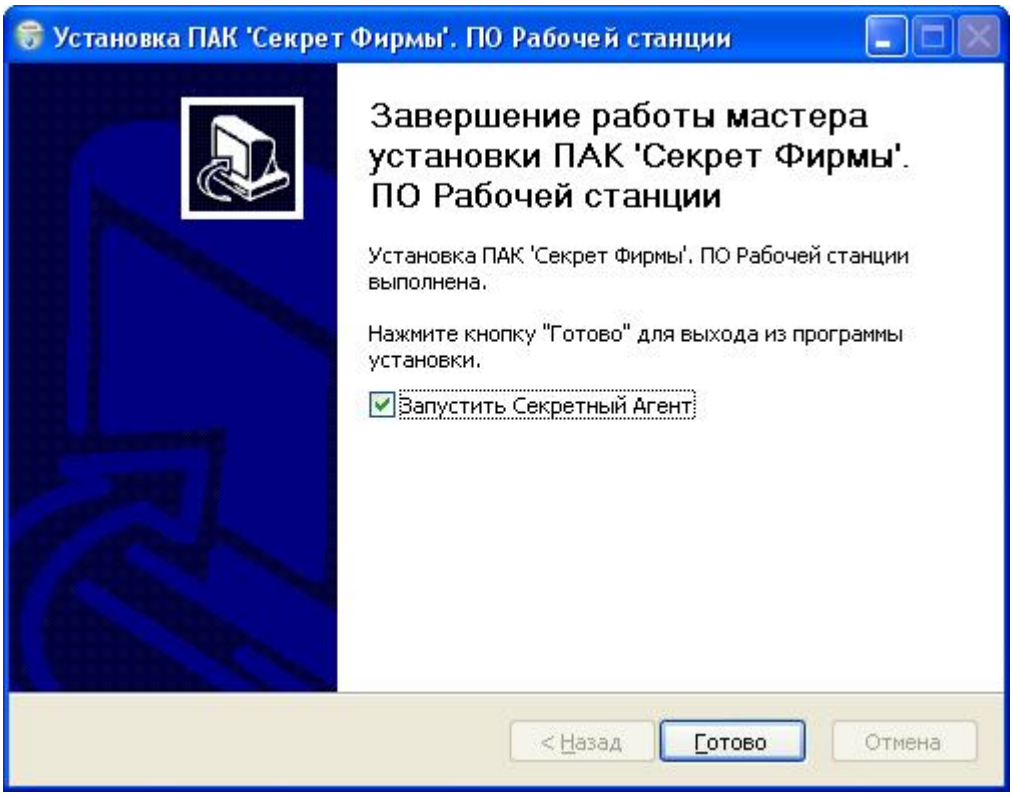

Рисунок 13 - Окно завершения установки ПО РС

После успешного завершения процесса установки можно начать применение «Секрета».

2.2 Подключение СН и СНСА

Подключение осуществляется установкой СН и СНСА в свободные USB-разъемы системного блока РС и СА[1].

2.3 Установка системного драйвера СН и СНСА

ВНИМАНИЕ! Для корректной установки драйвера необходимо идентифицироваться в системе в качестве пользователя с правами администратора.

После установки на жесткий диск ПО ПАК «Секрет Фирмы» (см. раздел 2.1) при первом подключении устройства «Секрет Фирмы» к USB-порту операционная система обнаруживает новое устройство (рисунок 14).

[1] В случае неудобного расположения USB-порта на системном блоке компьютера рекомендуется использовать удлинительный кабель USB, это предохранит «Секрет» (а также и все другие применяемые USB-устройства) от поломок и облегчит его подключение и отключение.

Рисунок 14 – Оповещение об обнаружении СН

Далее происходит автоматический запуск системной программы «Мастер нового оборудования»[1]. 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>.

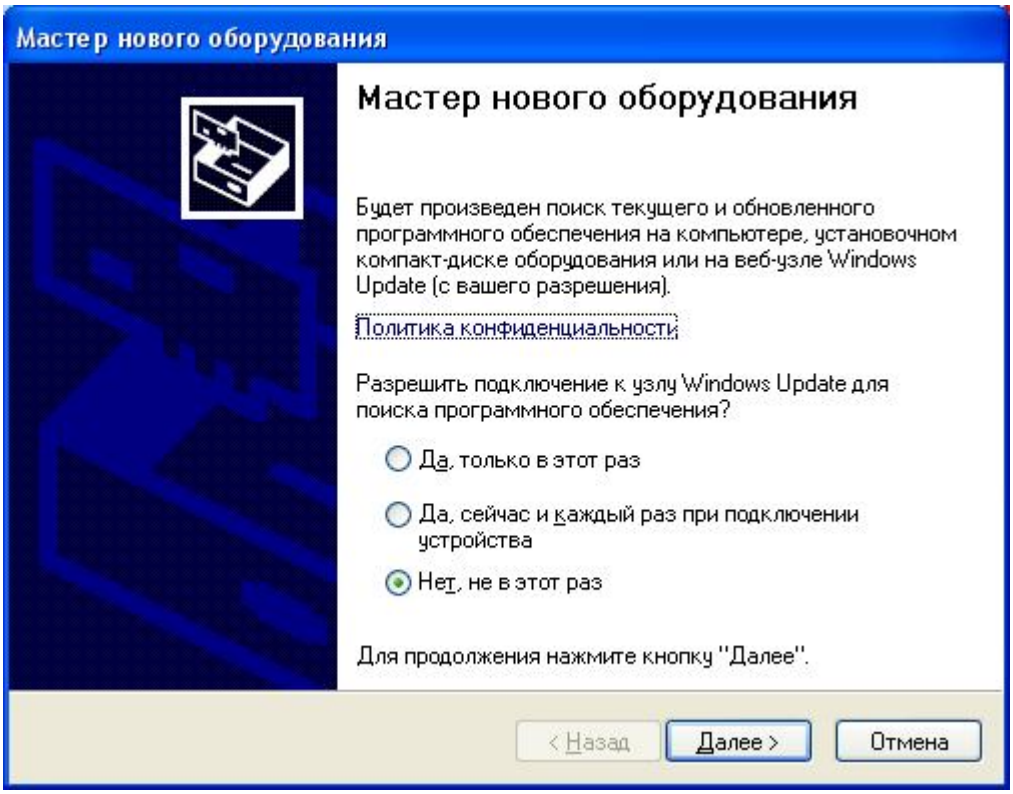

Рисунок 15 - Окно поиска текущего и обновленного ПО

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

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

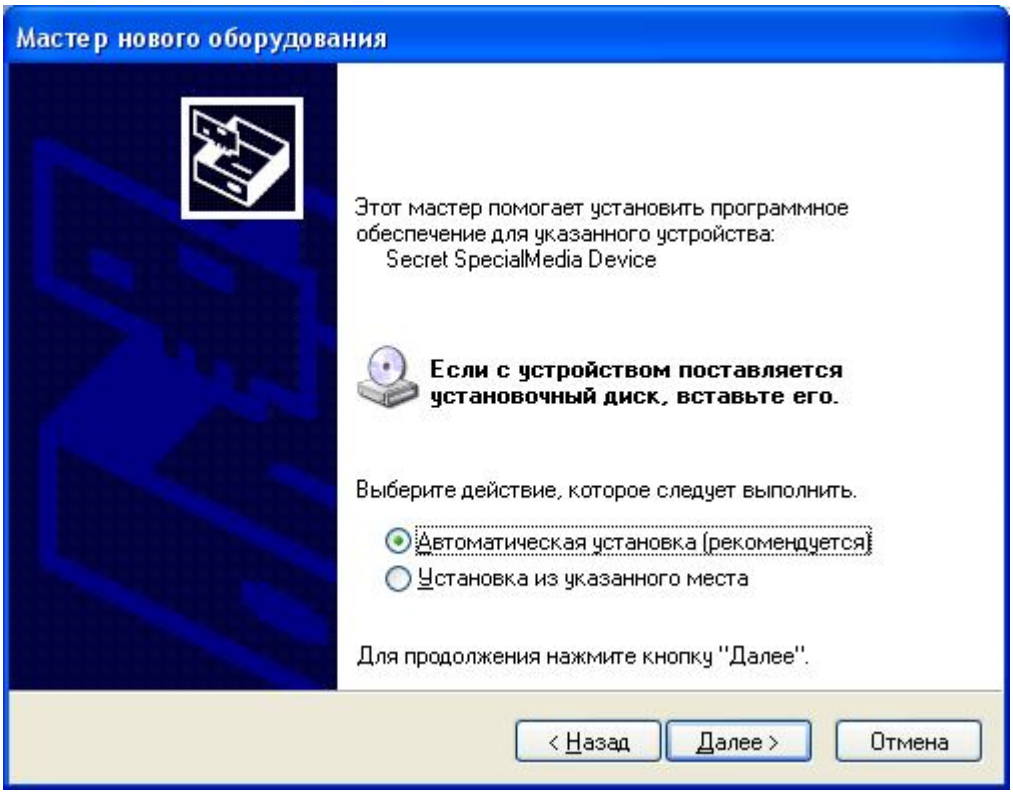

Рисунок 16 – Окно установки нового оборудования

После этого начинается процесс установки драйвера СН (рисунок 17).

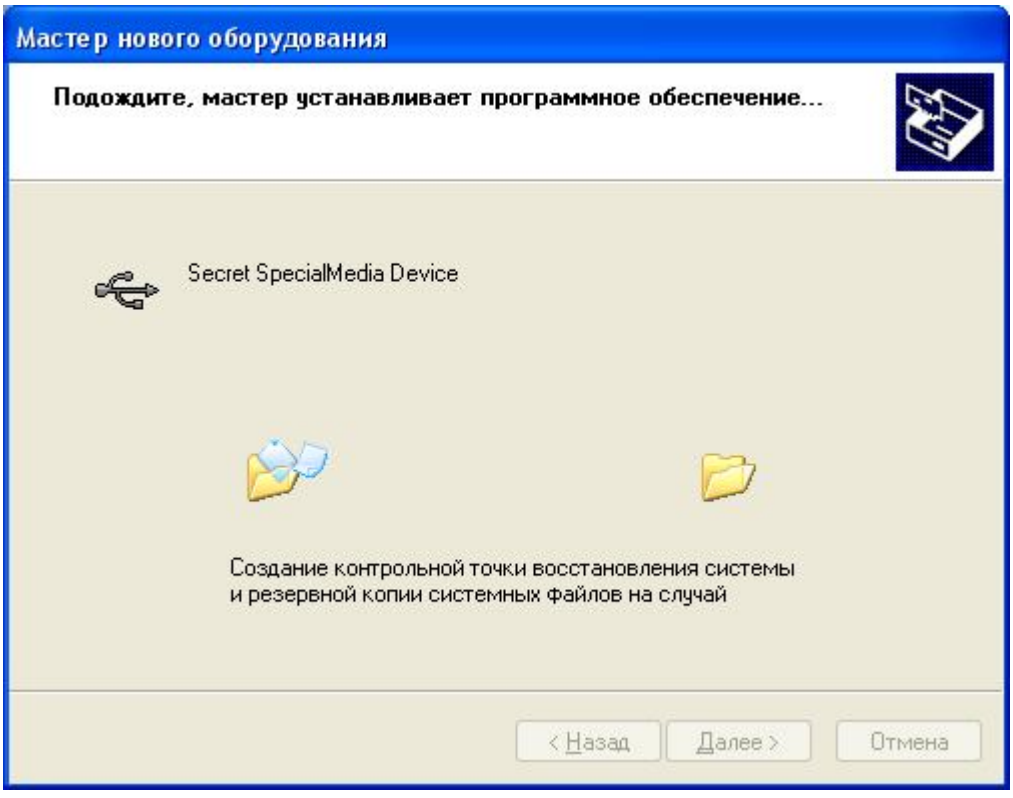

Рисунок 17 – Установка драйвера СН

При установке драйвера выводится сообщение об отсутствии теста на совместимость с ОС (рисунок 18). Необходимо выбрать пункт <Все равно продолжить>.

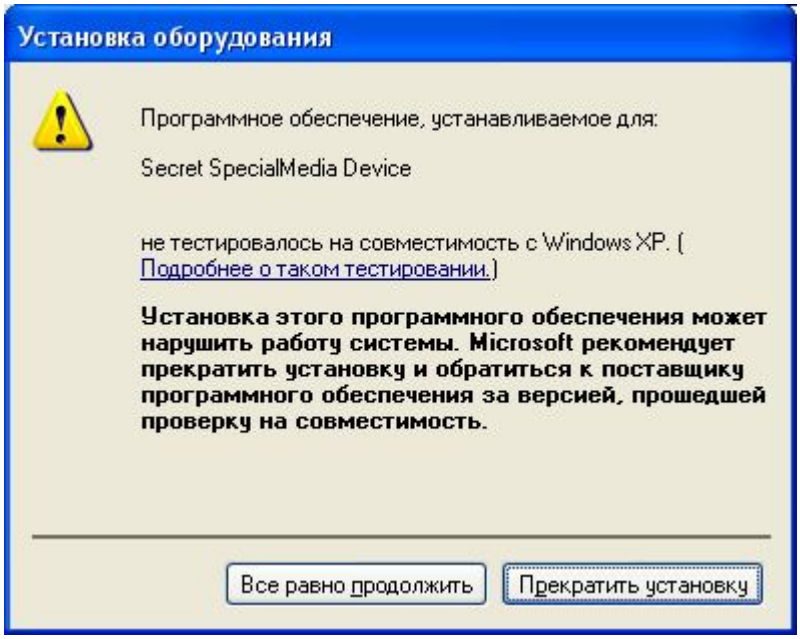

Рисунок 18 – Предупреждающее сообщение

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

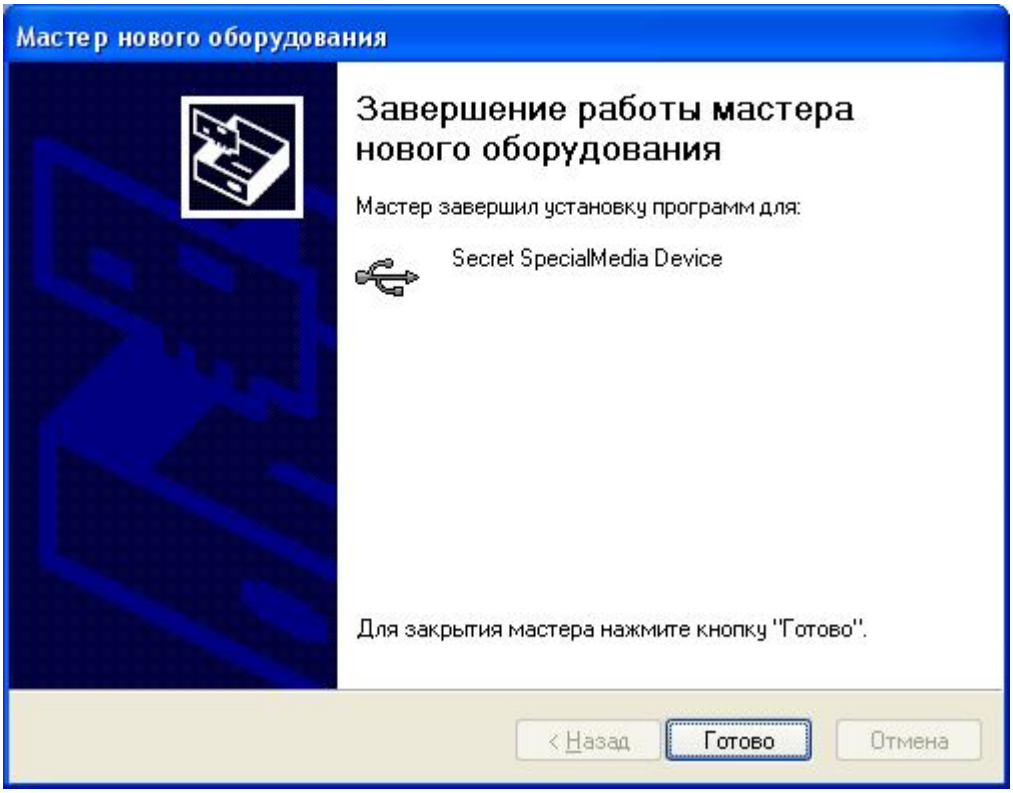

Рисунок 19 – Окно завершения работы Мастера нового оборудования

По нажатии кнопки <Готово> выполняется выход из программы установки драйвера СН.

Процедура установки драйвера СНСА аналогична процедуре, описанной выше.

2.4 Порядок работы

До начала использования «Секрета» на РС должно быть установлено ПО ПАК «Секрет Фирмы» (см. подраздел 2.1), выполнено подключение СН и СНСА (см. подраздел 2.2) и произведена установка системного драйвера СН и СНСА (см. подраздел 2.3).

При первом использовании ПАК «Секрет Фирмы» администратору необходимо создать эталонный СНСА (см. 3.1), который в дальнейшем используется исключительно для выполнения операции дублирования СНСА.

После создания эталонного СНСА необходимо путем операции дублирования создать рабочий СНСА (см. 3.2), помощью которого выполняются все действия, связанные с работой ПАК «Секрет Фирмы».

В результате выполнения процедур создания эталонного и рабочего СНСА формируются PIN–коды и коды регистрации эталонного и рабочего СНСА.

ВНИМАНИЕ! PIN-код эталонного СНСА необходим для выполнения следующих функций:

- дублирование СНСА;
- смена PIN-кода эталонного СНСА.

При утере PIN-кода эталонного СНСА выполнение этих функций становится невозможным!

PIN-код рабочего СНСА необходим для выполнения следующих функций:

- регистрация СН;
- подготовка СН к работе;
- смена PIN-кода СН, СНСА;
- подготовка СН к повторной регистрации;
- повторная регистрация СН;
- отмена регистрации СН;
- разблокирование СН.

При утере PIN-кода рабочего СНСА выполнение этих функций становится невозможным!

При утере кода регистрации эталонного (рабочего) СНСА становится невозможной процедура разблокирования эталонного (рабочего) СНСА.

При утере или выходе из строя рабочего СНСА можно создать новый рабочий СНСА с помощью дублирования эталонного. При этом рабочий СНСА не может использоваться для дублирования.

ВНИМАНИЕ! Эталонный СНСА необходимо надежно сохранить в сейфе организации во избежание кражи или потери. При утрате эталонного СНСА создание новых рабочих СНСА станет невозможным!

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

PIN-код в дальнейшем потребуется каждый раз перед монтированием СН на РС, то есть для того, чтобы «Секрет» был обнаружен в операционной системе как устройство mass-storage.

ВНИМАНИЕ! При утере PIN-кода СН становится невозможным выполнение следующих функций:

- получение доступа к СН;
- смена PIN-кода СН.

Код регистрации СН необходим для выполнения операций, связанных с управлением СН (повторная регистрация, отмена регистрации, разблокирование. Подробнее см. соответствующие подразделы раздела 3).

ВНИМАНИЕ! При утере кода регистрации СН становится невозможным выполнение следующих функций:

- подготовка СН к повторной регистрации;
- повторная регистрация СН;
- отмена регистрации СН;
- разблокирование СН.

При этом все еще сохраняется возможность получения доступа к СН на тех РС, на которых ранее была выполнена процедура регистрации.

Пользователю следует запомнить или надежно сохранить PIN-код и код регистрации СН; администратору следует запомнить или надежно сохранить PIN-код и код регистрации СНСА. В случае необходимости (например, при компрометации PIN-кода) PIN-код может быть изменен. Для выполнения этой операции потребуется знание старого значения PIN-кода. Изменение кода регистрации «Секрета» невозможно без полного обнуления устройства, возврата его к первоначальному состоянию (то есть обнулятся все данные о регистрации СН в каких-либо сегментах сети, его PIN-коде, и доступ к записанным на нем данным станет невозможен).

После выполнения процедуры первичной регистрации «Секрета» на сервере аутентификации, СН связывается с данным сервером аутентификации, который становится для него «первичным».

После успешной регистрации «Секрета» необходимо выполнить операции по подготовке СН к работе в части настройки параметров для получения

доступа: настроить списки доступа и параметры сетевого соединения (подробнее см. 3.4).

Для того чтобы процедура получения доступа к СН (выполняемая как на сервере аутентификации, так и на рабочих станциях) стала возможной, до начала использования СН «Секрет Фирмы» администратор должен выполнить загрузку ключевой информации СНСА в сервис сервера аутентификации (подробнее об этом см. в подразделе 3.5).

ВНИМАНИЕ! Если СНСА был отключен от СА (или был выполнен выход из программы «АРМ Администратора»), то ключевая информация выгружается из сервиса СА. Поэтому, для того чтобы процедура выполнения доступа к Секрету стала возможной, ключевую информацию СНСА необходимо загружать в сервис СА после каждого подключения СНСА к серверу аутентификации или перезапуска программы «АРМ Администратора».

После выполнения всех описанных выше операций доступ к данным СН (содержимому флеш-диска) может быть получен на разрешенных РС.

ВНИМАНИЕ! Обязательным условием получения доступа к СН на РС является наличие рабочего СНСА, подключенного к серверу аутентификации выделенного сегмента сети, которому принадлежит данная РС.

Для этого следует запустить на разрешенной РС ПО «Секретный Агент», подключить СН к USB-разъему соответствующей РС и выполнить доступ к Секрету по предъявлении корректного PIN-кода (подробнее об этом см. подраздел «Получение доступа к данным СН» руководства пользователя (11443195.4012.032-34)).

3 Управление ПАК «Секрет Фирмы»

3.1 Создание эталонного СНСА

При первом использовании ПАК «Секрет Фирмы» администратору необходимо создать эталонный СН сервера аутентификации, который в дальнейшем может быть использован только для выполнения операции дублирования СНСА.

ВНИМАНИЕ! Во время выполнения операций, связанных с созданием эталонного СНСА, не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

Для создания эталонного СНСА необходимо выполнить подключение СНСА к USB-порту СА (см. 2.2) и запустить приложение «АРМ Администратора», главное окно которого показано на рисунке 20. Данное приложение может быть запущено посредством выбора пункта меню Пуск→Программы→Секрет Фирмы→Сервер Аутентификации→АРМ Администратора.

В данном окне следует выбрать вкладку «Генерация». Она содержит список подключенных эмитированных СНСА с указанием их серийного номера.

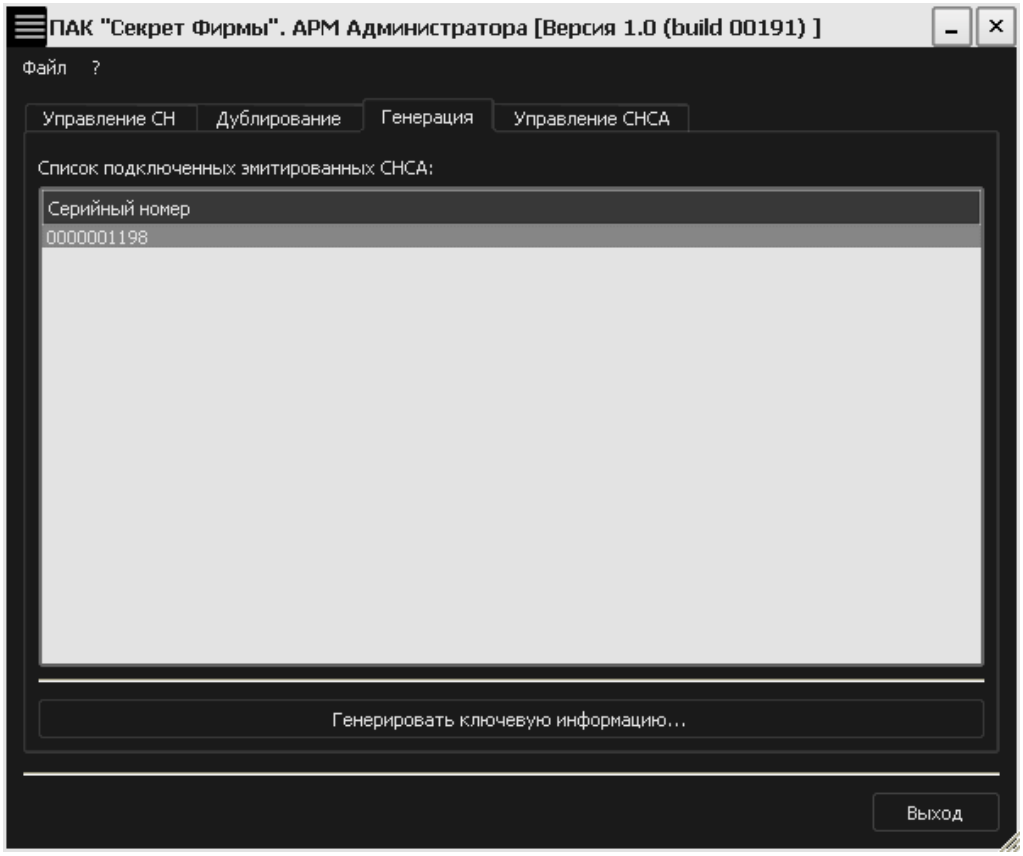

Рисунок 20 – Главное окно АРМ Администратора. Вкладка «Генерация»

В списке подключенных СНСА следует выделить нужный СНСА и нажать кнопку <Генерировать ключевую информацию…>.

В появившемся окне необходимо ввести имя регистрируемого СНСА (рисунок 21). Имя представляет собой строку, длина которой ограничена 32 произвольными символами. В качестве имени целесообразно использовать одно или несколько слов, характеризующих принадлежность СНСА к серверу аутентификации. Имя 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.

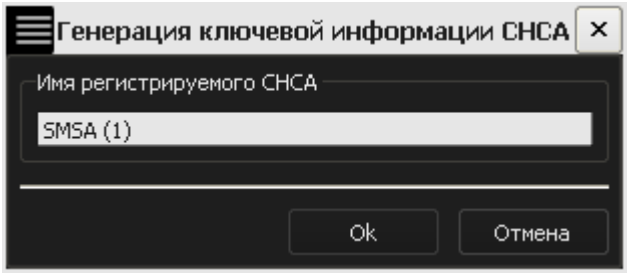

Рисунок 21 – Окно для ввода имени СНСА

После успешного выполнения процедуры генерации ключевой информации для СНСА на экране появляется следующее окно:

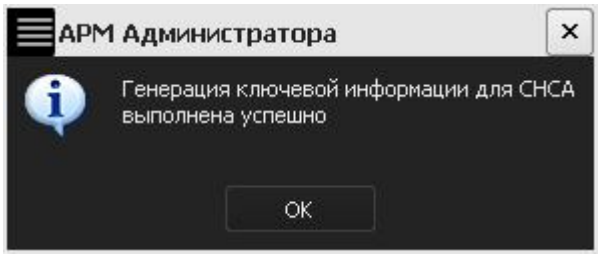

Рисунок 22 – Оповещение об успешной генерации КИ для СНСА

Затем на экран выводится окно с основной информацией о СНСА:

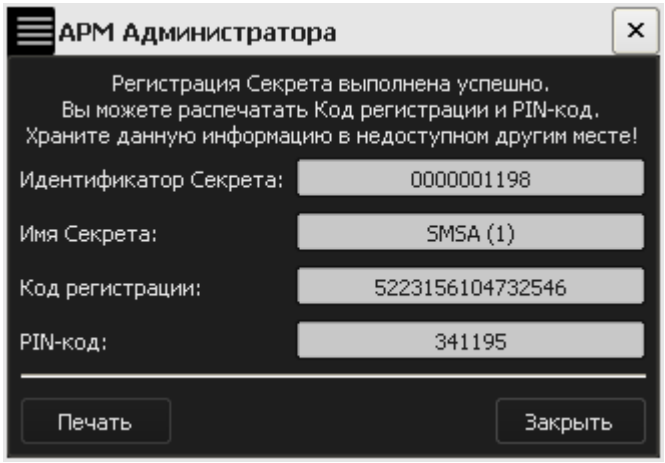

Рисунок 23 – Окно с основной ключевой информацией об СНСА

ВНИМАНИЕ! Администратор СНСА должен запомнить или надежно сохранить PIN-код и код регистрации эталонного СНСА.

Знание PIN-кода эталонного СНСА позволяет провести операцию дублирования СНСА.

Знание кода регистрации эталонного СНСА позволяет провести процедуру разблокирования эталонного СНСА.

Имеется возможность печати кода регистрации и PIN-кода эталонного СНСА (при наличии подключенного принтера).

Следует помнить о необходимости сохранения этих данных недоступными третьим лицам!

Далее следует нажать кнопку <Закрыть>. Если регистрационная информация не распечатана, то на экране появляется оповещающее окно:

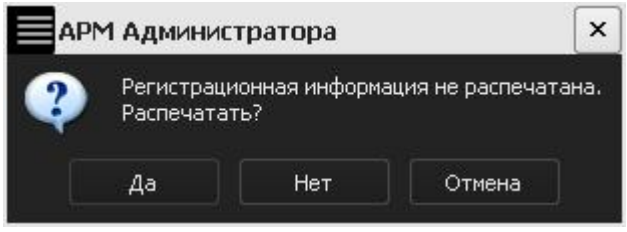

Рисунок 24 – Предупреждающее сообщение

При наличии подключенного принтера имеется возможность распечатать информацию об СНСА, нажав кнопку <Да>. В случае, если печать не требуется, следует нажать кнопку <Нет> или <Отмена>.

Далее во вкладке «Управление СНСА» появляется информация о только что зарегистрированном эталонном СНСА (рисунок 25). При этом статус зарегистрированного СНСА изменяется на «Снаряженный эталонный».

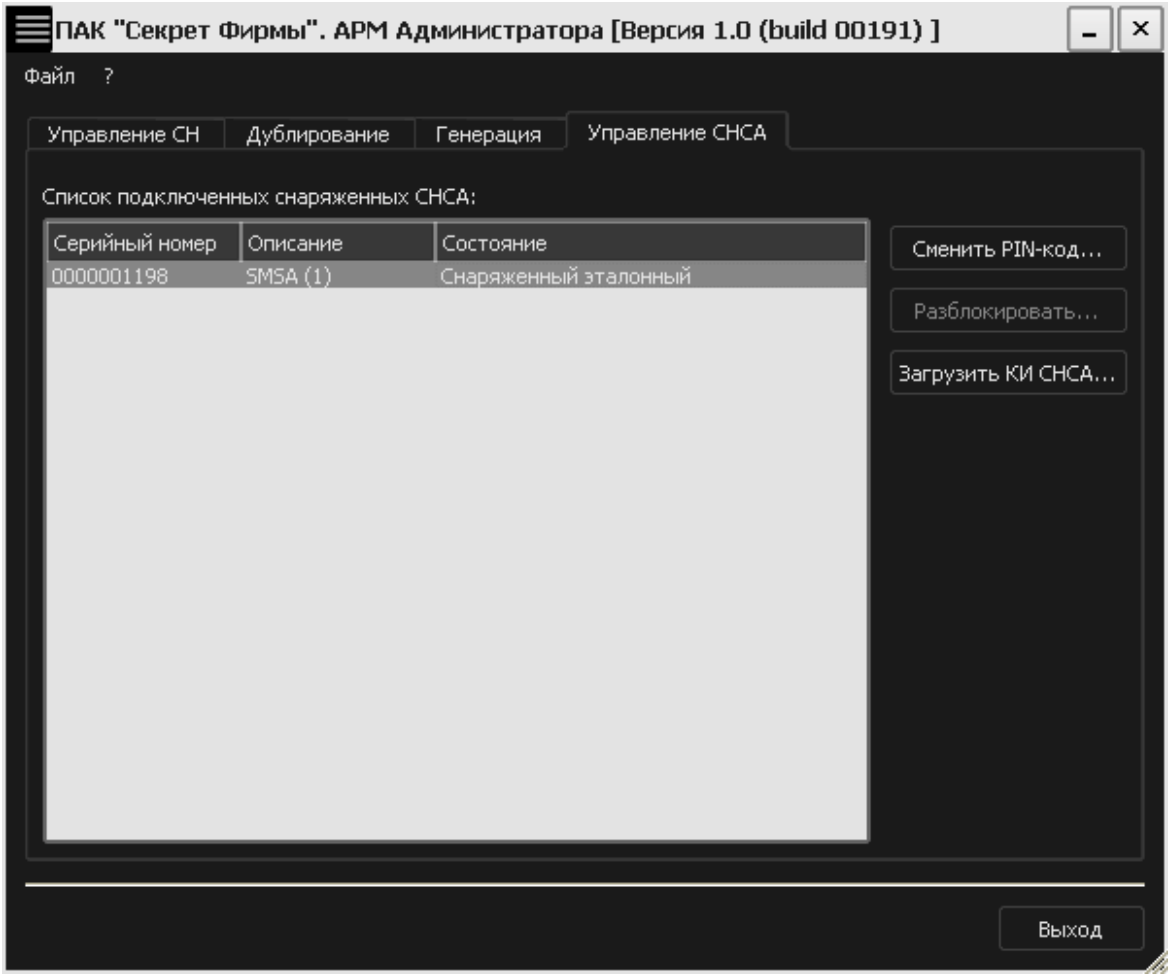

Рисунок 25 – Главное окно АРМ Администратора. Вкладка «Управление СНСА»

Для дальнейшей работы с ПАК «Секрет Фирмы» необходимо создать рабочий СНСА с помощью операции дублирования эталонного СНСА. Эталонный СНСА необходимо надежно сохранить в сейфе организации. Он должен использоваться исключительно в целях дублирования СНСА.

3.2 Дублирование СНСА

Перед выполнением регистрации СН необходимо путем дублирования эталонного СНСА создать рабочий СНСА, с помощью которого будут производиться дальнейшие действия по работе с ПАК «Секрет Фирмы».

Для этого необходимо подключить эмитированный СНСА к USB-порту сервера аутентификации. При этом эталонный СНСА должен быть подключен во второй разъем СА (также допускается использование USB-хаба с собственным источником питания, см. 1.3).

Далее следует запустить приложение АРМ Администратора и выбрать вкладку «Дублирование» (см. рисунок 26). Она содержит список подключенных эмитированных СНСА с указанием их серийного номера.

ВНИМАНИЕ! Во время выполнения операций, связанных с дублированием СНСА, не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

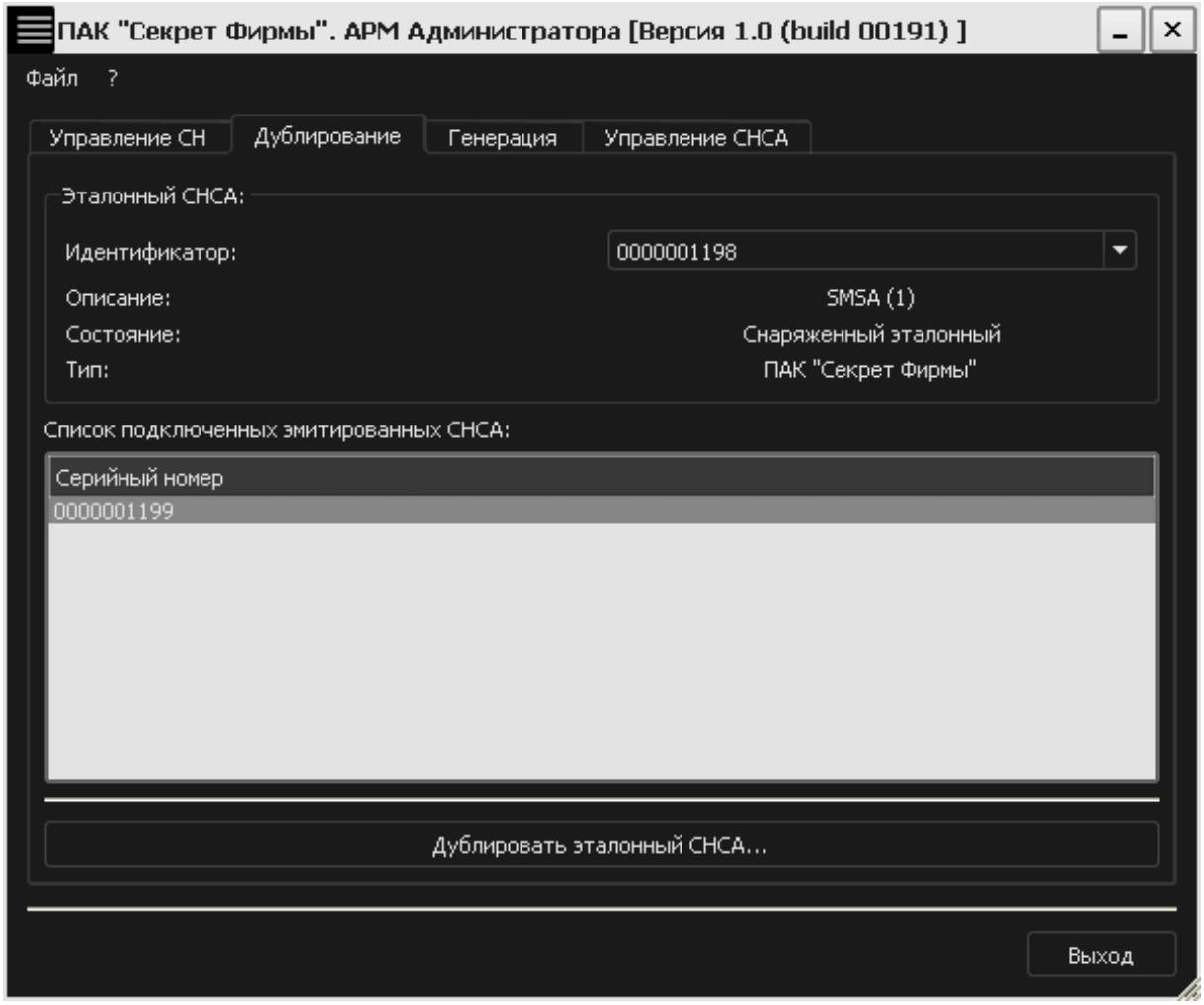

Рисунок 26 – Приложение АРМ Администратора. Вкладка «Дублирование»

В списке подключенных СНСА следует выделить нужный СНСА и нажать кнопку <Дублировать эталонный СНСА…>.

В появившемся окне необходимо ввести PIN-код эталонного СНСА, полученный при его создании (рисунок 27).

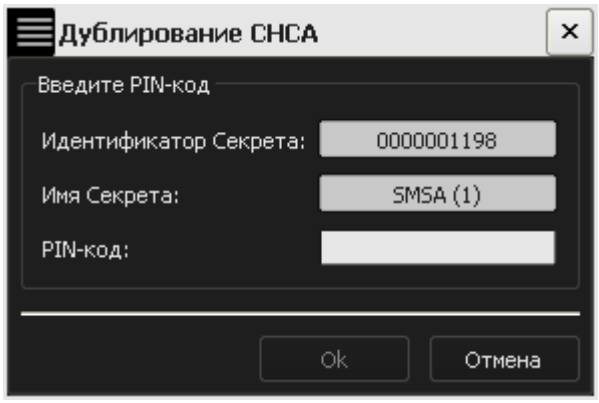

Рисунок 27 – Окно ввода PIN-кода эталонного СНСА

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

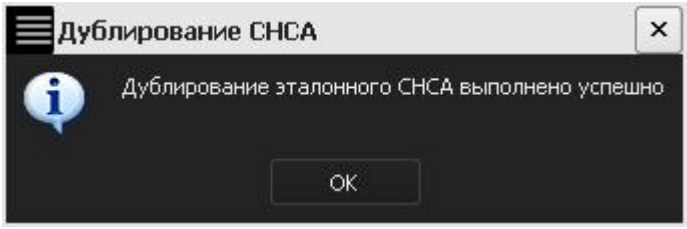

Рисунок 28 – Сообщение об успешном дублировании эталонного СНСА

Далее на экран выводится окно с основной информацией о только что созданном рабочем СНСА (рисунок 29).

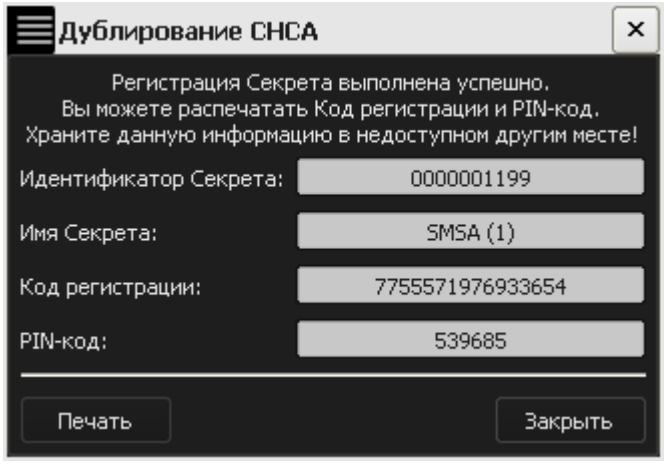

Рисунок 29 – Окно с регистрационными данными рабочего СНСА

ВНИМАНИЕ! Администратор СНСА должен запомнить или надежно сохранить PIN-код и код регистрации рабочего СНСА.

Знание PIN-кода рабочего СНСА позволяет получить доступ к следующим функциям ПАК «Секрет Фирмы»:

- регистрация СН;
- подготовка СН к возможности получения к нему доступа;
- подготовка СН к повторной регистрации;

- повторная регистрация СН;
- отмена регистрации СН;
- смена PIN-кода СНСА;
- смена PIN-кода СН;
- разблокирование СН.

Знание кода регистрации СНСА позволяет провести процедуру разблокирования СНСА.

Следует помнить о необходимости сохранения этих данных недоступными третьим лицам!

Затем следует нажать кнопку <Закрыть>. Если регистрационная информация не распечатана, то на экране появляется оповещение:

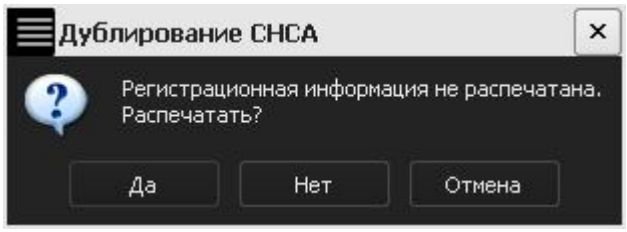

Рисунок 30 – Предупреждающее сообщение

При наличии подключенного принтера имеется возможность распечатать информацию об СНСА, нажав кнопку <Да>. В случае если печать не требуется, следует нажать кнопку <Нет> или <Отмена>.

Далее во вкладке «Управление СНСА» появляется информация о только что созданном рабочем СНСА (рисунок 31).

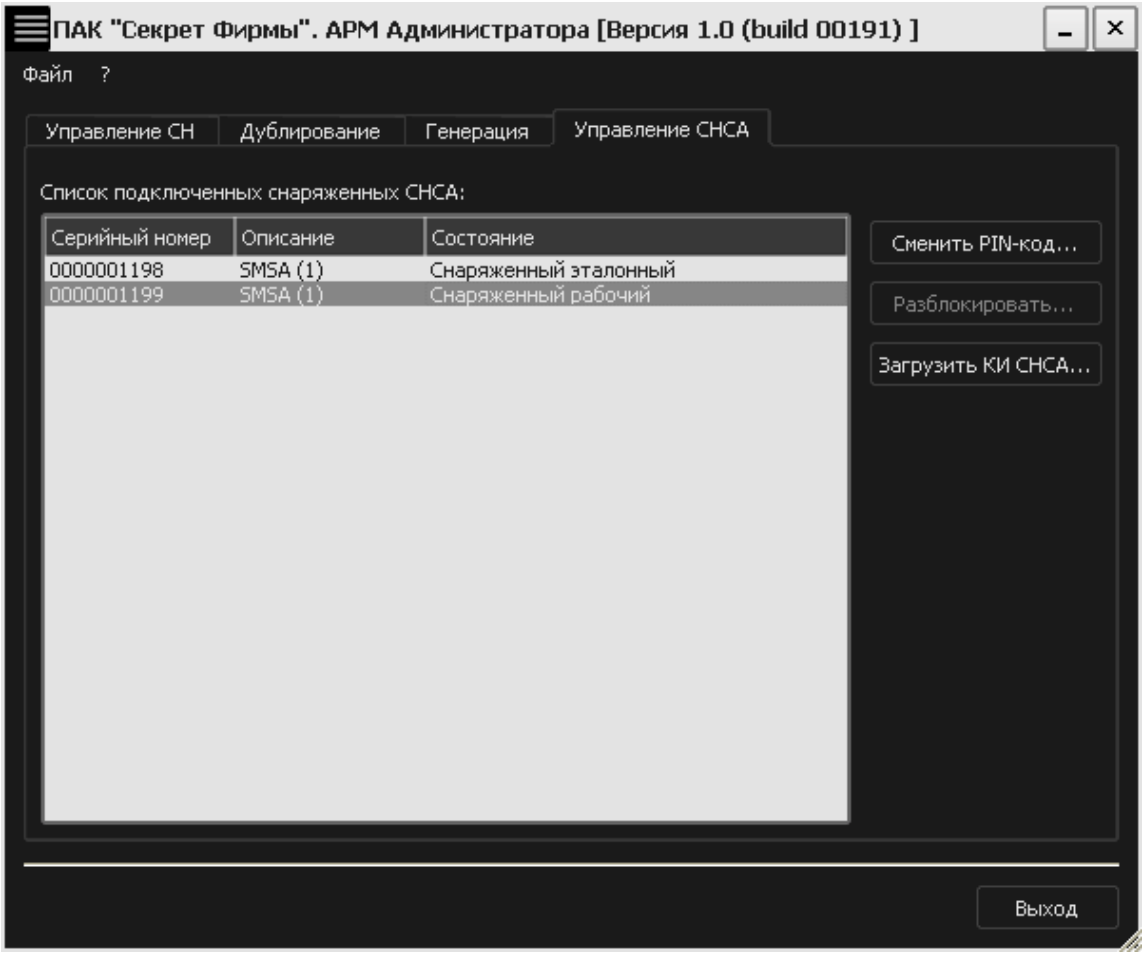

Рисунок 31 – АРМ Администратора. Вкладка «Управление СНСА»

Эталонный СНСА необходимо извлечь из USB-разъема СА и надежно сохранить в сейфе. Все дальнейшие действия, связанные с использованием ПАК «Секрет Фирмы», должны выполняться с применением только рабочего СНСА.

3.3 Регистрация СН

До начала использования СН на РС должно быть установлено ПО ПАК «Секрет Фирмы» и выполнена процедура регистрации СН. В результате выполнения процедуры регистрации СН формируются PIN–код и код регистрации СН, с использованием которых осуществляются операции получения доступа к данным в «Секрете» и администрирования СН.

ВНИМАНИЕ! Во время выполнения операции регистрации СН не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

Для выполнения регистрации необходимо выполнить подключение СН и рабочего СНСА 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 СН «Секрет» не зарегистрирован (рисунок 32).

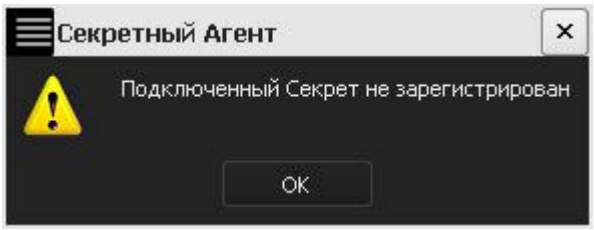

Рисунок 32 – Сообщение об отсутствии регистрации подключенного СН

Затем необходимо посредством выбора пункта меню Пуск → Программы → Секрет Фирмы → Сервер Аутентификации → АРМ Администратора запустить АРМ Администратора, главное окно которого показано на рисунке 33.

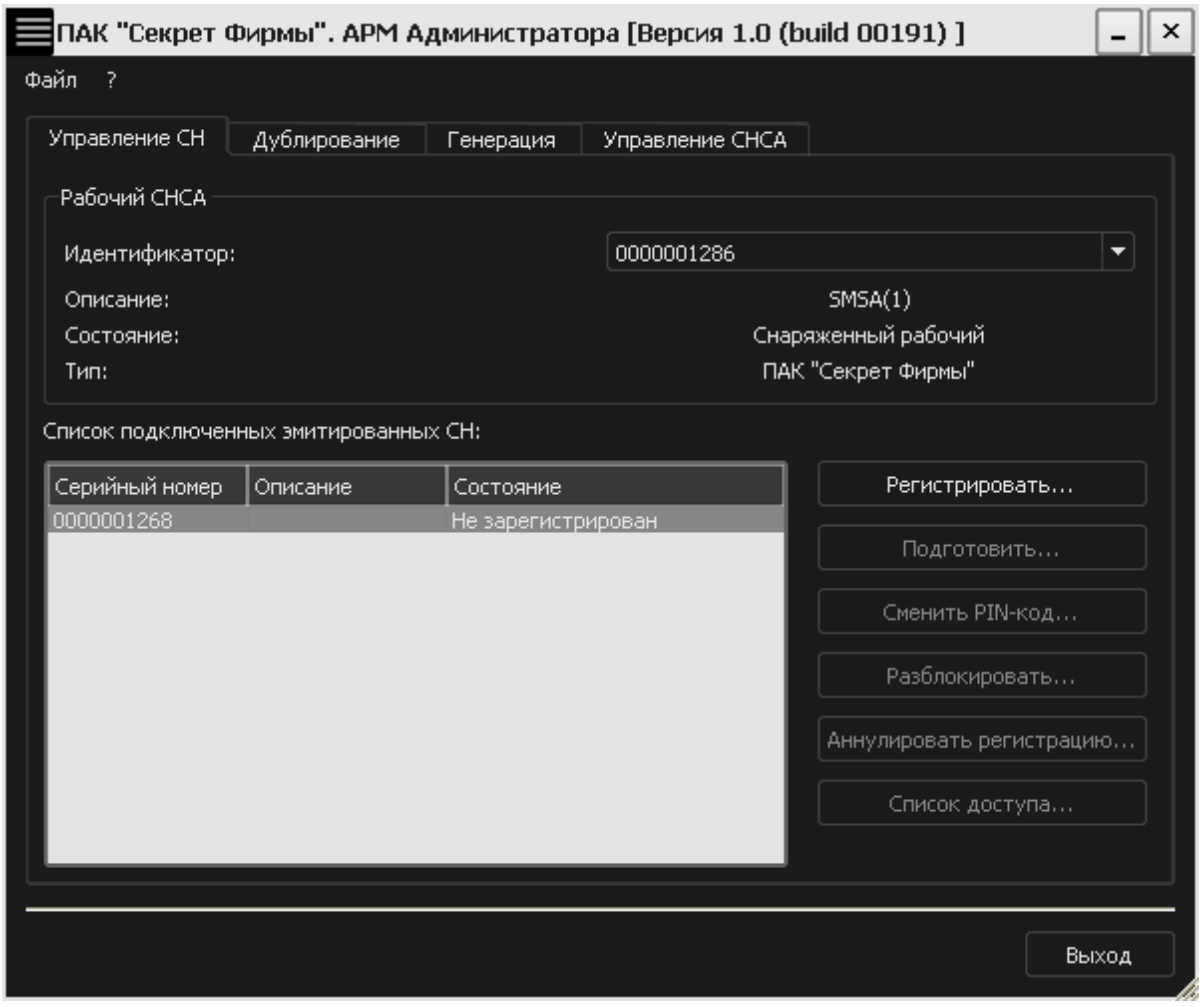

Рисунок 33 – Главное окно АРМ Администратора

Вкладка «Управление СН» главного окна данного приложения содержит идентификатор рабочего СНСА, а также список подключенных эмитированных СН, с указанием имени, серийного номера и состояния. Для регистрации нужного СН необходимо выбрать соответствующий элемент списка с состоянием

<Не зарегистрирован> и нажать кнопку <Регистрировать> (рисунок 33). (Если не выбран ни один элемент списка, кнопка <Регистрировать> недоступна).

После этого на экран выводится окно, в котором нужно задать имя регистрируемого СН (рисунок 34).

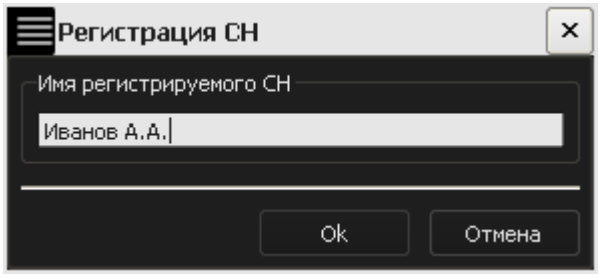

Рисунок 34 – Окно для задания имени регистрируемого СН

Имя представляет собой строку, длина которой ограничена 32 произвольными символами. В качестве имени целесообразно использовать одно или несколько слов, характеризующих принадлежность СН или его назначение (например, это удобно, если в наличии имеется несколько СН, используемых для различных целей. В этом случае их легко отличить друг от друга). Имя «Секрета» 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.

После того как имя СН задано, следует нажать кнопку <OK> (она недоступна, если имя «Секрета» не задано).

Затем в появившемся окне необходимо ввести PIN-код рабочего СНСА, относящегося к данному сегменту сети (рисунок 35).

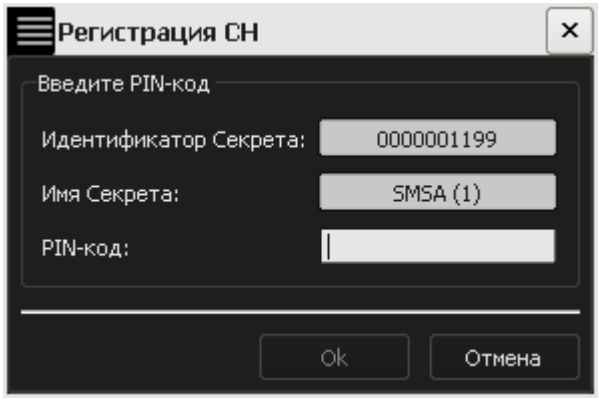

Рисунок 35 – Окно ввода PIN-кода для используемого СНСА

В случае возникновения ошибки в процессе выполнения регистрации СН (в большинстве случаев причиной является ввод неправильного PIN-кода) на экран выводится оповещение об ошибке (рисунок 36).

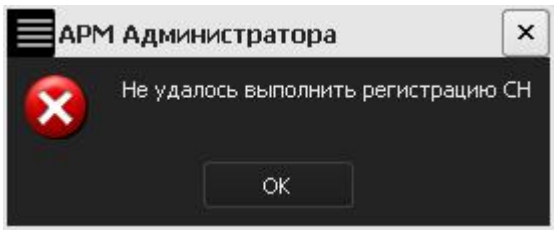

Рисунок 36 - Оповещение об ошибке в ходе регистрации

При отсутствии ошибок в процессе регистрации СН на экран выводится сообщение об успешном завершении процедуры регистрации СН (рисунок 37).

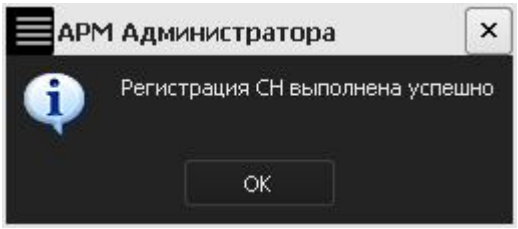

Рисунок 37 - Сообщение об успешной регистрации СН

После нажатия кнопки <OK> на экран выводится окно с основной информацией о зарегистрированном СН.

Организационными мерами необходимо исключить возможность ознакомления администратора с регистрационными данными СН «Секрет Фирмы». Пользователь должен запомнить или надежно сохранить PIN-код и код регистрации СН и обеспечить их недоступность другим лицам.

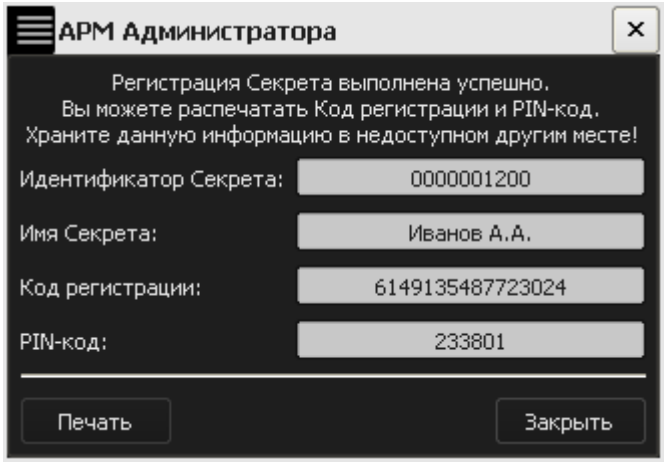

Рисунок 38 – Окно с информацией о зарегистрированном СН

ВНИМАНИЕ! Пользователь должен запомнить или надежно сохранить PIN-код и код регистрации СН, знание которых позволяет получать доступ к перечисленным ниже функциям ПАК «Секрет Фирмы». Пользователь может распечатать код регистрации и PIN-код СН (при наличии подключенного принтера). При этом для облегчения использования «Секрет Фирмы» код регистрации и PIN-код СН печатаются на разных листах (см. рисунок 39, рисунок 40).

Следует помнить о необходимости сохранения этих данных недоступными третьим лицам!

PIN-код СН используется для получения доступа к данным СН.

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 СН

Код регистрации СН используется для выполнения операций:

- регистрации СН в другом сегменте сети;
- отмены регистрации СН;
- разблокирования СН.

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 СН

Посредством нажатия кнопки <Печать> при подключенном принтере пользователь может распечатать информацию о зарегистрированном СН (рисунок 39, рисунок 40). Если информация не была распечатана, то на экран выводится предупреждающее сообщение (рисунок 41).

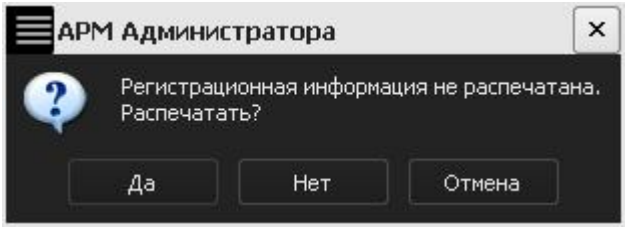

Рисунок 41 – Предупреждающее сообщение

В случае, если печать не требуется, следует нажать кнопку <Нет> или <Отмена>.

После регистрации СН его статус в главном окне АРМ Администратора изменяется на «Зарегистрирован» (рисунок 42), и становится доступным выполнение операций получения доступа (с использованием ПО Рабочей станции, см. руководство пользователя (11443195.4012.032-34), смены PIN-кода, подготовки к повторной регистрации, отмены регистрации и настройки списка доступа (см. соответствующие подразделы 3).

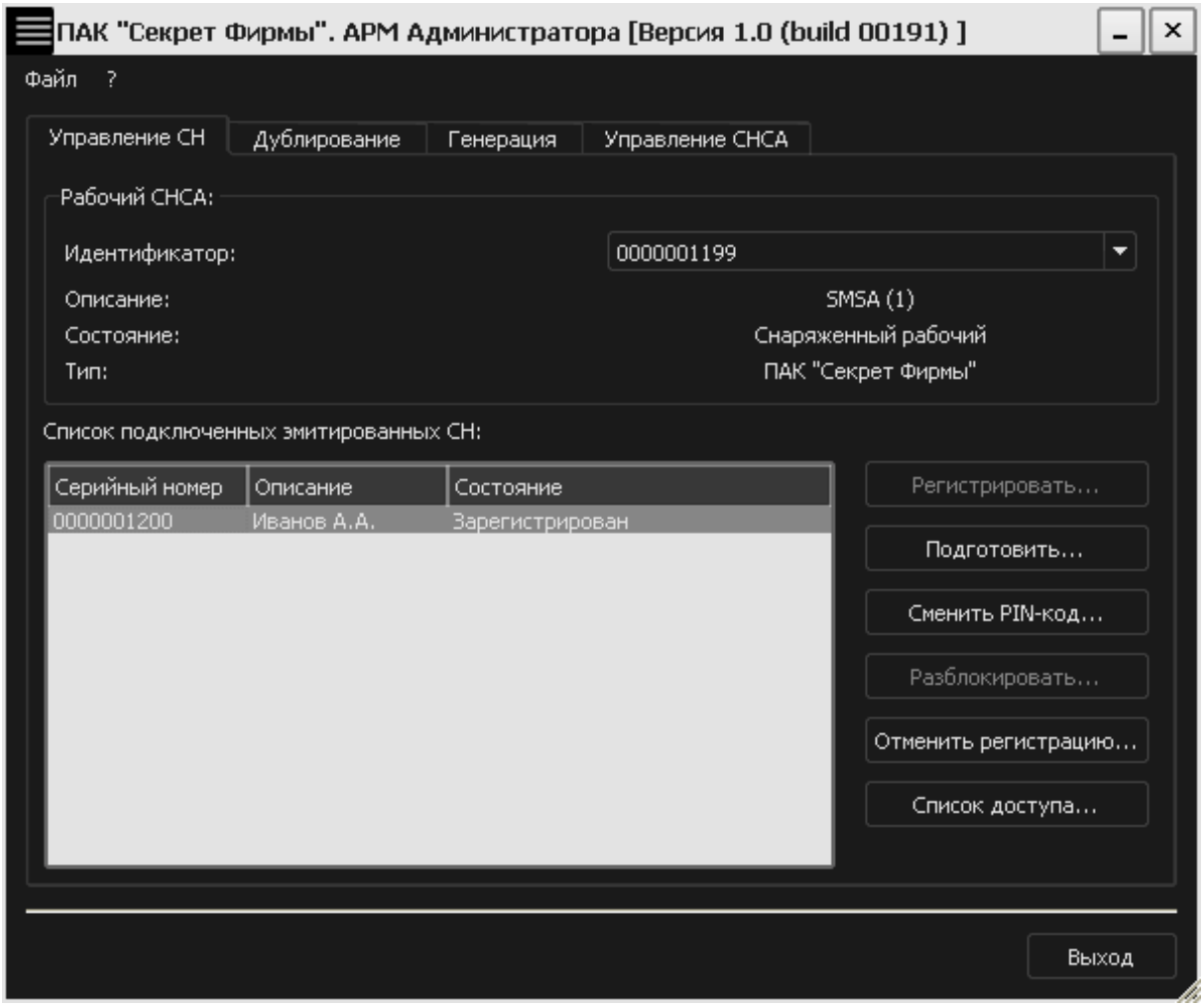

Рисунок 42 – АРМ Администратора. Вкладка «Управление СН»

После успешного завершения процедуры регистрации необходимо выполнить процедуру подготовки СН «Секрет Фирмы» к работе в части настройки параметров получения доступа к данным (см. подраздел 3.4).

Для того чтобы иметь возможность применять «Секрет» в других сегментах сети, необходимо выполнить на них его повторную регистрацию (см. подраздел 3.6).

3.4 Подготовка СН к работе

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

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

ВНИМАНИЕ! Во время выполнения операций, связанных с подготовкой СН, не отключайте устройства «Секрет» от USB-порта компьютера, т. к. это может привести к нарушению их работоспособности!

3.4.1 Настройка списков доступа

До начала использования СН «Секрет Фирмы» администратор должен настроить списки доступа, использование которых позволяет разграничивать доступ к СН на различных компьютерах данного сегмента сети.

В ПАК «Секрет Фирмы» предусмотрено два варианта организации списка доступа:

- «белый» список доступа позволяет использовать СН только на тех компьютерах, имена которых указаны в списке. На остальных РС сегмента сети применение данного СН запрещается;
- «черный» список запрещает использование СН на тех компьютерах, имена которых указаны в списке. На остальных РС сегмента сети применение данного СН разрешается.

Для настройки списков доступа следует во вкладке «Управление СН» АРМ Администратора выбрать из списка необходимый СН и нажать кнопку <Список доступа…> (рисунок 42).

В появившемся окне следует выбрать тот вариант организации списка, который необходимо использовать в соответствии с принятой на предприятии политикой безопасности информации для данной ИС (рисунок 43).

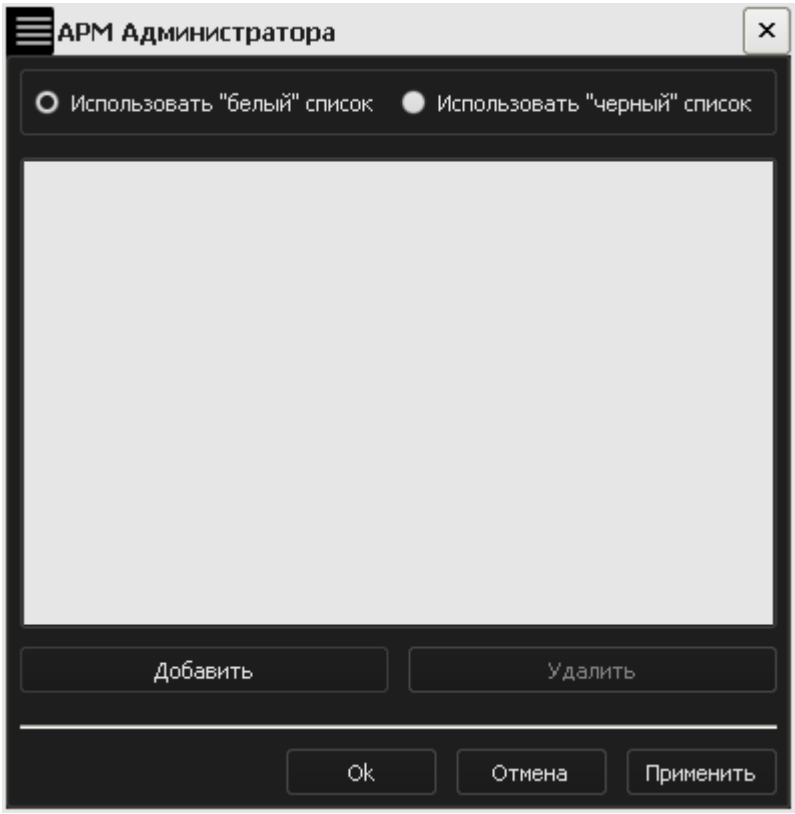

Рисунок 43 – Выбор списка доступа

Для того чтобы добавить компьютер в выбранный список, следует нажать кнопку <Добавить>. В появившемся окне необходимо ввести сетевое имя нужного компьютера (Следует учитывать, что при добавлении в список доступа компьютеров, находящихся в домене, их имена могут содержать имя домена.) и нажать кнопку <OK> (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 (.).

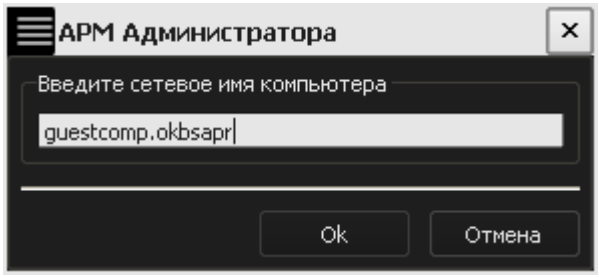

Рисунок 44 – Окно ввода сетевого имени компьютера

Сетевое имя компьютера будет добавлено в список доступа (рисунок 45). Для того чтобы добавить в список необходимое количество компьютеров, описанную процедуру следует провести соответствующее число раз. При необходимости любое имя из списка можно удалить, выделив его и нажав кнопку <Удалить>.

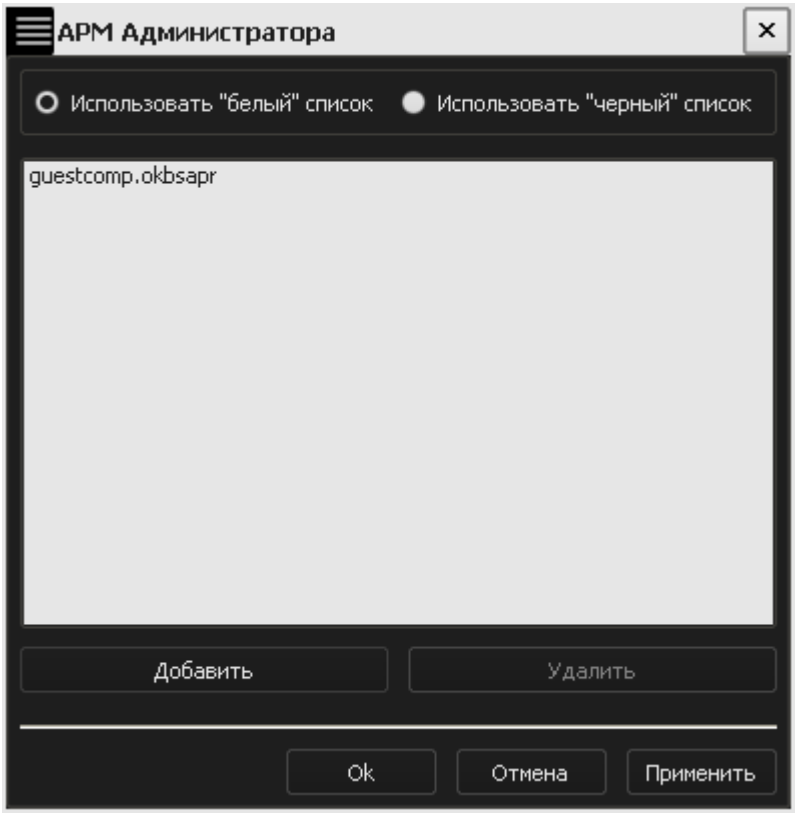

Рисунок 45 – Окно списка доступа

Далее следует нажать кнопку <Применить>, затем – <OK>.

3.4.2 Настройка сетевых параметров

После настройки списков доступа необходимо выполнить настройку сетевых параметров на РС. Для этого следует в трее щелкнуть правой кнопкой мыши на значке «Секретного Агента» (рисунок 46) и в меню выбрать пункт «Настройки».

Рисунок 46 – Значок приложения «Секретный Агент» в трее

Появившееся окно содержит следующие 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 «Секретный Агент» ждет ответа от сервера аутентификации на отправленный им пакет данных.

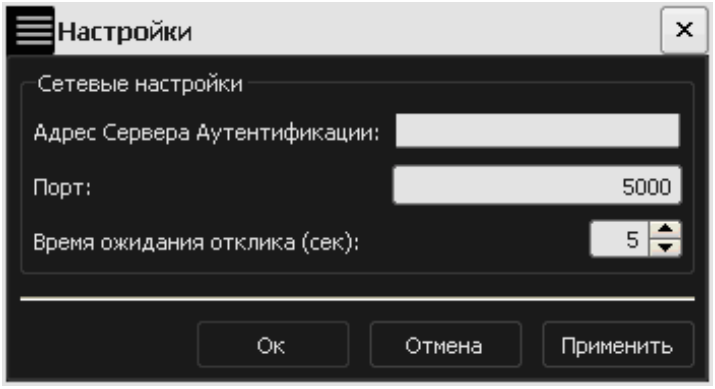

Рисунок 47 – Окно ввода адреса сервера аутентификации

После задания сетевых настроек следует нажать кнопку <OK>. После успешного выполнения описанной процедуры становится возможным применение СН в сегменте сети, который «привязан» к указанному СА. При этом СН обнаруживается системой как обычный флеш-накопитель.

3.5 Загрузка ключевой информации СНСА в сервис СА

Для того чтобы процедура получения доступа к СН (выполняемая как на сервере аутентификации, так и на рабочих станциях) стала возможной, до начала использования СН «Секрет Фирмы» администратор должен выполнить загрузку ключевой информации СНСА в сервис сервера аутентификации.

ВНИМАНИЕ! Если СНСА был отключен от СА (или был выполнен выход из программы «АРМ Администратора»), то ключевая информация выгружается из сервиса СА. Поэтому, для того чтобы процедура выполнения доступа к Секрету стала возможной, ключевую информацию СНСА необходимо загружать в сервис СА после каждого подключения СНСА к серверу аутентификации или перезапуска программы «АРМ Администратора».

Для того чтобы передать в сервис СА ключевую информацию СНСА необходимо подключить рабочий СНСА к USB-порту сервера аутентификации. Во вкладке «Управление СНСА» АРМ Администратора необходимо выбрать требуемый СНСА и нажать кнопку <Загрузить КИ СНСА…> (рисунок 48).

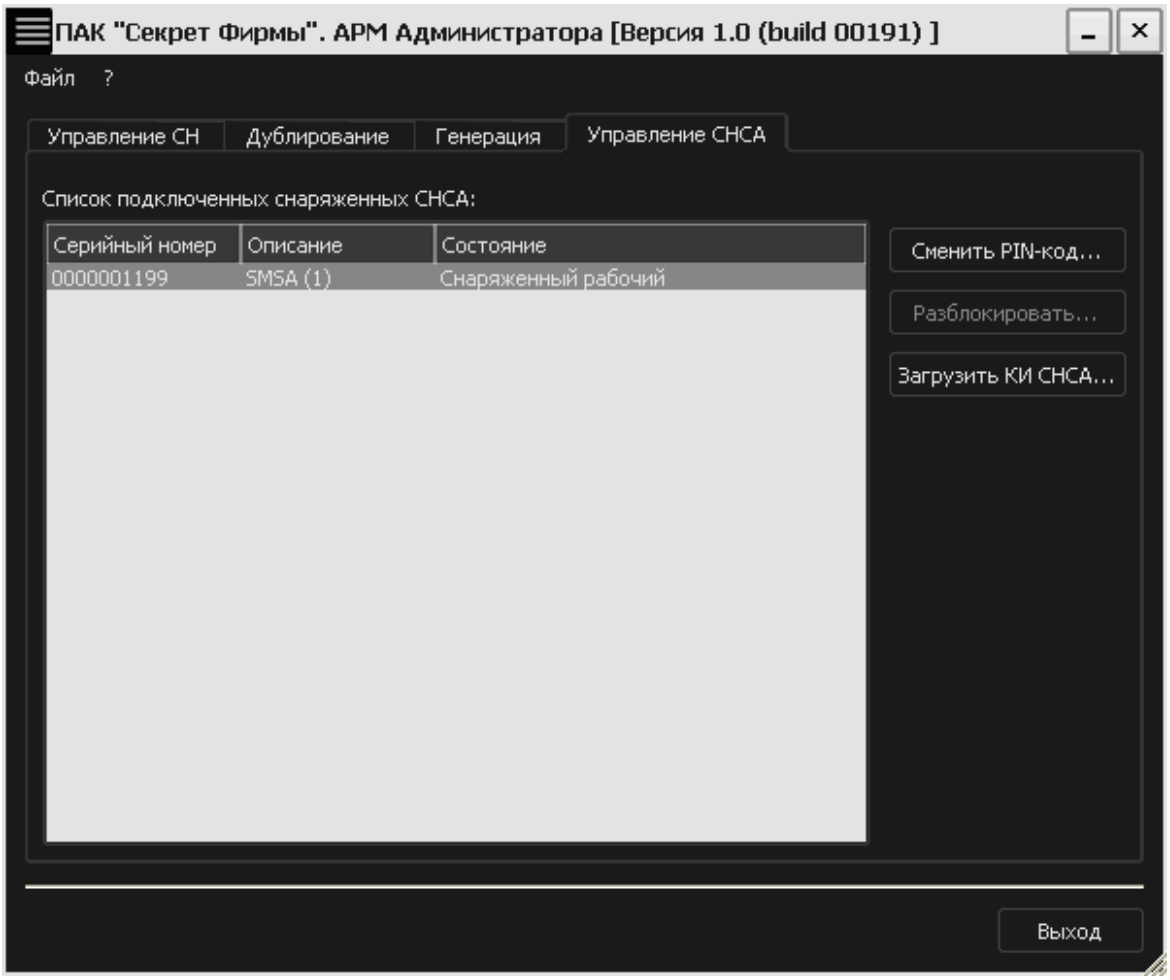

Рисунок 48 – АРМ Администратора. Вкладка «Управление СНСА»

В появившемся окне необходимо ввести PIN-код данного СНСА (рисунок 49).

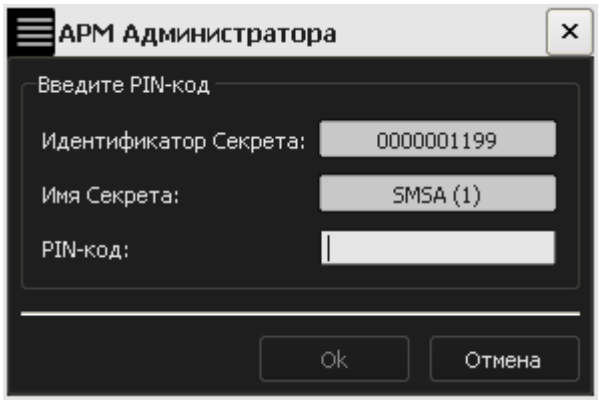

Рисунок 49 - Окно ввода PIN-кода для СНСА

В случае успешного выполнения чтения ключевой информации на экран выводится соответствующее оповещение (рисунок 50).

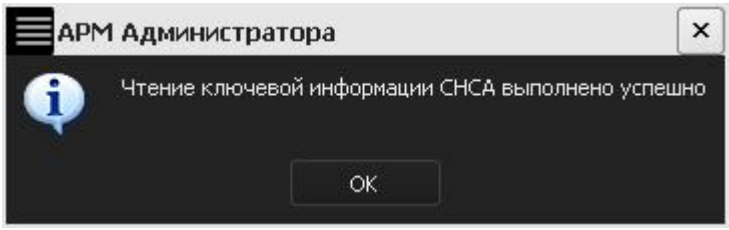

Рисунок 50 – Сообщение об успешном выполнении чтения КИ СНСА

3.6 Регистрация СН в другом сегменте сети

3.6.1 Подготовка СН к процедуре повторной регистрации

Перед выполнением процедуры регистрации СН в другом сегменте сети необходимо произвести подготовку данного СН к процедуре повторной регистрации.

Для этого следует во вкладке «Управление СН» АРМ Администратора выбрать из списка подключенных зарегистрированных СН нужный и нажать кнопку <Подготовить…> (рисунок 51).

ВНИМАНИЕ! Во время выполнения операций, связанных с подготовкой СН к процедуре повторной регистрации, не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

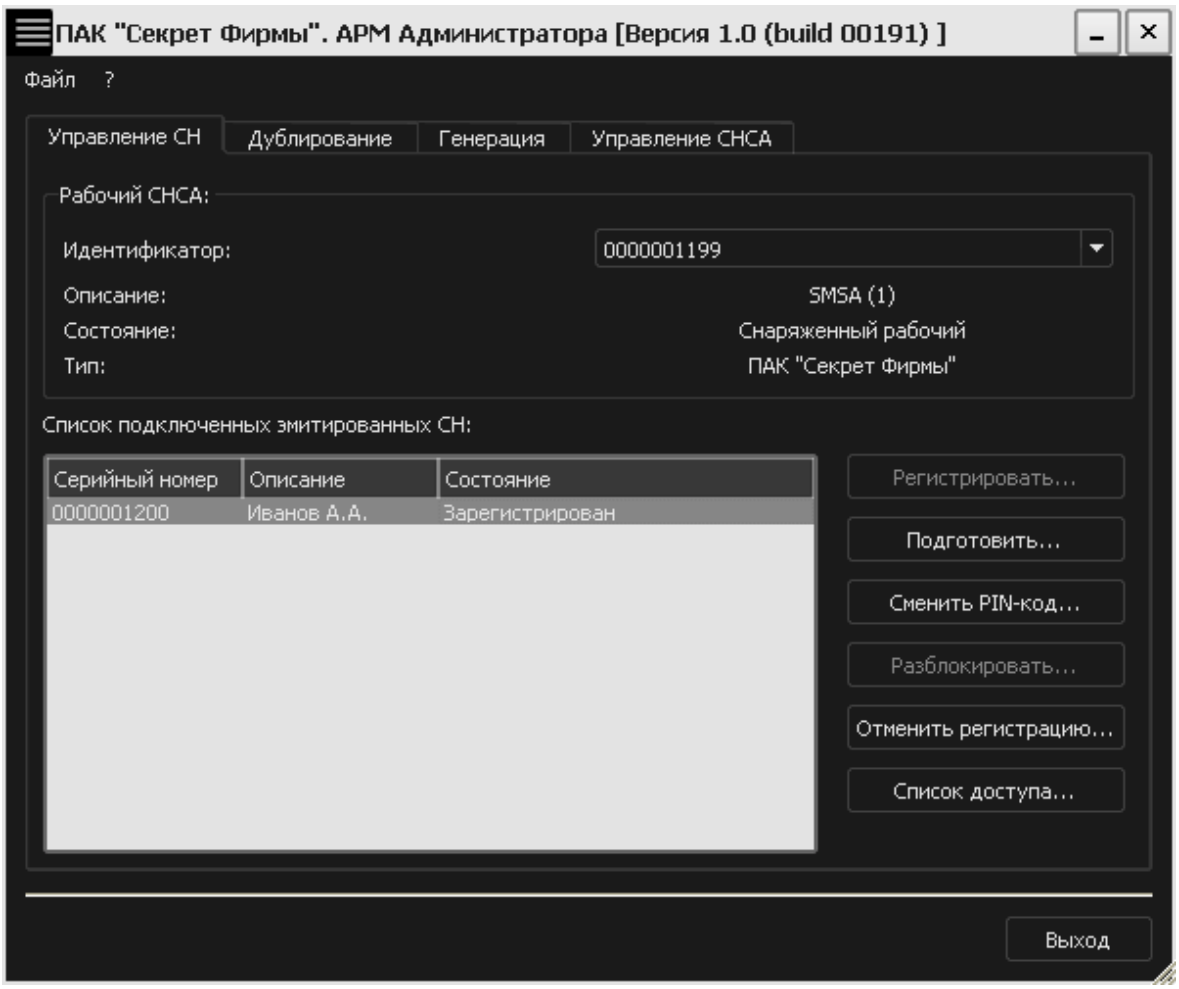

Рисунок 51 – АРМ Администратора. Вкладка «Управление СН»

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

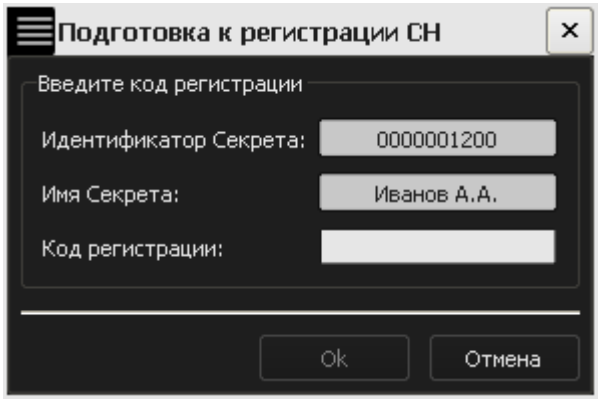

Рисунок 52 – Окно ввода кода регистрации для данного СН

Далее в появившемся окне администратору необходимо ввести PIN-код первичного СНСА, на котором СН зарегистрирован в данный момент, и нажать кнопку <OK> (рисунок 53).

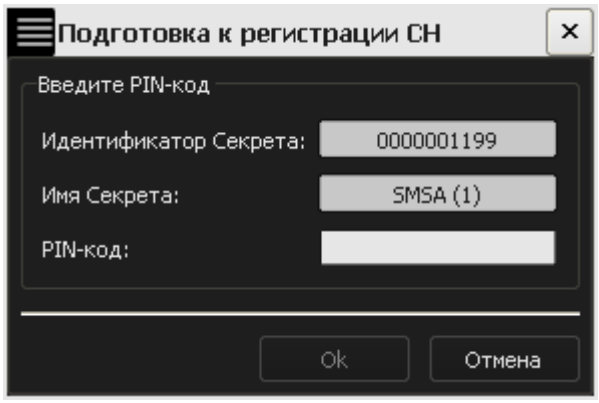

Рисунок 53 – Окно ввода PIN-кода старого СНСА

Появившееся далее окно содержит следующие поля, которые необходимо заполнить (рисунок 54):

- Идентификатор дружественного СНСА. Это номер (нового) СНСА, на котором планируется произвести повторную регистрацию.
- Дата окончания срока действия мандатов. Это дата, до которой (включительно) необходимо провести повторную регистрацию СН[1]. По истечении действия мандата, регистрация на дружественном СНСА становится невозможной[2]. 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, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <…>. Если указанный каталог не существует, он будет создан автоматически.

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

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

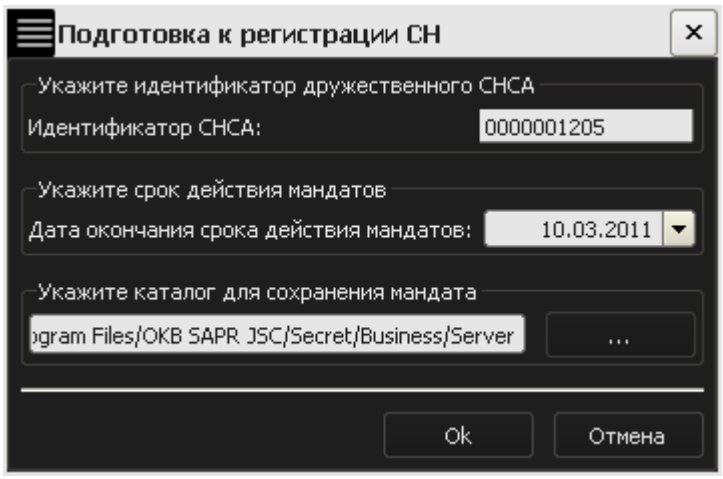

Рисунок 54 – Окно создания мандата регистрации

После заполнения всех полей следует нажать кнопку <OK>.

При успешном выполнении подготовки к повторной регистрации на экран выводится соответствующее оповещение. Данное оповещение содержит также имя файла, в котором сохранен полученный мандат (рисунок 55).

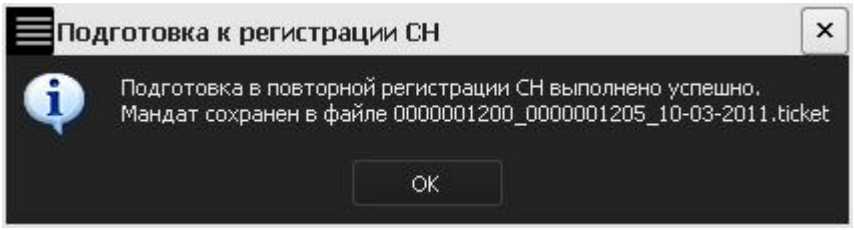

Рисунок 55 – Оповещающее сообщение

ВНИМАНИЕ! Повторная регистрация невозможна при отсутствии файла с мандатом регистрации. Поэтому при выполнении процедуры повторной регистрации администратор первичного СА должен обеспечить доступ к данному файлу для администратора дружественного СА (например, отправить по почте или скопировать на любой носитель информации и перенести в дружественный сегмент сети). При этом безопасность процедуры передачи мандата регистрации обеспечивается средствами организации, эксплуатирующей ПАК «Секрета Фирмы».

После получения мандата регистрации администратор дружественного СА может провести операцию регистрации данного СН на дружественном СНСА.

3.6.2 Повторная регистрация СН

После успешного выполнения подготовки СН к повторной регистрации может быть выполнена повторная регистрация СН в дружественном сегменте сети.

Для этого СНСА дружественного СА и СН, который необходимо повторно зарегистрировать, следует подключить к USB-портам дружественного сервера

аутентификации. При этом допускается использование USB-хаба с собственным источником питания (см. 1.3).

Далее следует запустить приложение «АРМ Администратора». Оно может быть запущено посредством выбора пункта меню Пуск → Программы → Секрет Фирмы → Сервер Аутентификации → АРМ Администратора.

ВНИМАНИЕ! Во время выполнения операций, связанных проведением повторной регистрации СН, не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

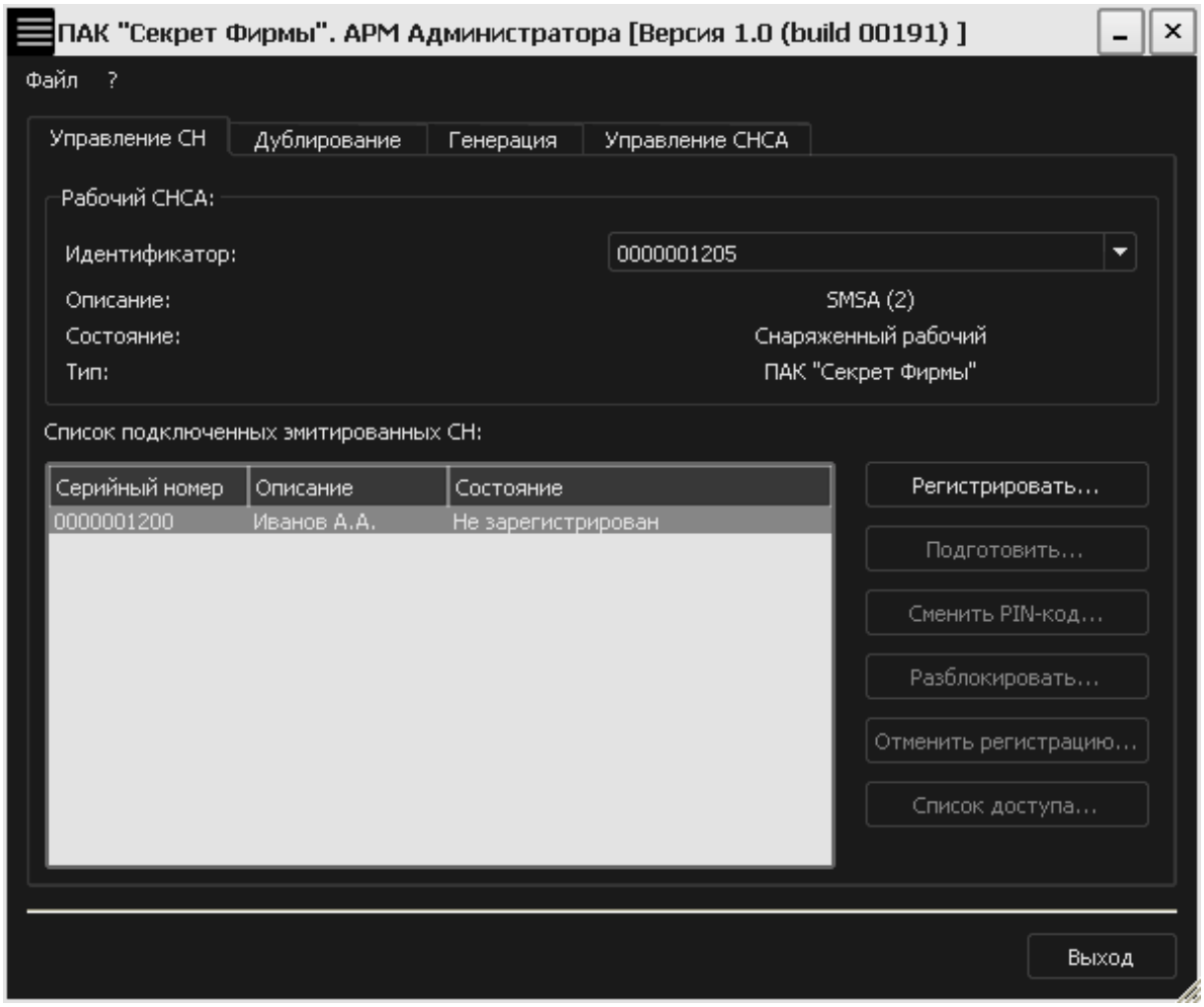

Рисунок 56 – АРМ Администратора. Вкладка «Управление СН»

Из списка подключенных эмитированных СН следует выбрать тот, который необходимо зарегистрировать, и нажать кнопку <Регистрировать…> (рисунок 56).

В появившемся окне (рисунок 57) пользователь должен ввести код регистрации данного СН, полученный при первичной регистрации СН (см. 3.3).

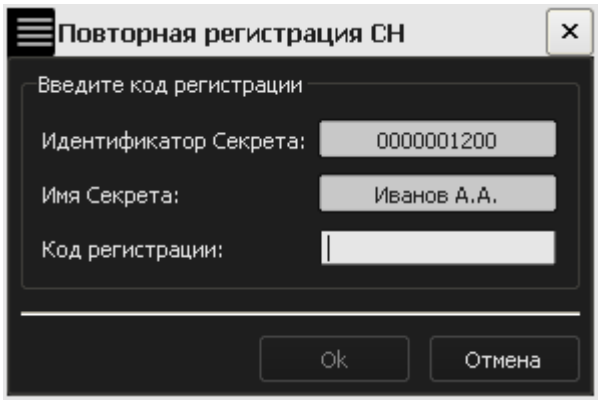

Рисунок 57 – Окно ввода кода регистрации для регистрируемого СН

Далее в появившемся окне администратору необходимо ввести PIN-код СНСА, на котором производится процедура повторной регистрации (рисунок 58).

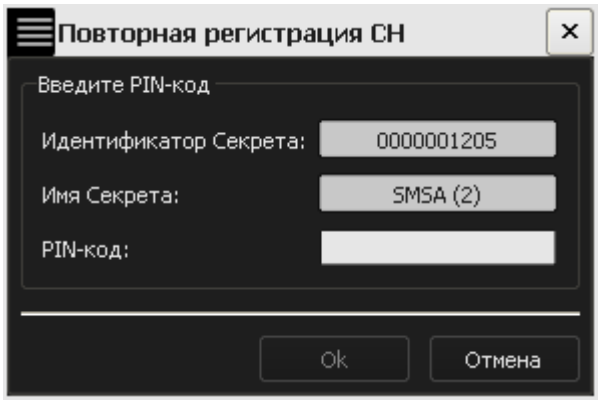

Рисунок 58 – Окно ввода PIN-кода дружественного СНСА

После корректного ввода PIN-кода дружественного СНСА администратору необходимо указать путь к файлу с мандатом регистрации и нажать кнопку <OK> (рисунок 59).

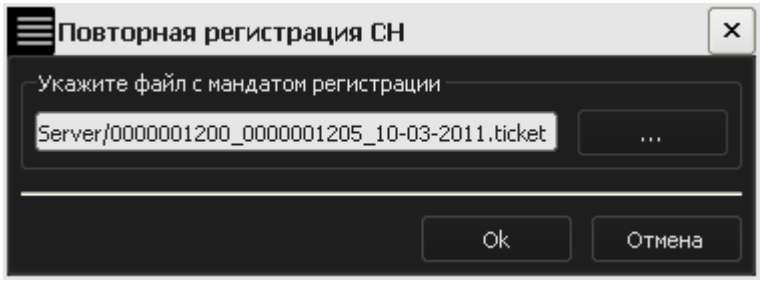

Рисунок 59 – Окно для указания файла с мандатом регистрации

Путь может быть указан вручную или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <…>.

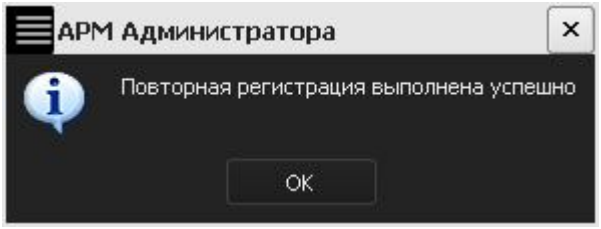

Рисунок 60 – Оповещение об успешной повторной регистрации

После верного выполнения описанной последовательности действий на экран выводится сообщение об успешной повторной регистрации СН (рисунок 60)

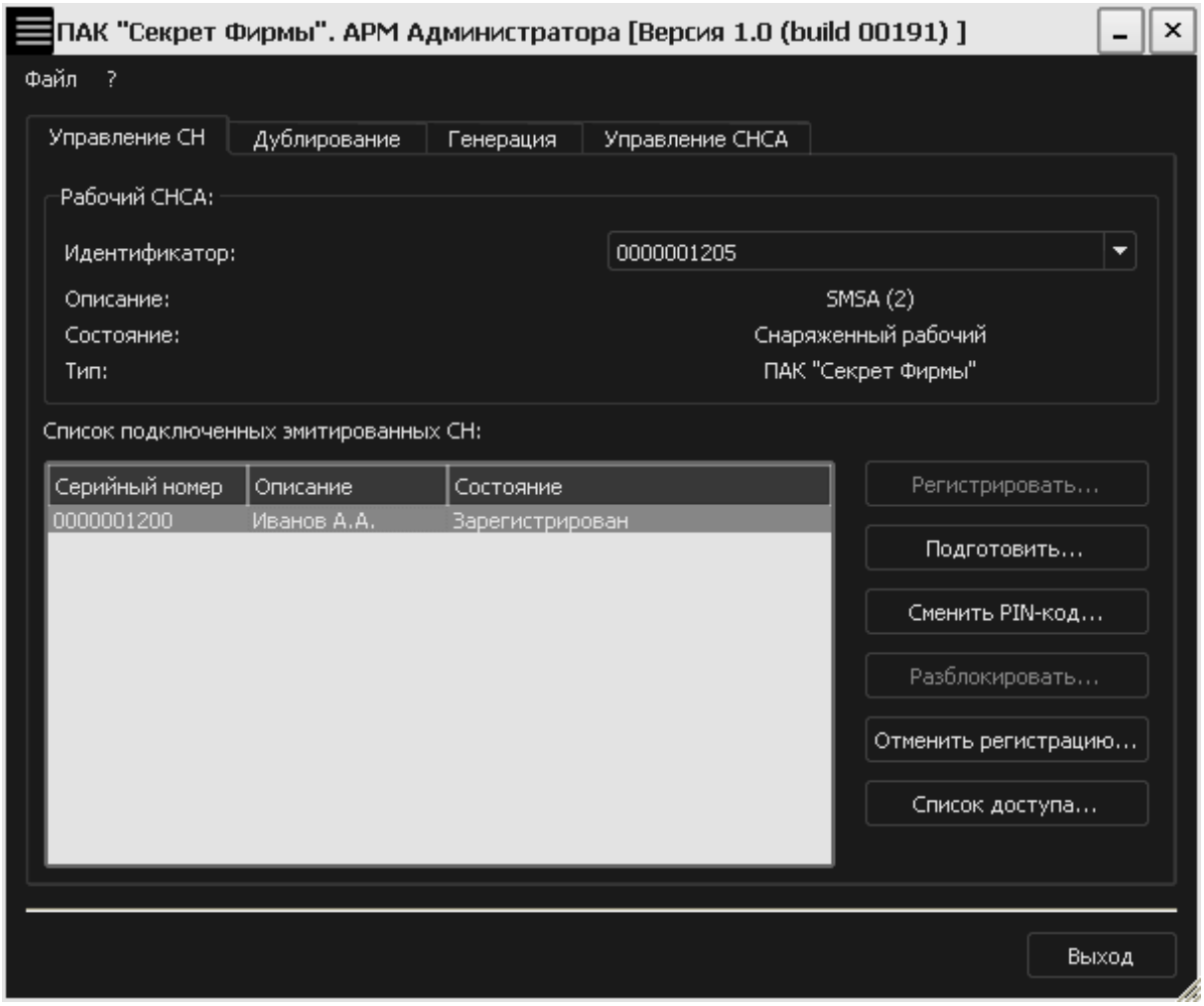

Рисунок 61 – АРМ Администратора. Вкладка «Управление СН»

После выполнения процедуры повторной регистрации СН его статус во вкладке «Управление СН» АРМ Администратора изменяется на «Зарегистрирован» (рисунок 61) и становится возможным управление СН. При этом возможность использования СН в сегменте сети первичного сервера аутентификации сохраняется.

3.7 Отмена регистрации СН

Процедура отмены регистрации СН предназначена для исключения сегментов сети из списка тех, на которых возможен доступ к данным, хранящимся в «Секрете». Использование этого механизма позволяет контролировать список сегментов сети, на которых может быть осуществлен доступ к содержимому «Секрета».

После выполнения процедуры отмены регистрации доступ к данному «Секрету» в данном сегменте сети станет невозможным до выполнения процедуры регистрации заново.

Процедура отмены регистрации СН в одном из дружественных сегментов сети не влияет на возможность работы с «Секретом» в других сегментах сети (дружественных или первичном). При отмене регистрации СН в первичном сегменте сети работа с «Секретом» становится невозможной во всех сегментах сети до выполнения процедур регистрации заново.

Необходимо своевременно выполнять процедуру отмены регистрации СН в сегментах сети, на которых не требуется доступ к содержимому СН.

Для отмены регистрации СН необходимо во вкладке «Управление СН» АРМ Администратора выбрать соответствующий элемент из списка зарегистрированных СН и нажать кнопку <Отменить регистрацию> (рисунок 62).

ВНИМАНИЕ! Во время выполнения операций, связанных проведением процедуры отмены регистрации СН, не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

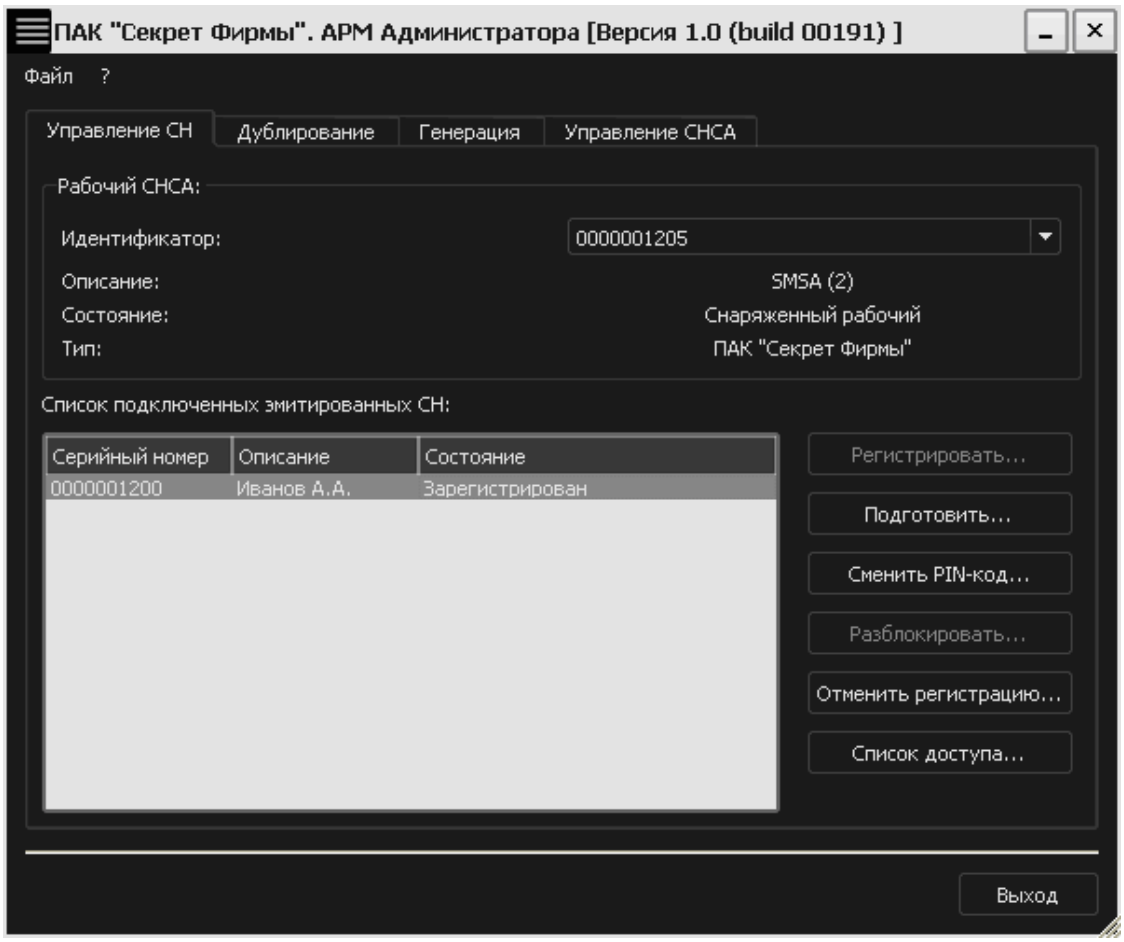

Рисунок 62 – Главное окно АРМ Администратора. Вкладка «Управление СН»

В появившемся окне пользователю необходимо ввести код регистрации данного СН (рисунок 63).

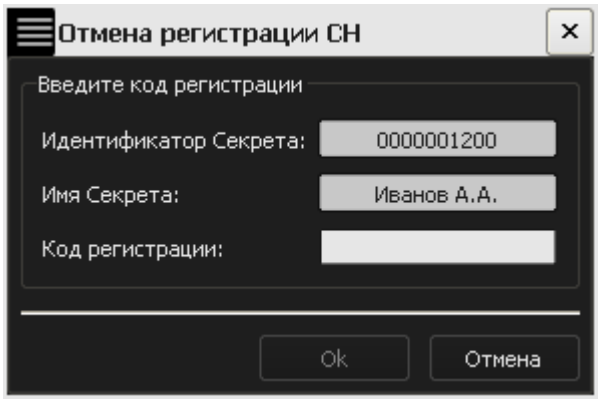

Рисунок 63 – Окно ввода кода регистрации СН

По нажатии кнопки <OK> на экран выводится окно, в котором администратору следует ввести PIN-код соответствующего СНСА (рисунок 64).

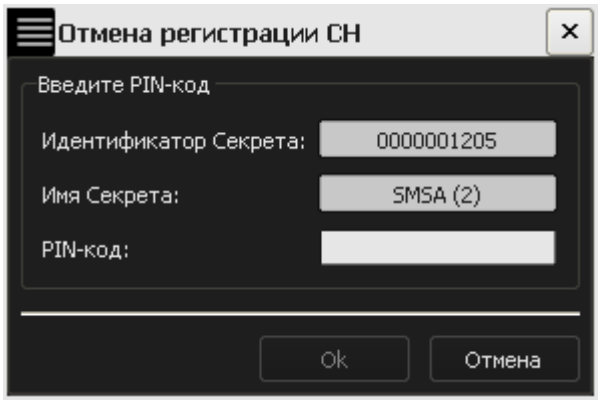

Рисунок 64 – Окно ввода PIN-кода для соответствующего СНСА

В случае возникновения ошибки в процессе выполнения процедуры отмены регистрации СН (например, в результате ввода неправильного PIN-кода или кода регистрации) на экран выводится оповещение об ошибке:

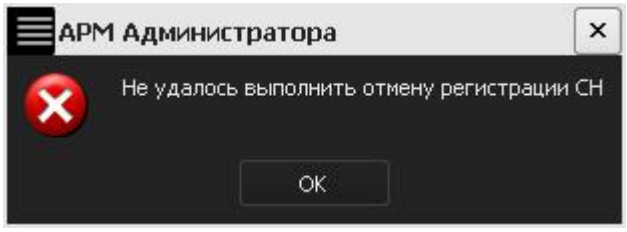

Рисунок 65 – Сообщение о сбое в ходе отмены регистрации

В случае корректного завершения процедуры на экран выводится сообщение об успешной отмене регистрации (рисунок 66).

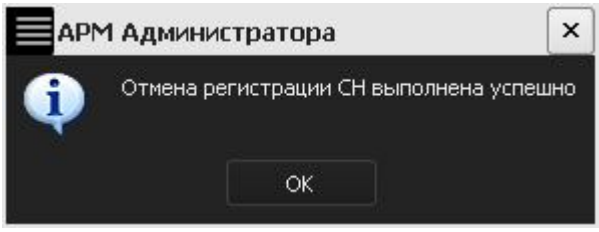

Рисунок 66 - Сообщение об успешной отмене регистрации

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

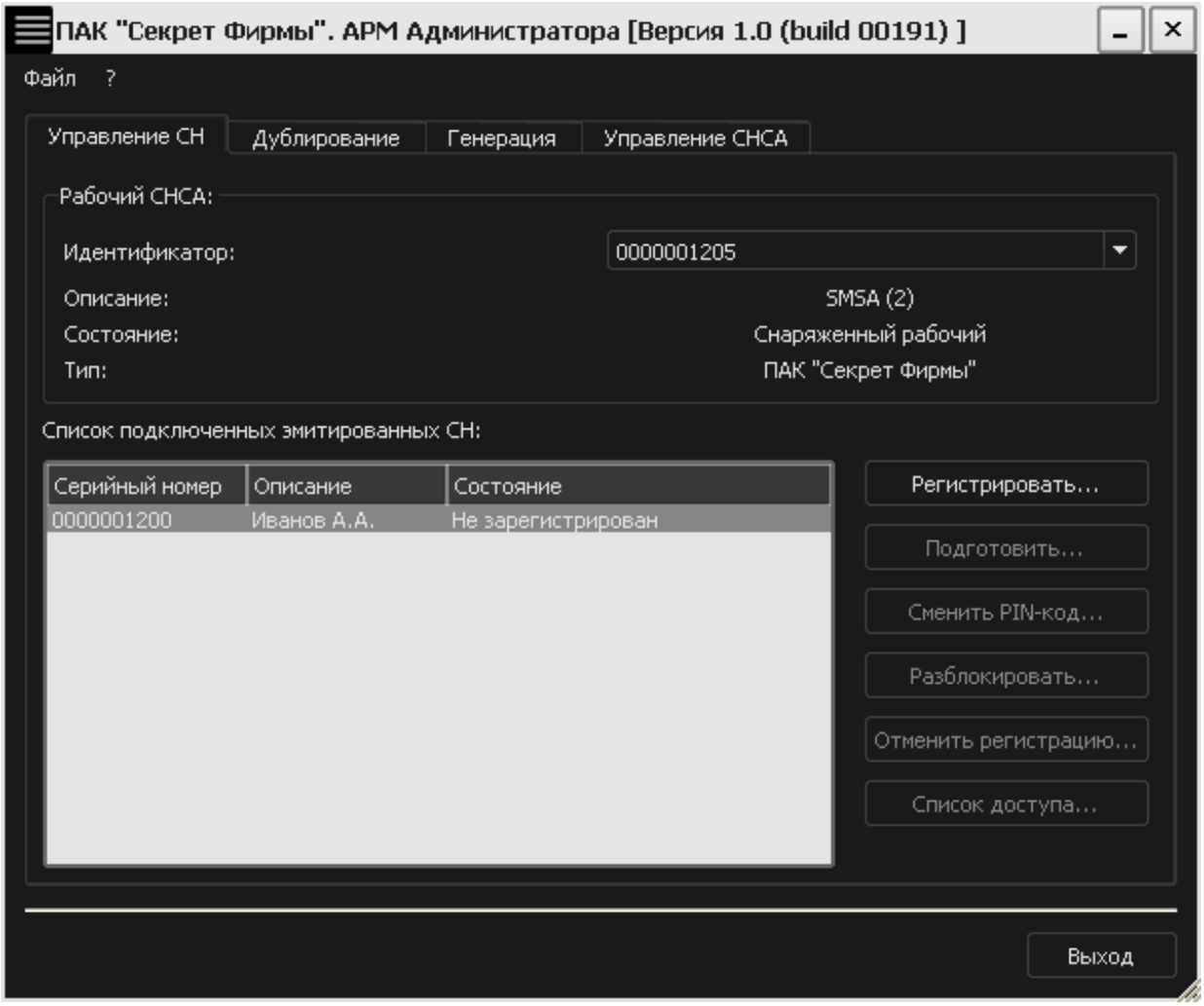

Рисунок 67 – Главное окно АРМ Администратора. Вкладка «Управление СН»

После этого выполнение операций с данным СН в данном сегменте сети становится невозможным.

3.8 Смена PIN-кода СНСА

Если администратор СНСА считает PIN-код скомпрометированным, он может сменить действующий PIN-код на новый. При этом СНСА должен быть подключен к СА. Для смены PIN-кода необходимо во вкладке «Управление СНСА» АРМ Администратора выбрать из списка нужный СНСА и нажать кнопку <Сменить PIN-код> (рисунок 68).

ВНИМАНИЕ! Во время выполнения операции смены PIN-кода СНСА не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

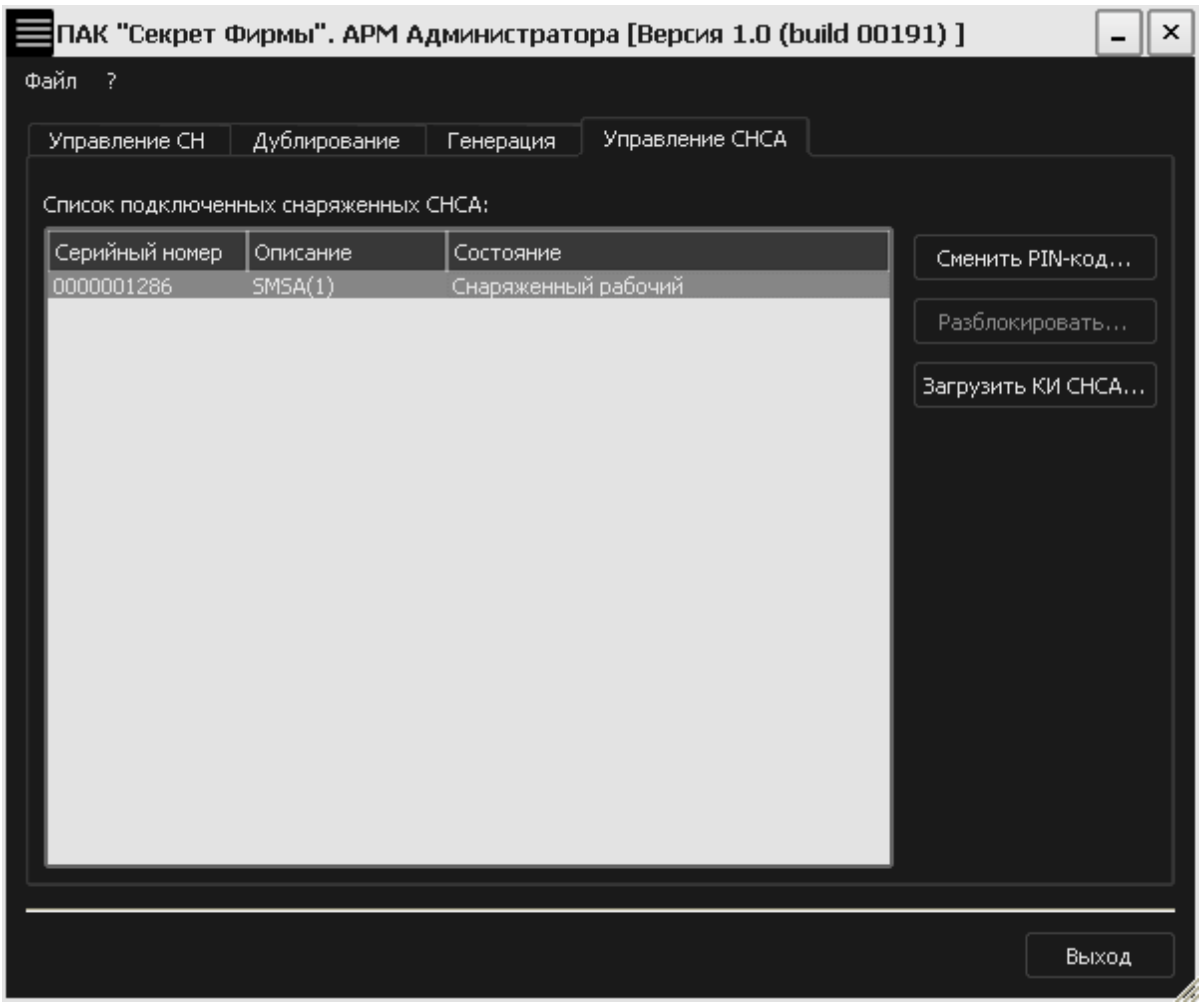

Рисунок 68 – Главное окно АРМ Администратора. Вкладка «Управление СНСА»

В появившемся окне следует ввести старый PIN-код для данного СНСА (рисунок 69).

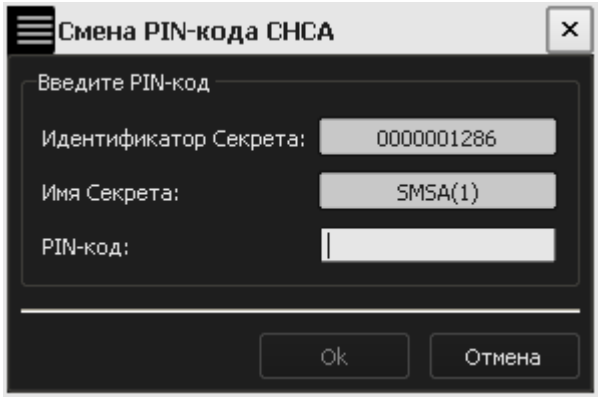

Рисунок 69 – Окно ввода PIN-кода для данного СНСА

В случае корректного ввода старого PIN-кода СНСА на экране появляется сообщение об успешной смене PIN-кода (рисунок 70), который генерируется автоматически.

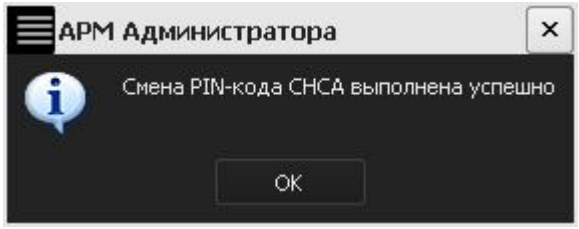

Рисунок 70 - Сообщение об успешной смене PIN-кода СНСА

После нажатия кнопки <OK> на экране появится окно с новым PIN-кодом СНСА, который необходимо запомнить или надежно сохранить (рисунок 71).

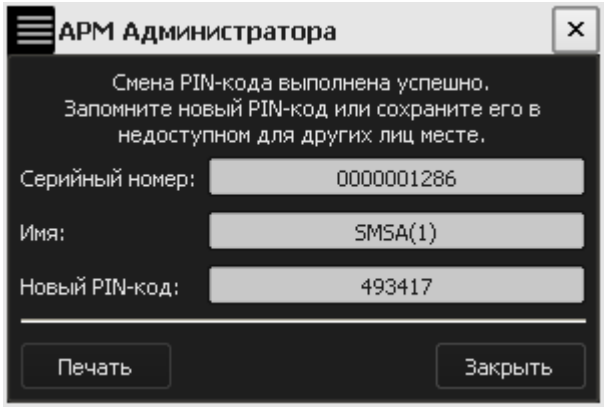

Рисунок 71 – Окно с новым PIN-кодом для СНСА

Имеется возможность печати нового PIN-кода с помощью кнопки <Печать>.

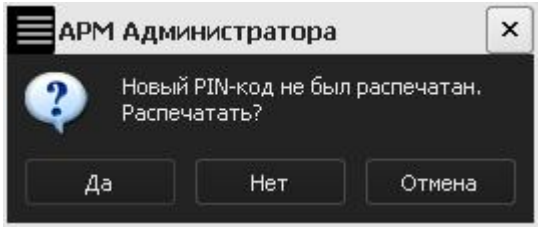

Рисунок 72 – Предупреждающее сообщение

В случае если новый PIN-код не был распечатан, на экран выводится предупреждающее сообщение (рисунок 72). В соответствии с принятым решением следует нажать кнопку <Да>, <Нет> или <Отмена>.

3.9 Смена PIN-кода СН

Если у пользователя СН имеются подозрения о компрометации PIN-кода, имеется возможность сменить действующий PIN-код на новый. При выполнении процедуры смены PIN-кода СН должен быть подключен к USB-порту сервера аутентификации. При этом допускается использование USB-хаба с собственным источником питания (см. 1.3).

Используемый в ПАК «Секрет Фирмы» механизм смены PIN-кода СН на сервере аутентификации позволяет обеспечить безопасность выполнения

данной процедуры за счет исключения передачи критически важных данных между сервером аутентификации и рабочей станцией по сети.

Для смены PIN-кода необходимо во вкладке «Управление СН» АРМ Администратора выбрать из списка нужный СН и нажать кнопку <Сменить PIN-код> (рисунок 73).

ВНИМАНИЕ! Во время выполнения операции смены PIN-кода СН не отключайте устройство «Секрет» от USB-порта компьютера, т. к. это может привести к нарушению его работоспособности!

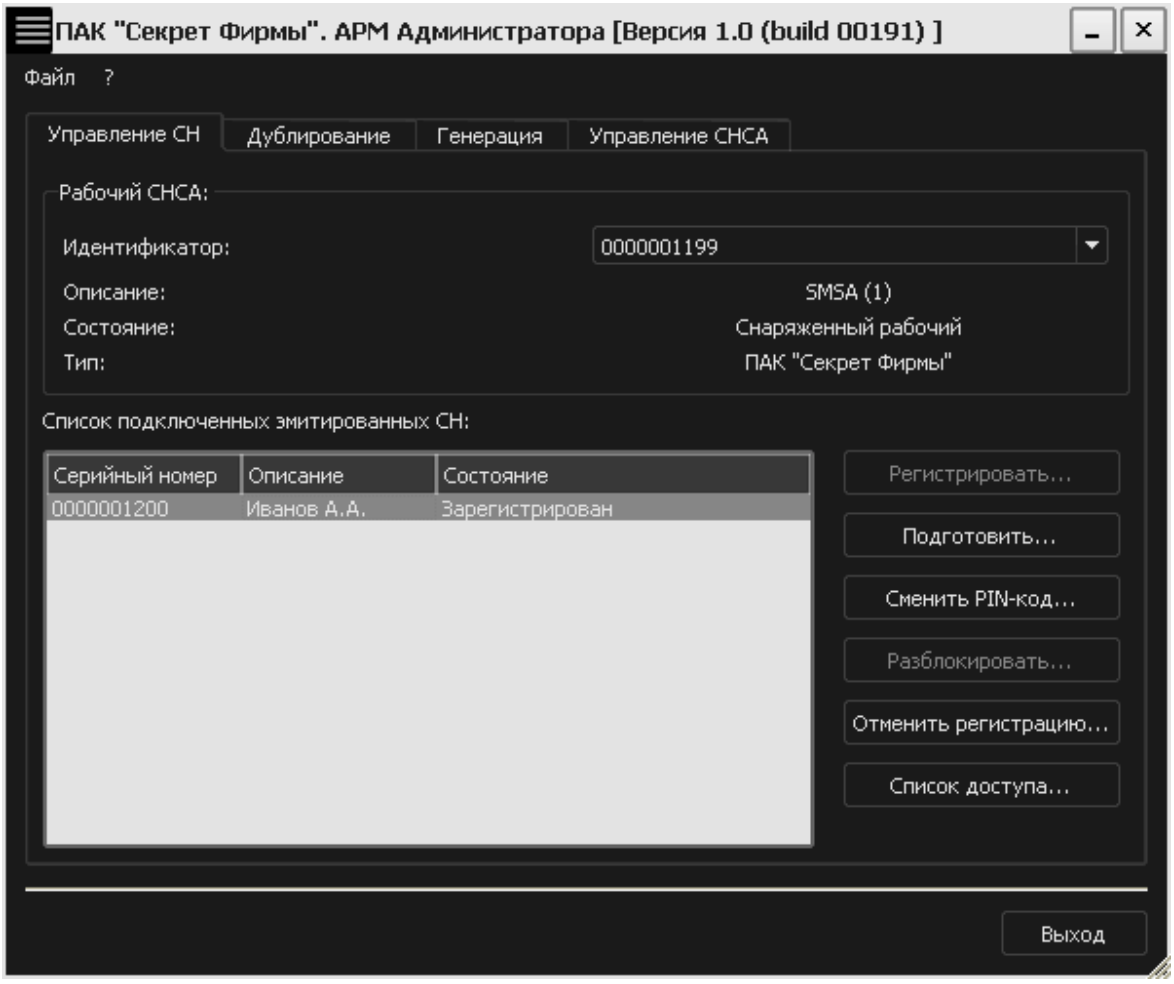

Рисунок 73 – Главное окно АРМ Администратора. Вкладка «Управление СН»

В появившемся окне пользователь должен ввести старый PIN-код данного СН, указать новый PIN-кода, а также подтвердить ввод нового PIN-кода (рисунок 74).

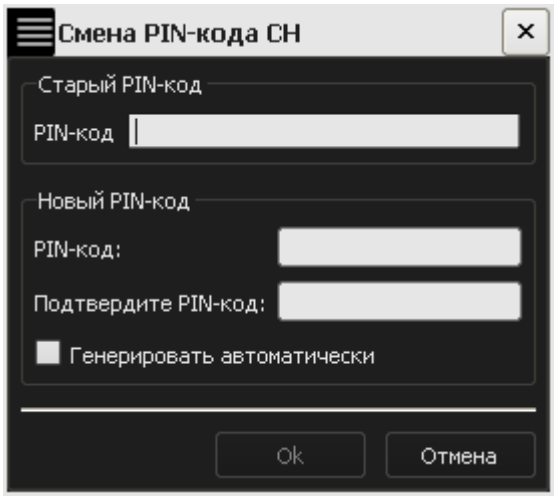

Рисунок 74 – Окно смены PIN-кода для данного СН на желаемый пользователем

Имеется возможность задать новый PIN-код самостоятельно (как описано выше) или сгенерировать его автоматически с помощью установки флага <Генерировать автоматически> (рисунок 75).

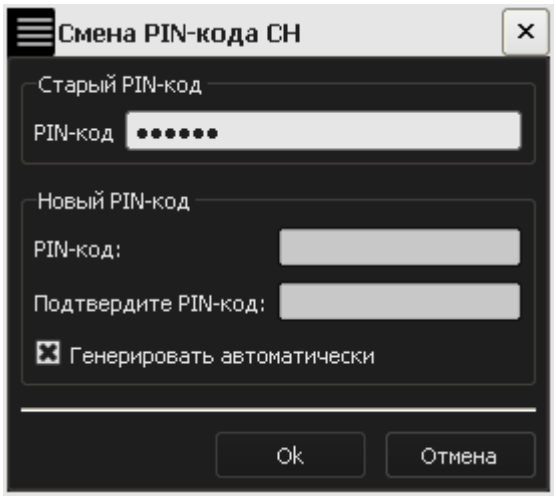

Рисунок 75 - Окно смены PIN-кода для данного СН на сгенерированный автоматически

В появившемся далее окне администратору необходимо ввести PIN-код СНСА, к которому относится данный СН (рисунок 76).

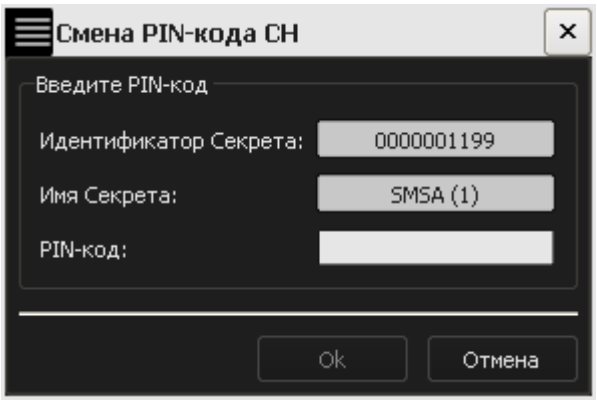

Рисунок 76 – Окно ввода PIN-кода для соответствующего СНСА

В случае некорректного выполнения описанной процедуры на экран выводится сообщение о том, что смену PIN-кода СН выполнить не удалось (рисунок 77).

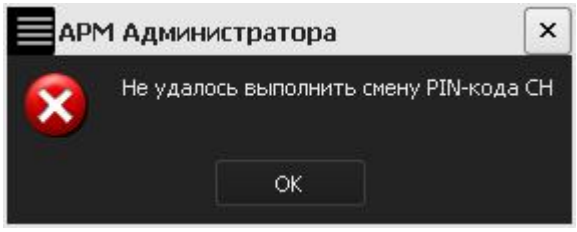

Рисунок 77 - Сообщение об ошибке в ходе смены PIN-кода СН

В случае корректного выполнения описанной последовательности действий на экран выводится сообщение об успешной смене PIN-кода СН (рисунок 78).

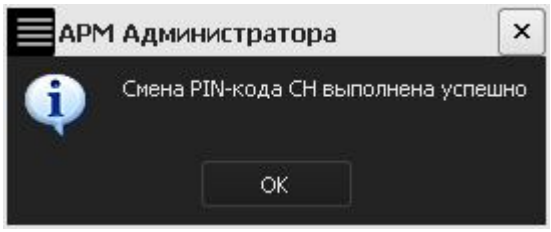

Рисунок 78 - Сообщение об успешной смене PIN-кода СН

Далее на экран выводится окно с новым PIN-кодом СН (рисунок 79).

При выполнении процедуры смены PIN-кода организационными мерами необходимо обеспечить невозможность ознакомления администратора с PIN-кодом СН «Секрет Фирмы». Пользователь должен запомнить или надежно сохранить новый PIN-код СН и обеспечить его недоступность другим лицам.

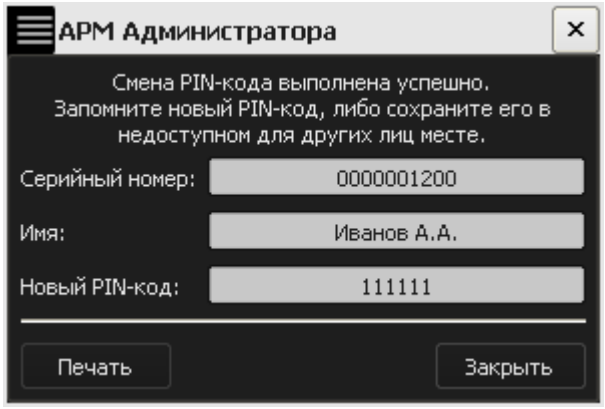

Рисунок 79 – Окно с новым PIN-кодом СН

Имеется возможность печати нового PIN-кода с помощью кнопки <Печать>.

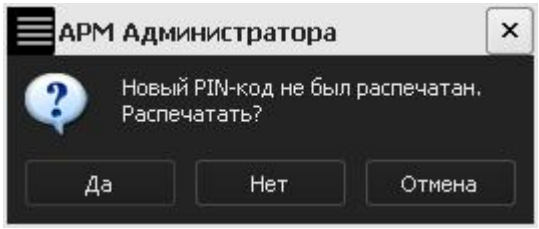

Рисунок 80 – Предупреждающее сообщение

В случае если новый PIN-код не был распечатан, на экран выводится предупреждающее сообщение (рисунок 80).

3.10 Разблокирование СН

В случае трех последовательных неудачных попыток ввода PIN-кода СН блокируется и на экран выводится соответствующее сообщение (рисунок 81).

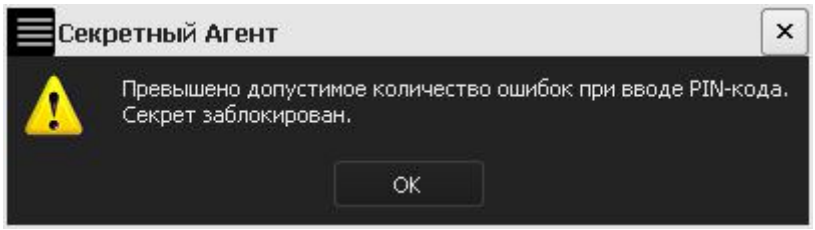

Рисунок 81 – Оповещение о блокировке СН

В таком случае при подключении заблокированного «Секрета» к USB-порту компьютера на экране появляется следующее окно:

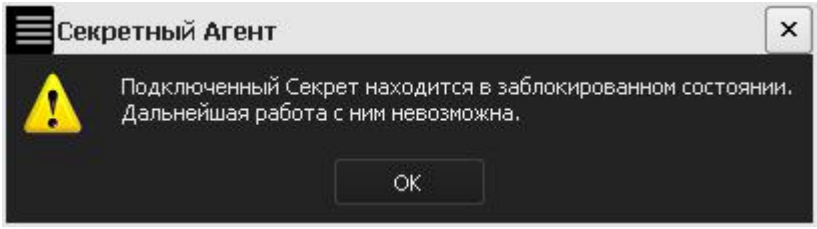

Рисунок 82 – Оповещение при подключении к USB-порту компьютера о блокировке СН

При этом статус СН во вкладке «Управление СН» в главном окне АРМ Администратора изменяется на «Заблокирован» и единственной доступной операцией становится <Разблокировать> (рисунок 83).

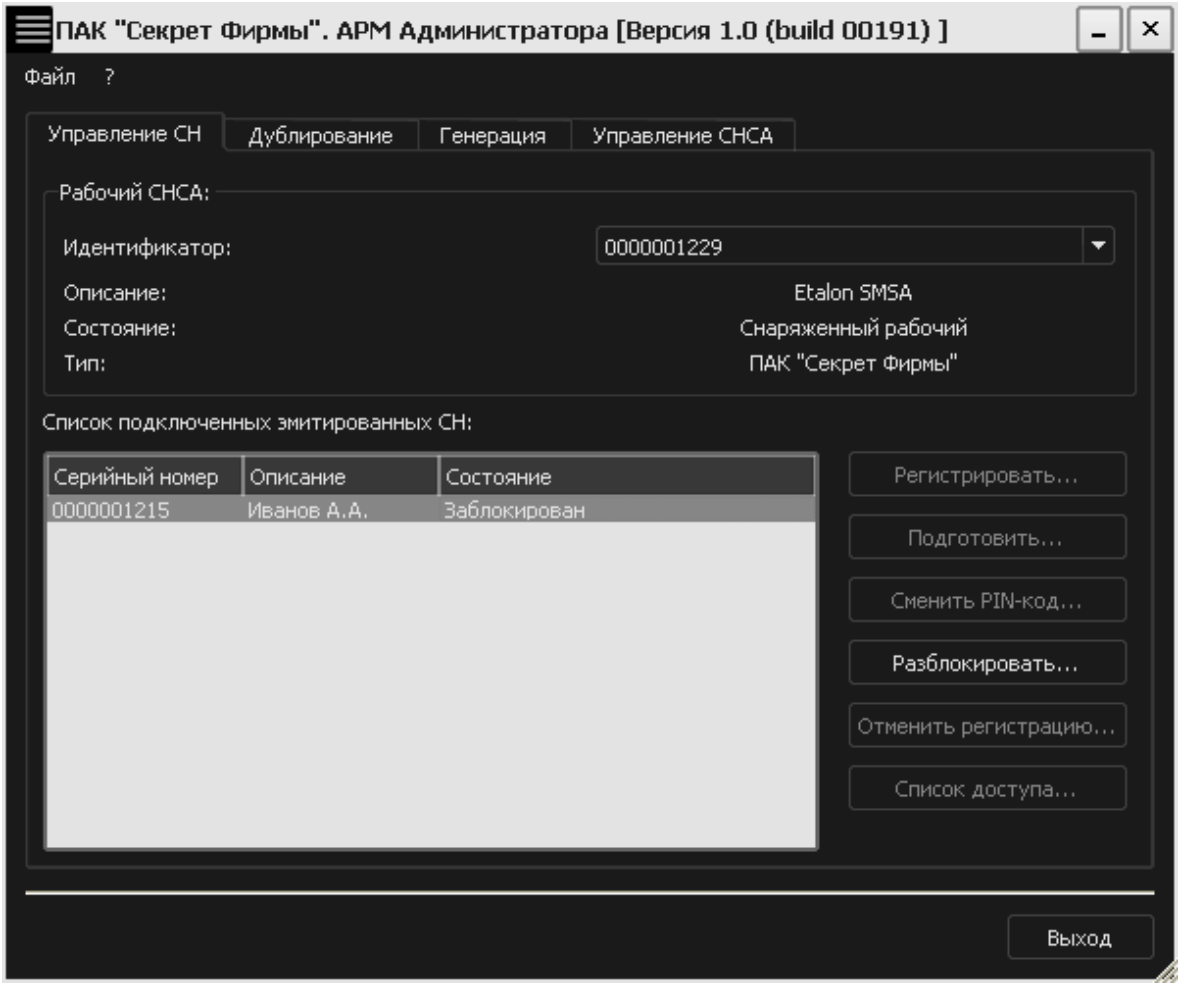

Рисунок 83 – Вкладка «Управление СН» АРМ Администратора

Для выполнения процедуры разблокирования СН необходимо подключить к USB-портам сервера аутентификации заблокированный СН и рабочий СНСА для данного сегмента сети. При этом допускается использование USB-хаба с собственным источником питания (см. 1.3).

СН может быть разблокирован посредством выбора соответствующего элемента списка и нажатия кнопки <Разблокировать>.

ВНИМАНИЕ! Во время выполнения операции разблокирования СН не отключайте устройства «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению их работоспособности!

В появившемся окне пользователю необходимо ввести код регистрации, полученный в результате первичной регистрации СН (рисунок 38), и новое значение PIN-кода.

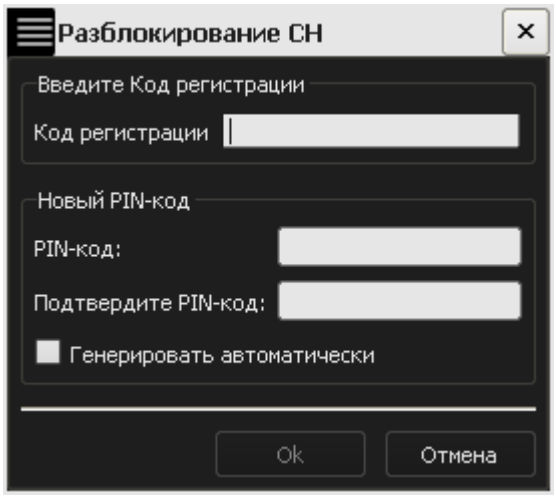

Рисунок 84 – Разблокирование СН

Пользователь может задать новый PIN-код самостоятельно или сгенерировать его автоматически с помощью установки флага <Генерировать> (рисунок 84).

После ввода кода регистрации СН и задания нового PIN-кода следует нажать кнопку <OK>. В появившемся далее окне администратору следует ввести PIN-код рабочего СНСА, к которому относится данный СН (рисунок 85).

При выполнении данных операций организационными мерами необходимо обеспечить невозможность ознакомления администратора с PIN-кодом СН «Секрет Фирмы», а также невозможность ознакомления пользователя с PIN-кодом рабочего СНСА «Секрет Фирмы».

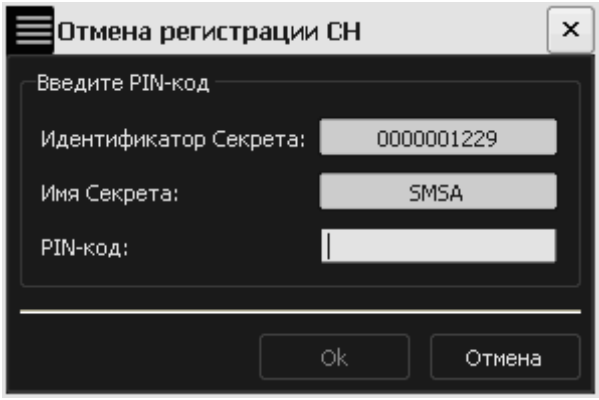

Рисунок 85 – Окно ввода PIN-кода СНСА

При успешном выполнении описанной процедуры на экран выводится сообщение об успешном разблокировании СН (рисунок 86).

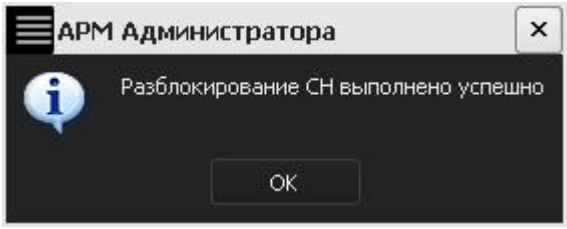

Рисунок 86 – Оповещение об успешной разблокировке СН

По нажатии кнопки <OK> на экран выводится окно с новым PIN-кодом разблокированного СН, который необходимо запомнить или надежно сохранить в недоступном для других лиц месте (рисунок 87). Пользователь может распечатать новый PIN-код посредством нажатия кнопки <Печать>.

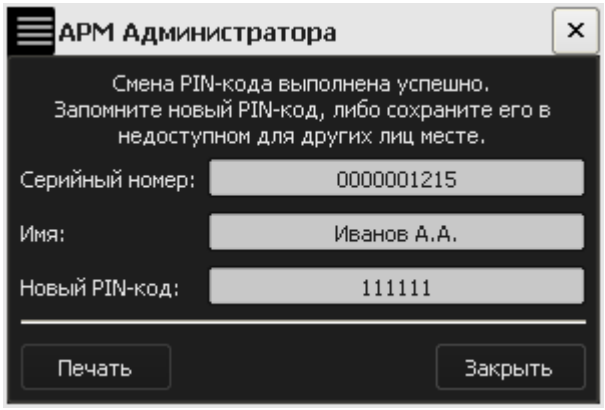

Рисунок 87 – Новый PIN-код разблокированного СН

Если PIN-код не был распечатан, то по нажатии кнопки <Закрыть> на экран выводится предупреждающее сообщение (рисунок 88).

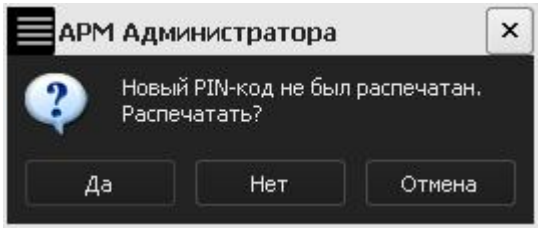

Рисунок 88 – Предупреждающее сообщение

В случае, если печать не требуется, следует нажать кнопку <Нет> или <Отмена>.

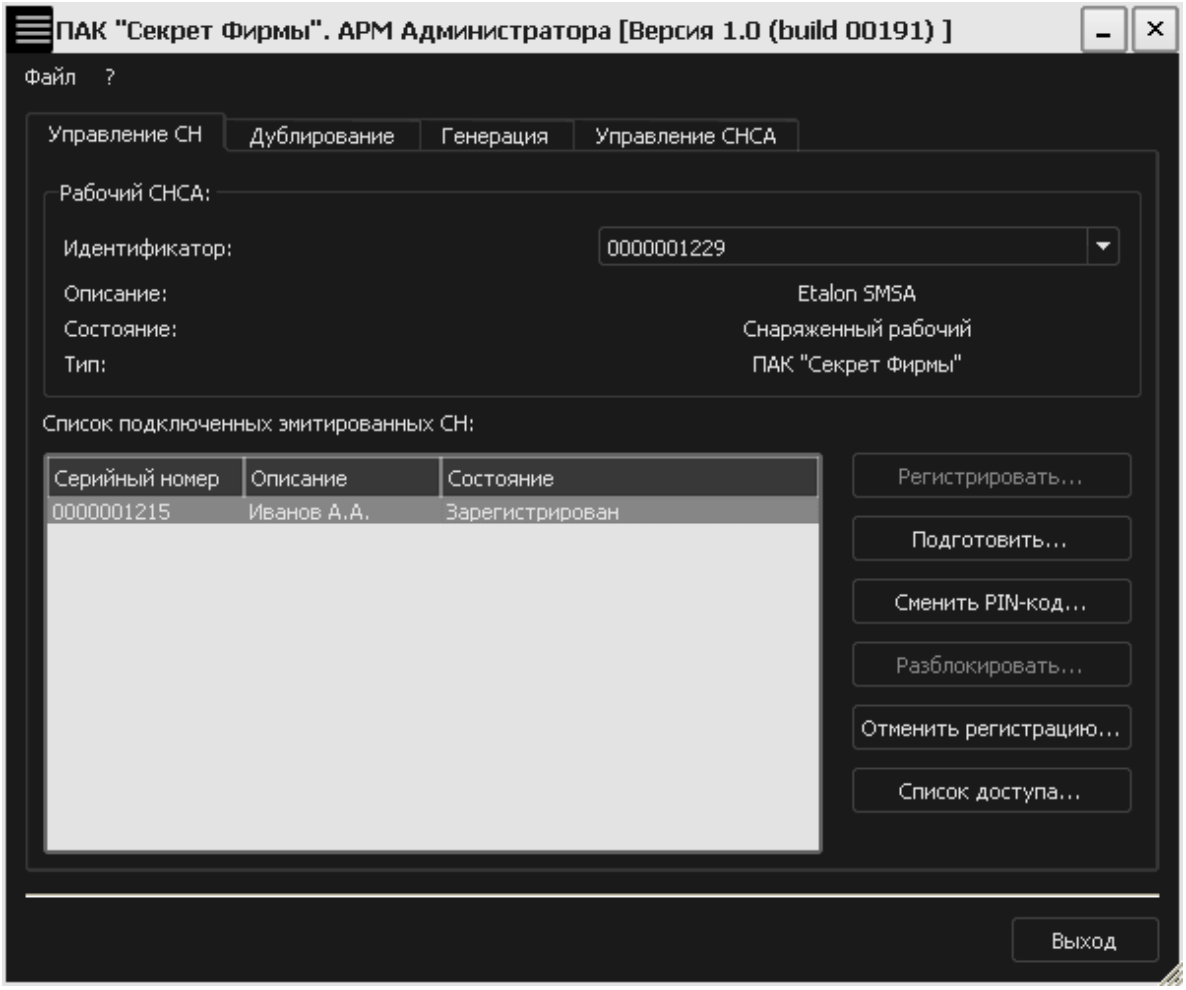

Рисунок 89 – Вкладка «Управление СН» АРМ Администратора

После успешного разблокирования СН его статус во вкладке «Управление СН» АРМ Администратора изменяется на «Зарегистрирован» и управление СН становится возможным (рисунок 89).

3.11 Разблокирование СНСА

В случае трех последовательных неудачных попыток ввода PIN-кода СНСА блокируется и работа с ним становится невозможной. При этом его статус во вкладке «Управление СНСА» изменяется на «Заблокированный» (рисунок 90).

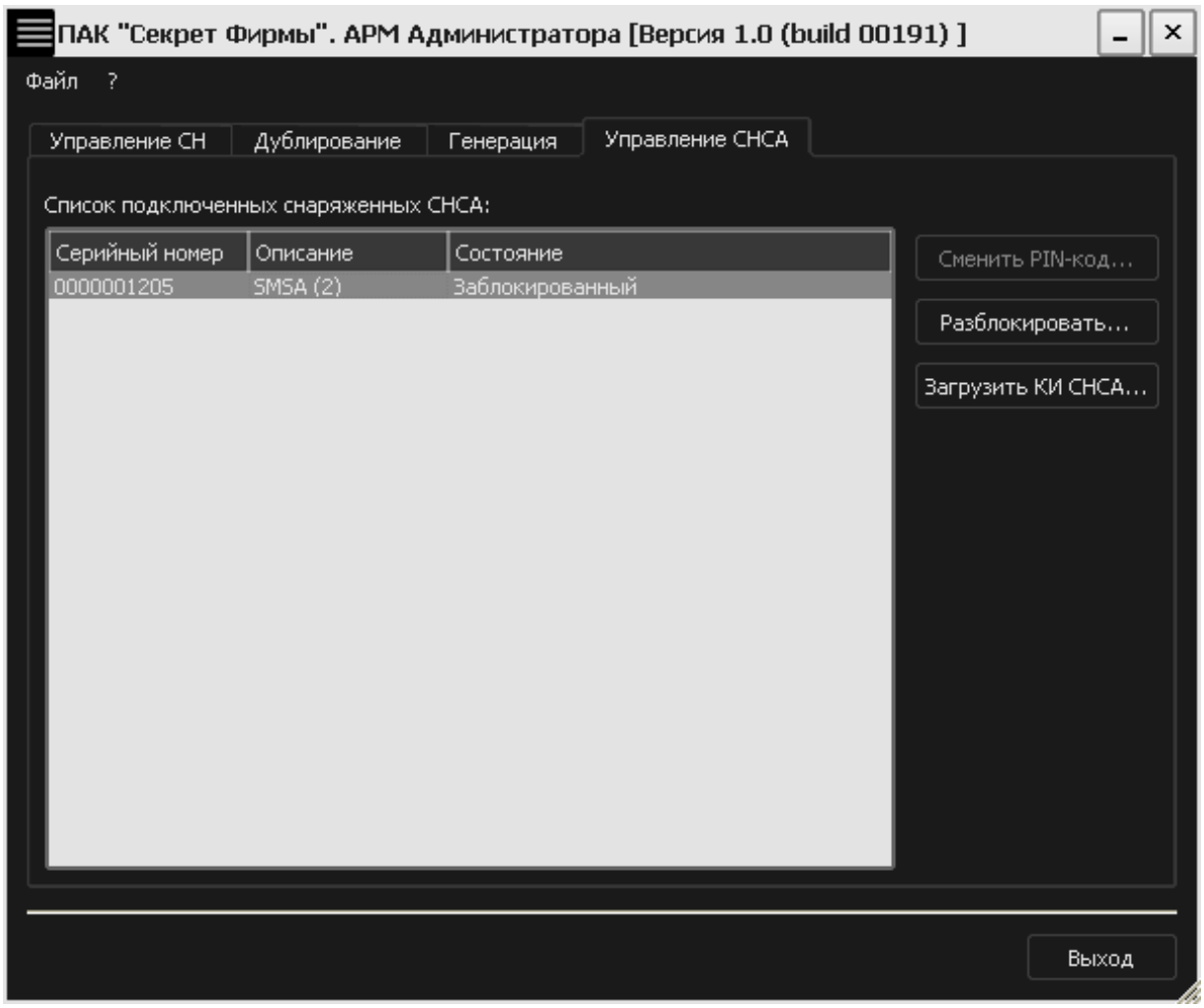

Рисунок 90 - Вкладка «Управление СНСА» АРМ Администратора

Для разблокирования СНСА необходимо выбрать из списка подключенных снаряженных СНСА нужный и нажать кнопку <Разблокировать>.

ВНИМАНИЕ! Во время выполнения операции разблокирования СНСА не отключайте устройство «Секрет» от USB-порта компьютера, т.к. это может привести к нарушению его работоспособности!

В появившемся далее окне следует ввести код регистрации того СНСА, который необходимо разблокировать (рисунок 91).

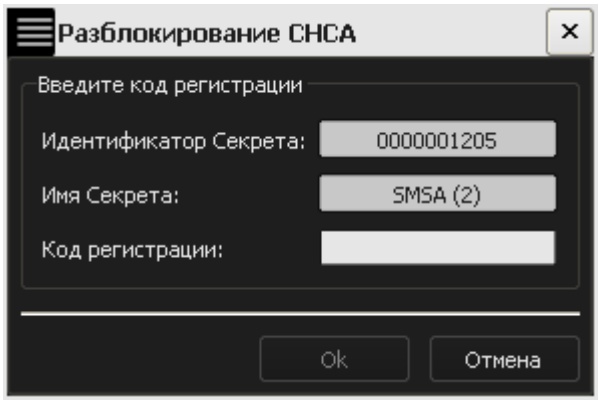

Рисунок 91 – Окно ввода кода регистрации СНСА, который необходимо разблокировать

После корректного ввода кода регистрации на экран выводится сообщение об успешном разблокировании СНСА (рисунок 92).

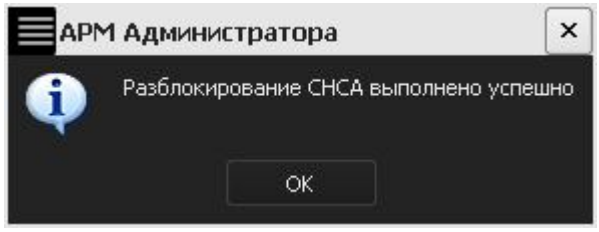

Рисунок 92 – Оповещение о разблокировке СНСА

После нажатия кнопки <OK> на экран выводится сообщение с новым PIN-кодом СНСА, который необходимо запомнить или надежно сохранить (рисунок 93).

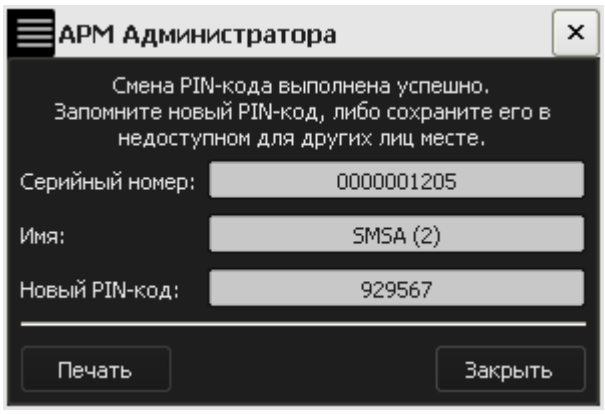

Рисунок 93 – Новый PIN-код разблокированного СНСА

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

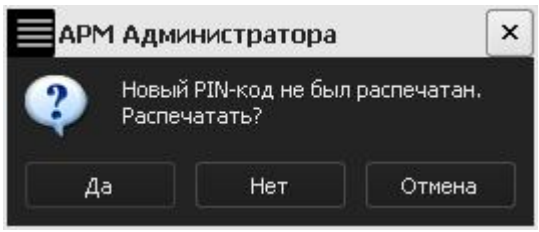

Рисунок 94 – Предупреждающее сообщение

В случае, если печать не требуется, следует нажать кнопку <Нет> или <Отмена>.

После успешного разблокирования управление СНСА становится возможным.

4 Журнал регистрации событий

Для обеспечения возможности мониторинга работы с «Секретами» все производимые действия с СН, зарегистрированными на данной РС, записываются в журнал регистрации событий, окно просмотра которого показано на рисунке 95.

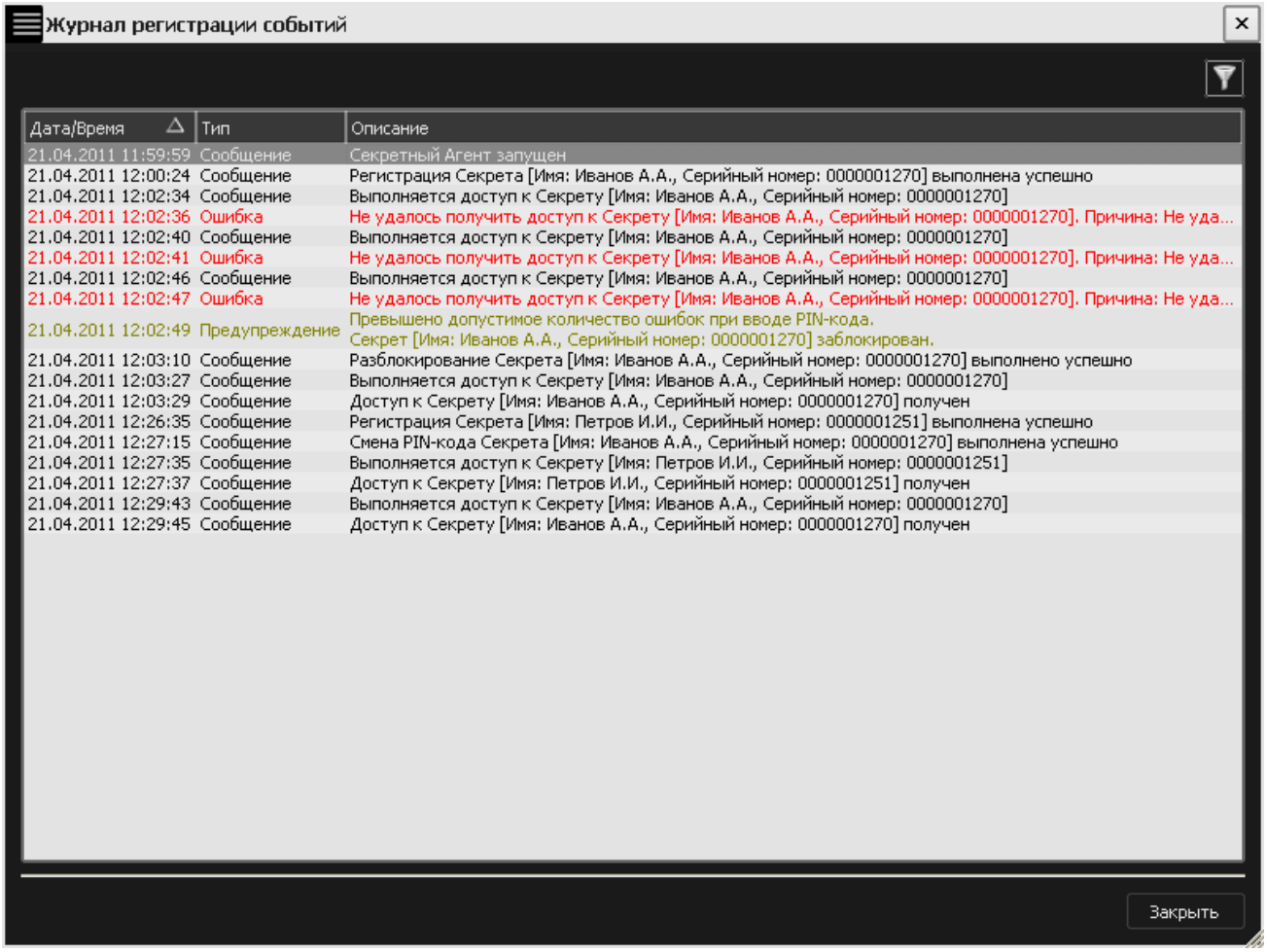

Рисунок 95 – Окно просмотра журнала регистрации событий

Работа с журналом может быть начата посредством выбора пункта «Журнал работы» из контекстного меню приложения «Секретный Агент», вызываемого по щелчку правой кнопки мыши на значке в трее (рисунок 96).

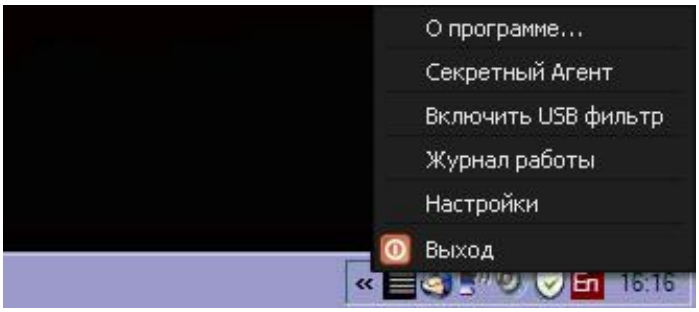

Рисунок 96 - Контекстное меню приложения «Секретный Агент»

Окно просмотра журнала регистрации событий содержит информацию о событиях, зафиксированных в процессе работы пользователя с СН «Секрет Фирмы» на данной РС.

Имеется возможность фильтрации списка для упрощения поиска необходимых событий. Для этого следует в правом верхнем углу журнала нажать кнопку <Фильтр>.

По нажатии кнопки <Фильтр> в окне журнала появляется панель для задания параметров фильтрации (рисунок 97).

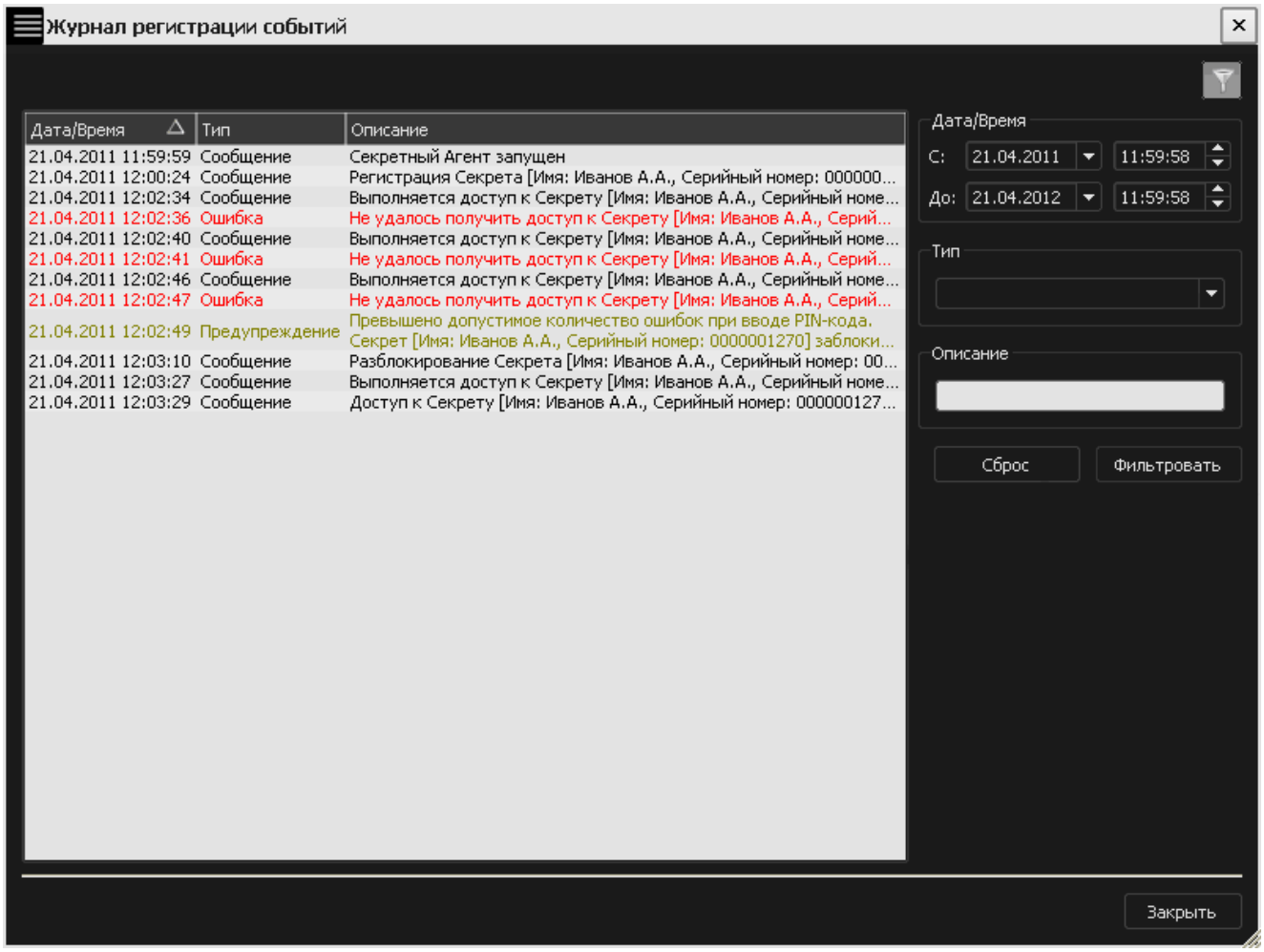

Рисунок 97 – Окно просмотра журнала регистрации событий с панелью для задания параметров фильтрации

Данная панель содержит следующие поля для заполнения:

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

7)«Тип» – поле для выбора типа событий, зафиксированных при работе с СН. 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>;

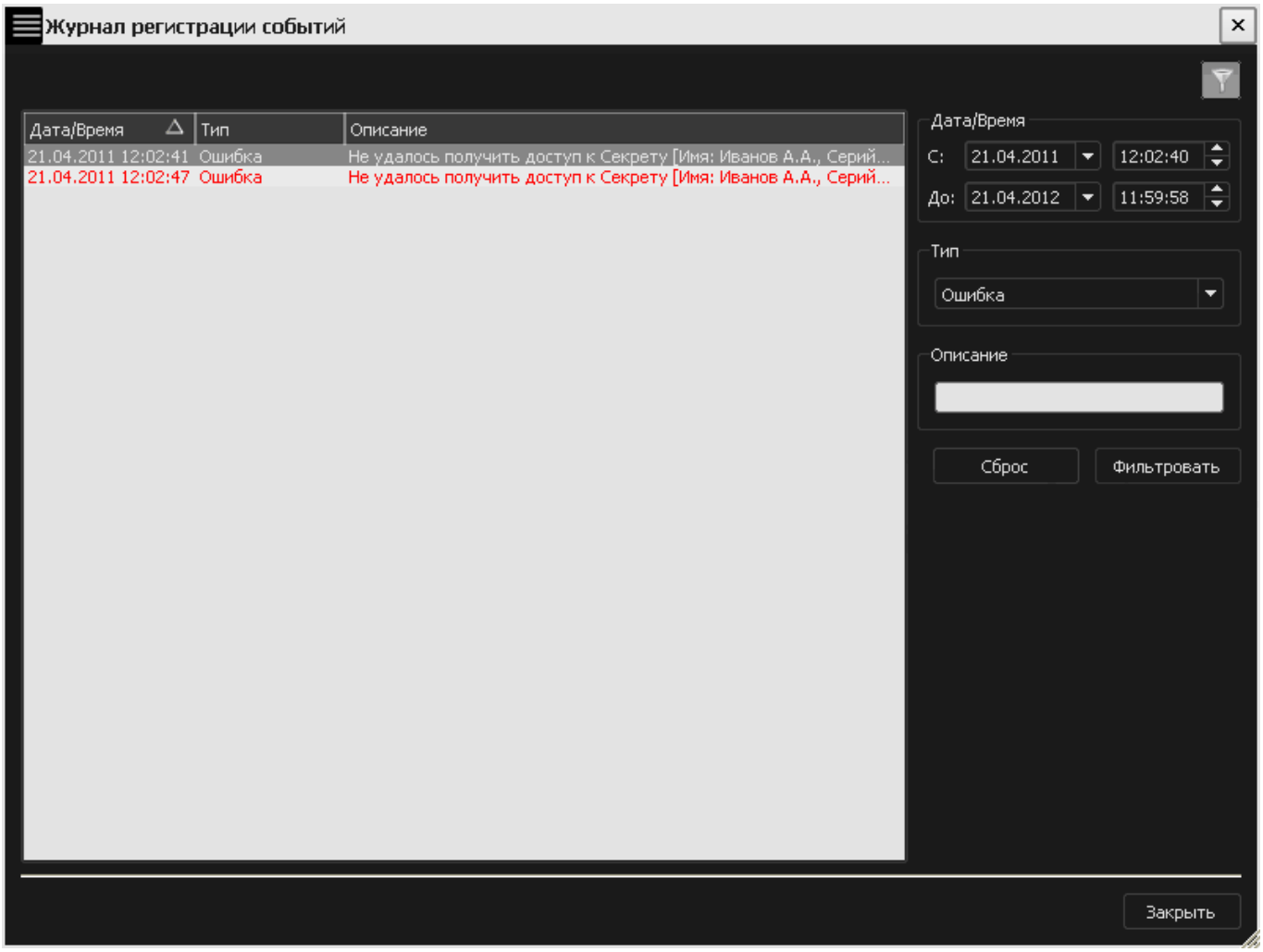

Рисунок 98 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по типу

8) «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, следует заполнить поля «Дата/Время» и «Описание» и нажать кнопку <Фильтровать>. В окне просмотра журнала регистрации событий появится информация о событиях, удовлетворяющих заданным параметрам фильтрации (рисунок 99).

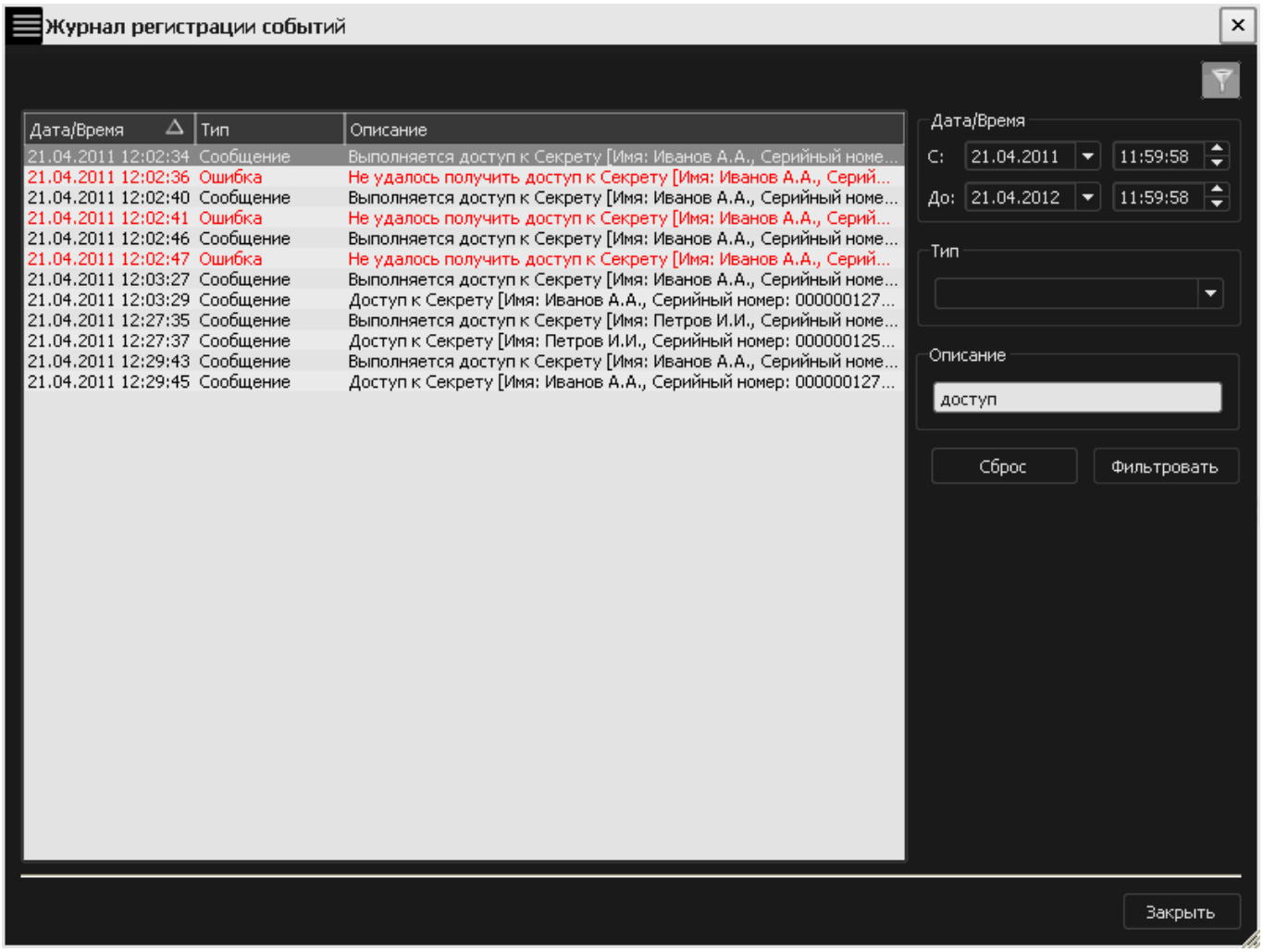

Рисунок 99 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по описанию

Если на данной РС используется несколько зарегистрированных СН «Секрет Фирмы» (рисунок 95), то с помощью фильтрации по описанию можно легко отследить все события, зафиксированные в журнале при работе с конкретным СН, введя в поле «Описание» имя или серийный номер нужного «Секрета» (рисунок 100).

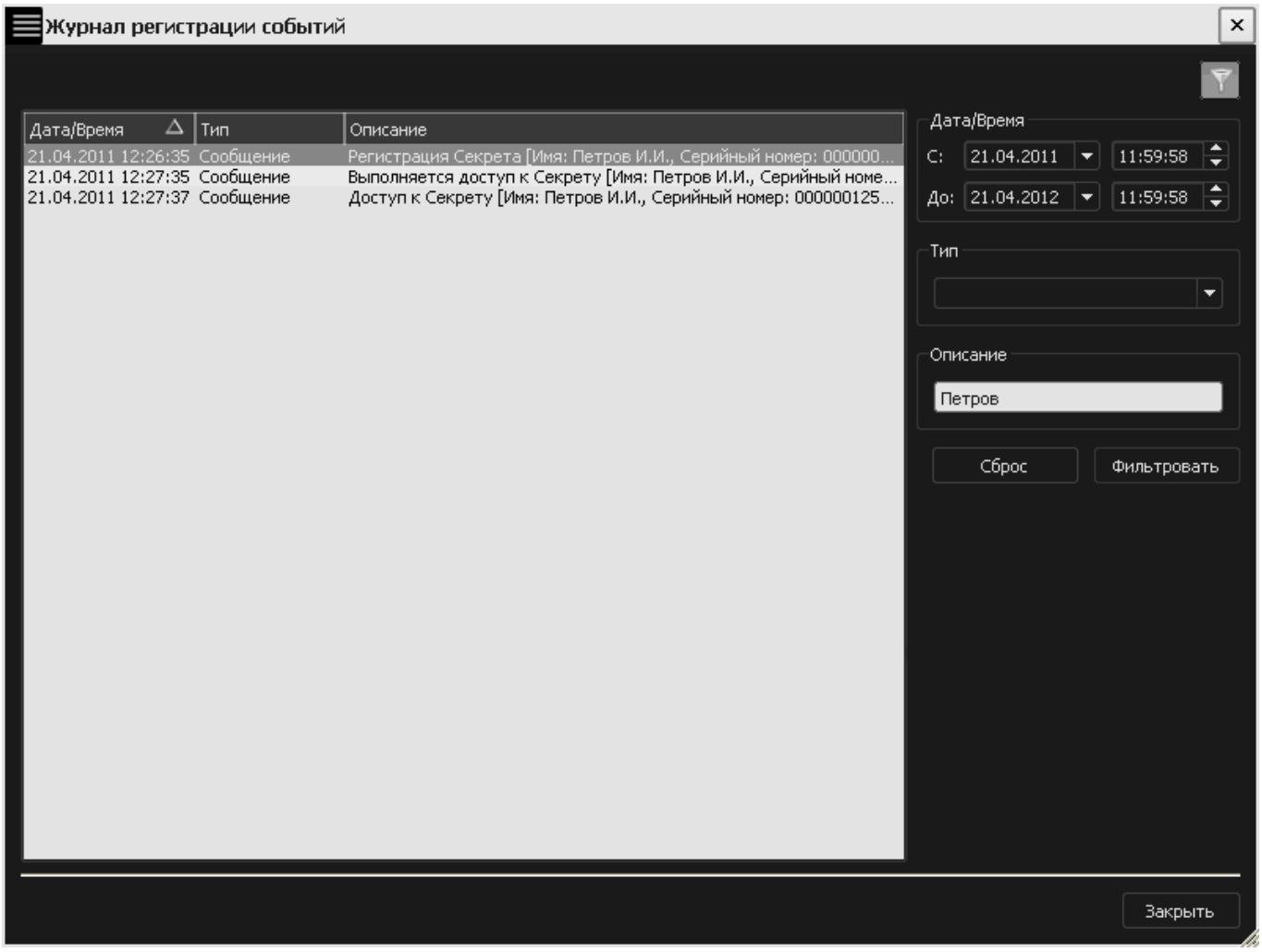

Рисунок 100 - Окно просмотра журнала регистрации событий со списком событий, отфильтрованных по имени СН

5 Рекомендации по организации безопасного применения ПАК «Секрет Фирмы»

5.1 Общие сведения

При применении ПАК «Секрет Фирмы» следует проявлять осторожность в случае, когда пользователь совершает перерывы в работе на РС: 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 он отсутствует на рабочем месте, а сеанс работы с ПАК «Секрет Фирмы» еще не завершен.

Во избежание недоразумений, связанных с ситуациями, когда пользователь забыл заблокировать экран, администратору рекомендуется на рабочих станциях:

- устанавливать вход пользователя в систему с обязательным вводом пароля;
- настраивать автоматическую блокировку экрана РС по истечении заданного периода неактивности.

5.2 Установка входа пользователя в систему с обязательным вводом пароля

Для того чтобы установить вход пользователя в систему с обязательным вводом пароля, необходимо выполнить следующие действия:

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). Данная операция может быть выполнена для рабочих станций, не включенных в домен.

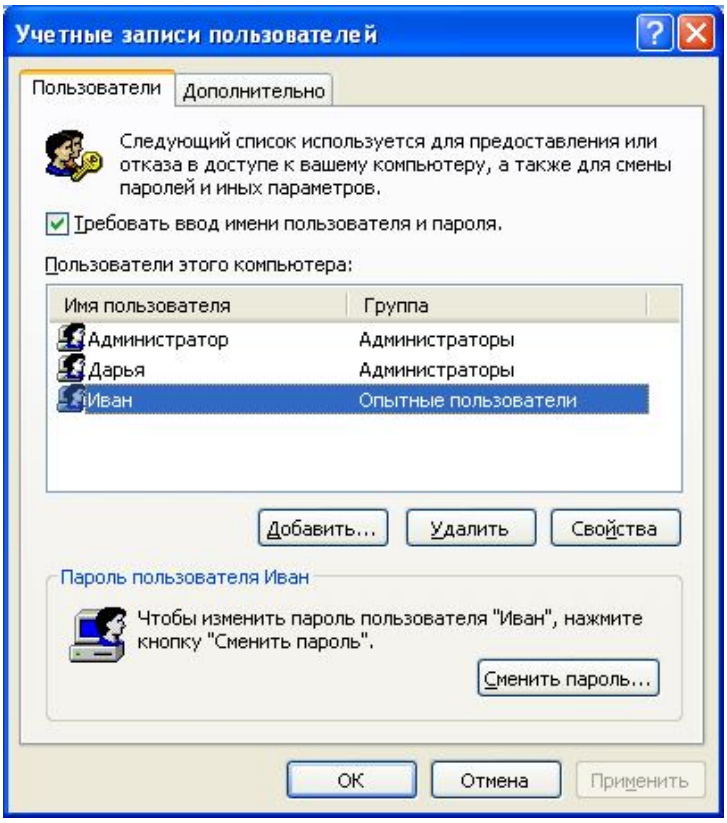

Рисунок 101 – Окно настроек учетных записей пользователей

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).

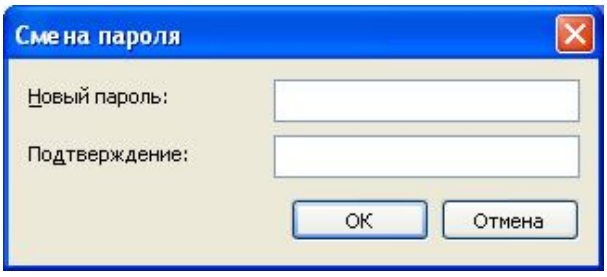

Рисунок 102 – Окно смены пароля пользователя для входа в ОС

5.3 Включение режима автоматической блокировки экрана

Для включения режима автоматической блокировки экрана по истечении заданного периода неактивности следует выполнить следующие действия:

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

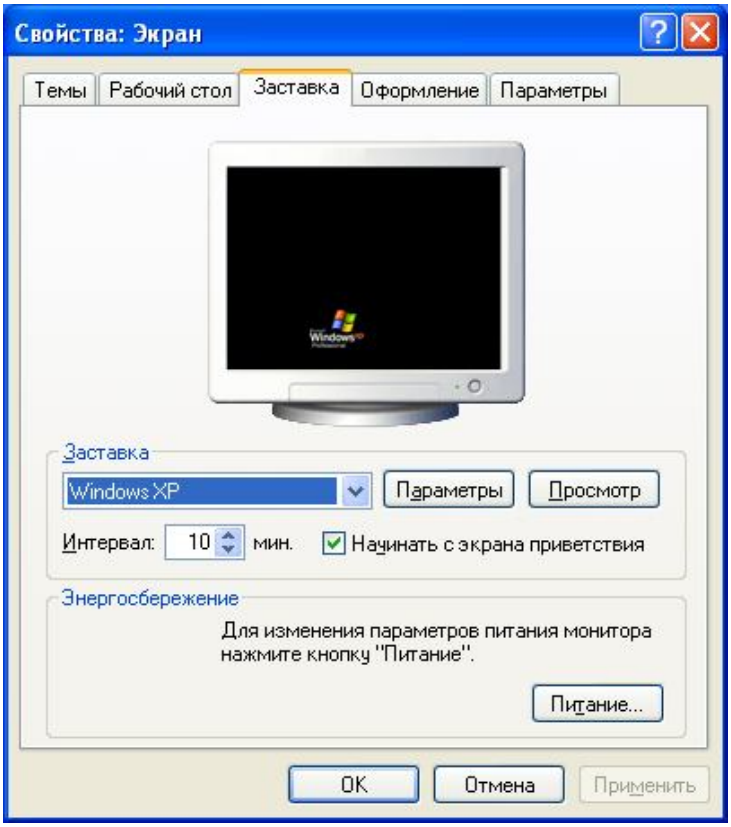

Рисунок 103 – Окно настройки заставки экрана в ОС Windows XP

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

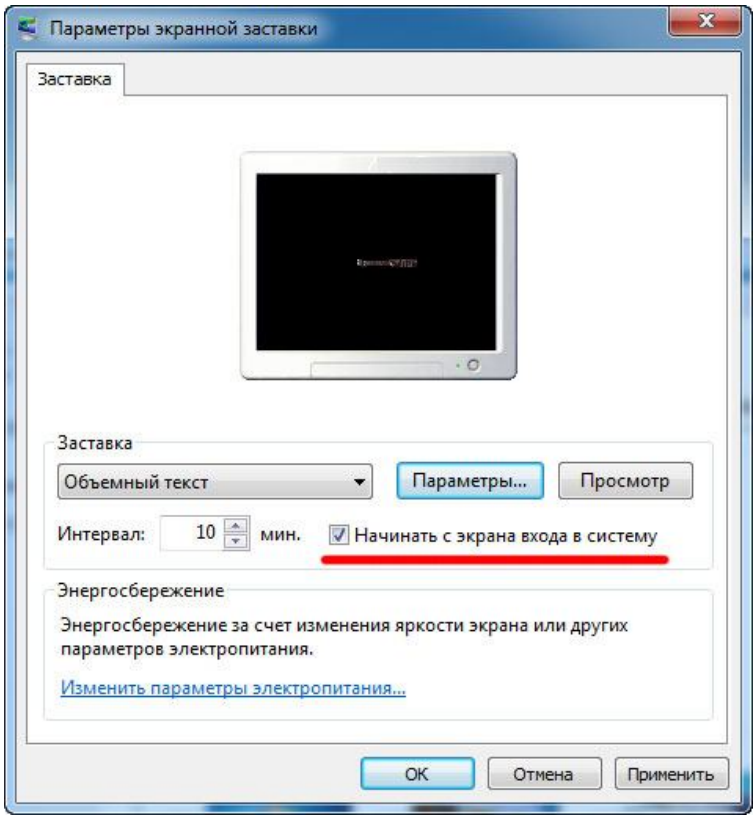

Рисунок 104 - Окно настройки заставки экрана в ОС Windows 7

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 Методы устранения неполадок в работе ПАК «Секрет Фирмы»

При работе на ПЭВМ, оснащенной ПАК «Секрет Фирмы», могут возникать неполадки.

Описание возможных неполадок, причины их появления и порядок действий администратора по их устранению приведены в таблице 1.

Таблица 1 - Возможные неполадки в работе ПАК «Секрет 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	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить дублирование СНСА»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить регистрацию СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить отмену регистрации СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА и код регистрации СН введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен код регистрации СН	
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить смену PIN-кода СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА и PIN-код СН введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен PIN-код СН	
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить разблокирование СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА и код регистрации СН введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен код регистрации СН	
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить смену PIN-кода СНСА»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить разблокирование СНСА»	Неверно введен код регистрации СНСА	Повторить операцию. В случае если код регистрации СНСА введен
	Неисправность устройства	

Описание неполадки	Возможные причины возникновения неполадки	Порядок действий по устранению
	Программная ошибка в процессе выполнения операции	верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
«Не удалось выполнить чтение ключевой информации СНСА»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить подготовку к повторной регистрации СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА и код регистрации СН введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен код регистрации СН	
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Не удалось выполнить повторную регистрацию СН»	Неверно введен PIN-код СНСА	Повторить операцию. В случае если PIN-код СНСА и код регистрации СН введены верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен код регистрации СН	
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«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 РС		
«Не удалось выполнить аутентификацию Секрета [Имя: %1]»	Неверно введен PIN-код СН	Повторить операцию. В случае если PIN-код СН введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«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 РС и СА.
«Соединение с Сервером Аутентификации прервано»	Истекло установленное время ожидания ответа от СА	Повторить операцию
«Доступ к Секрету на данном компьютере запрещен»	Хост, с которого выполняется доступ к Секрету, находится в черном списке на СА	Удалить данный хост из черного списка на СА

Описание неполадки	**Возможные причины возникновения неполадки**	**Порядок действий по устранению**
	Хост, с которого выполняется доступ к Секрету, отсутствует в белом списке 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 СНСА	Выполнить загрузку КИ СНСА в СА
	СНСА отключен от СА	1) Выполнить подключение СНСА к СА. 2) Выполнить загрузку КИ СНСА в СА.
	Закрыто приложение «АРМ Администратора»	1) Запустить приложение «АРМ Администратора». 2) Выполнить загрузку КИ СНСА в СА.
«Секрет не зарегистрирован на Сервере Аутентификации»	Данный СН отсутствует в базе зарегистрированных СН	Зарегистрировать СН 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	Выполнить переустановку ПО РС
«Невозможно выполнить доступ к Секрету. Служба доступа к Серверу Аутентификации не запускается»	Некорректно установлено ПО РС	Выполнить переустановку ПО РС
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.