ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс защищенного хранения информации «Секрет Фирмы»

Руководство пользователя

11443195.4012.032 34

Листов 21

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством пользователя (оператора) 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

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 семейства Microsoft Windows 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 средства 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 СА;
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 АРМ 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/ 7/8/8.1 (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:

– IBM PC совместимая ПЭВМ, работающая под управлением операционной системы Microsoft Windows XP/ 7/ 8/ 8.1/ Server 2003/ Server 2008/ Server 2008 Release 2/ Server 2012/ Server 2012 Release 2 (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:

– IBM PC совместимая ПЭВМ, работающая под управлением операционной системы Microsoft Windows XP/ 7/8/8.1 (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 должен быть установлен комплект необходимого программного обеспечения: ПО Сервера Аутентификации «АРМ Администратора» и ПО Рабочей станции «Секретный Агент» соответственно.

Установка ПО ПАК «Секрет Фирмы» выполняется Администратором в соответствии с «Руководством Администратора» (11443195.4012.032 90).

2.2 Подключение СН

Подключение осуществляется установкой СН в свободный USB-разъем системного блока РС (при получении доступа к данным СН) и СА (при управлении ПАК «Секрет Фирмы»)[1].

[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.

2.3 Установка системного драйвера СН

После установки на жесткий диск ПО ПАК «Секрет Фирмы» (см. подраздел 2.1) при первом подключении устройства «Секрет Фирмы» (см. подраздел 2.2) необходимо выполнить установку системного драйвера СН.

Установка системного драйвера СН выполняется Администратором в соответствии с «Руководством Администратора» (11443195.4012.032 90).

2.4 Порядок работы

До начала использования «Секрета» на РС должен быть установлен комплект необходимого ПО (см. подраздел 2.1), выполнено подключение СН (см. подраздел 2.2) и произведена установка системного драйвера СН (см. подраздел 2.3).

Следующий шаг – процедура первичной регистрации СН, в результате которой формируется PIN–код и код регистрации СН (подробнее об этом см. в подразделе 3.1).

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 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. 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. 3.2).

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 (см. 3.3).

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. 4.1).

3 Управление ПАК «Секрет Фирмы»

3.1 Регистрация СН

До начала использования СН на РС Администратором должно быть установлено ПО ПАК «Секрет Фирмы» и выполнена процедура регистрации СН. (подробнее об этом см. соответствующие разделы «Руководства Администратора» (11443195.4012.032 90)). В результате выполнения данной процедуры формируются PIN–код и код регистрации СН, с использованием которых осуществляются операции получения доступа к данным в «Секрете» и администрирования СН соответственно.

Организационными мерами необходимо исключить возможность ознакомления администратора с регистрационными данными СН «Секрет Фирмы».

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 1, рисунок 2).

Следует помнить о необходимости сохранения этих данных недоступными третьим лицам!

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

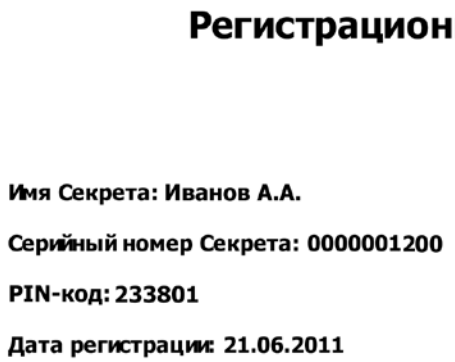

Рисунок 1 – Пример распечатанного PIN-кода СН

Код регистрации СН используется для выполнения операций:

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

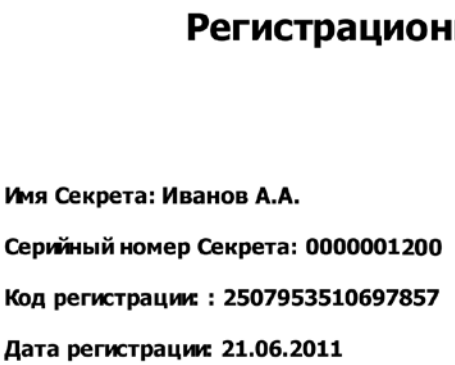

Рисунок 2 – Пример распечатанного кода регистрации СН

В ходе регистрации Администратор задает имя СН «Секрет Фирмы». Имя представляет собой строку, длина которой ограничена 32 произвольными символами. В качестве имени используется 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.

После успешного завершения процедуры регистрации необходимо подготовить СН «Секрет Фирмы» к дальнейшей работе (см. подраздел 3.2).

Для того чтобы иметь возможность применять «Секрет» в других сегментах сети, необходимо выполнить на них его повторную регистрацию (см. подраздел 3.4).

3.2 Подготовка СН к работе

После успешного выполнения регистрации Администратор должен выполнить операции по подготовке СН «Секрет Фирмы» к дальнейшей работе:

- настроить списки доступа (см. 3.2.1);
- настроить сетевые параметры (см. 3.2.2).

3.2.1 Настройка списков доступа

До начала использования СН «Секрет Фирмы» Администратор в соответствии с «Руководством Администратора» (11443195.4012.032 90) 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.

ВНИМАНИЕ! Необходимо помнить, что если по каким-либо причинам требуется изменить имя компьютера, который ранее уже был включен в «белый» список доступа в «Секрете Фирмы», следует выполнить также соответствующую корректировку «белого» списка: удалить из списка запись со старым именем компьютера и добавить запись, содержащую новое имя компьютера.

В случае если имя компьютера изменено, а «белый» список не скорректирован соответствующим образом, пользователь не сможет получить на данном компьютере доступ к СН!

3.2.2 Настройка сетевых параметров

После настройки списков доступа Администратор в соответствии с «Руководством Администратора» (11443195.4012.032 90) должен выполнить на РС настройку сетевых параметров посредством задания (рисунок 3):

- адреса сервера аутентификации;

- порта для взаимодействия с сервером аутентификации;
- времени ожидания отклика. Это время, в течение которого «Секретный Агент» ждет ответа от сервера аутентификации на отправленный им пакет данных.

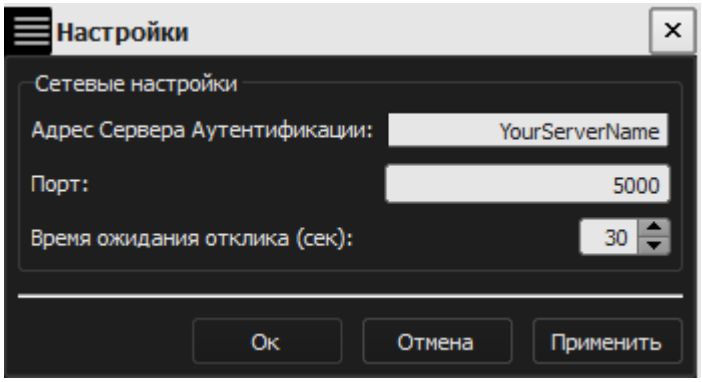

Рисунок 3 – Окно ввода адреса сервера аутентификации

Настройка сетевых параметров выполняется в пункте «Настройки» контекстного меню, вызываемого посредством нажатия правой кнопкой мыши по значку «Секретного Агента» в трее (рисунок 6).

После задания сетевых настроек становится возможным применение СН в сегменте сети, который «привязан» к указанному СА. При этом СН обнаруживается системой, как обычный флеш-накопитель.

3.3 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 в соответствии с «Руководством Администратора» (11443195.4012.032 90) 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».

3.4 Регистрация СН в другом сегменте сети

3.4.1 Подготовка СН к процедуре повторной регистрации

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

Данная операция выполняется Администратором в соответствии с «Руководством Администратора» (11443195.4012.032 90).

В процессе подготовки СН к повторной регистрации формируется мандат регистрации, с помощью которого может быть проведена операция регистрации данного СН на дружественном СНСА.

ВНИМАНИЕ! Повторная регистрация невозможна при отсутствии файла с мандатом регистрации. Поэтому при выполнении процедуры повторной регистрации администратору первичного СА следует обеспечить доступ к данному файлу для администратора дружественного СА (например, скопировать его на любой носитель информации и перенести в дружественный сегмент сети).

3.4.2 Повторная регистрация

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

Данная операция выполняется Администратором дружественного СА в соответствии с «Руководством Администратора» (11443195.4012.032 90).

После выполнения процедуры повторной регистрации становится возможным управление СН.

3.5 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.

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

Процедура отмены регистрации СН выполняется Администратором в соответствии с «Руководством Администратора» (11443195.4012.032 90).

3.6 Смена PIN-кода СН

Если у пользователя СН имеются подозрения о компрометации PIN-кода, имеется возможность сменить действующий PIN-код на новый.

Смена PIN-кода проводится при участии Администратора в соответствии с «Руководством Администратора» (11443195.4012.032 90) с использованием старого значения PIN-кода.

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.

3.7 Разблокирование СН

В случае трех последовательных неудачных попыток ввода PIN-кода СН блокируется и на экран выводится соответствующее сообщение (рисунок 4).

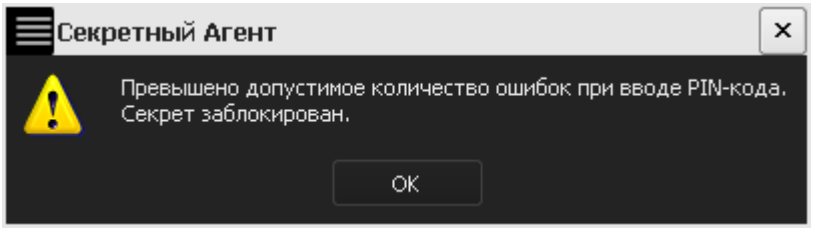

Рисунок 4 – Оповещение о блокировке СН

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

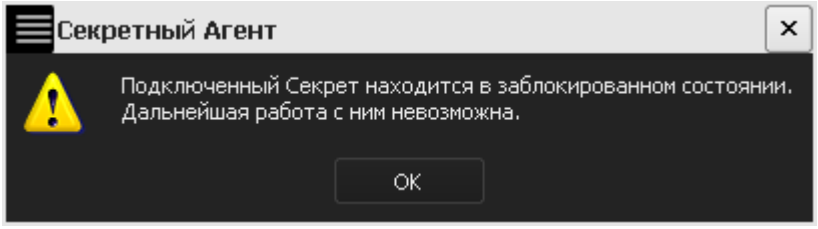

Рисунок 5 – Оповещение при подключении к USB-порту компьютера о блокировке СН

Процедура разблокирования СН проводится с участием Администратора в соответствии с «Руководством Администратора» (11443195.4012.032 90) с использованием кода регистрации, полученного в результате выполнения первичной регистрации СН (см. подраздел 3.1).

После успешного разблокирования применение СН становится возможным.

4 Применение ПАК «Секрет Фирмы»

4.1 Получение доступа к данным СН

«Секрет» используется точно так же, как и обыкновенный USB-накопитель. Отличие состоит только в процедуре получения доступа к данным, хранящимся в «Секрете».

После установки комплекта ПО ПАК «Секрет Фирмы» при загрузке ОС производится автоматический запуск приложения «Секретный Агент», предназначенного для управления доступом к данным СН. При этом в трее появляется соответствующий значок (рисунок 6). «Секретный Агент» также может быть запущен вручную (например, если он был по каким-либо причинам закрыт) посредством выбора пункта меню Пуск → Программы → Секрет Фирмы → Рабочая Станция → Секретный Агент.

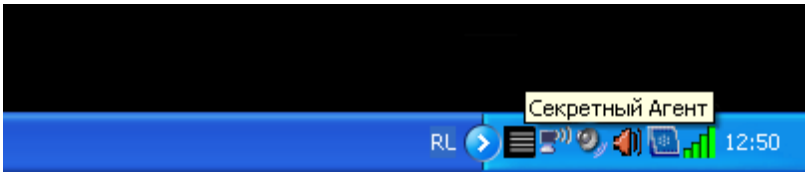

Рисунок 6 - Значок приложения «Секретный агент» в трее

Для получения доступа к данным, хранящимся в «Секрете», необходимо убедиться в том, что приложение «Секретный Агент» запущено. Пользователь должен подключить СН к USB-порту компьютера – так же, как любое USB-устройство. При этом допускается использование USB-хаба с собственным источником питания (см. 1.3).

ВНИМАНИЕ! Для того чтобы пользователи могли пользоваться своими «Секретами», к USB-порту СА Администратором обязательно должен быть подключен СНСА!

Если «Секрет» ранее был зарегистрирован в сегменте сети, к которому относится данная РС (подробнее об этом см. в разделах 3.1 и 3.4), после его подключения на экран автоматически выводится окно с запросом PIN-кода (рисунок 7). В появившемся окне пользователь должен ввести PIN-код, сформированный на этапе первичной регистрации СН (см. раздел 3.1) или полученный в результате смены PIN-кода (см. раздел 3.6).

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

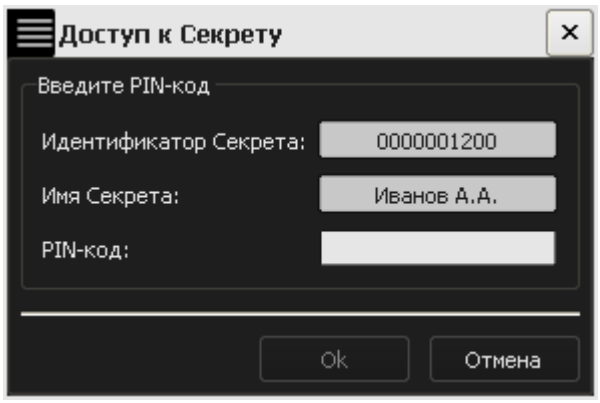

Рисунок 7 – Окно для ввода PIN-кода СН

После нажатии кнопки <OK> в зависимости от результата выполнения необходимых проверок предоставляется доступ к данным СН или производится отказ в доступе.

В случае успешного выполнения проверок на экран выводится информационное сообщение (рисунок 8) и СН предоставляет доступ к данным. Работать с данными при этом можно точно так же, как в случае с обычным USB флеш-накопителем («флешкой»).

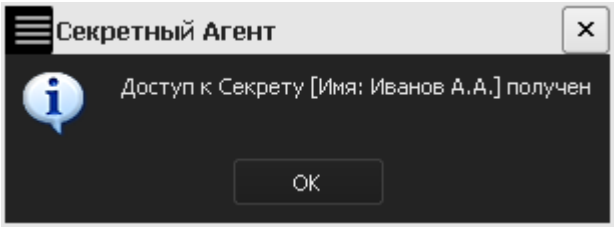

Рисунок 8 – Сообщение об успешном завершении процедуры получения доступа

Если PIN-код введен неверно, то на экран выводится сообщение о том, что доступ к «Секрету» получить не удалось (рисунок 9).

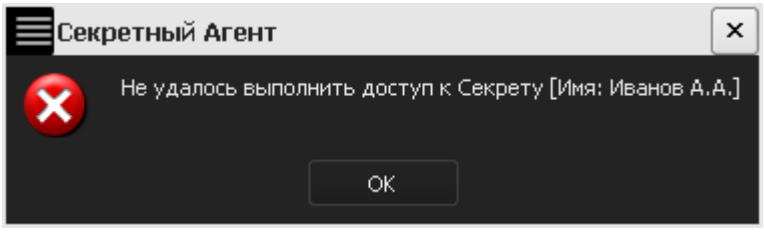

Рисунок 9 - Сообщение об отказе в получении доступа

ВНИМАНИЕ! В случае трех подряд неудачных попыток ввода PIN-кода СН блокируется. Его разблокирование может быть выполнено при участии Администратора с использованием кода регистрации СН (см. 3.7).

ВНИМАНИЕ! В случае если процедура получения доступа к данным СН производится впервые после регистрации, то после нажатия кнопки <OK> (рисунок 8) и попытки открыть диск СН (рисунок 10) на экран выводится

запрос на проведение операции форматирования закрытого диска, которая является частью процесса первой авторизации (рисунок 11).

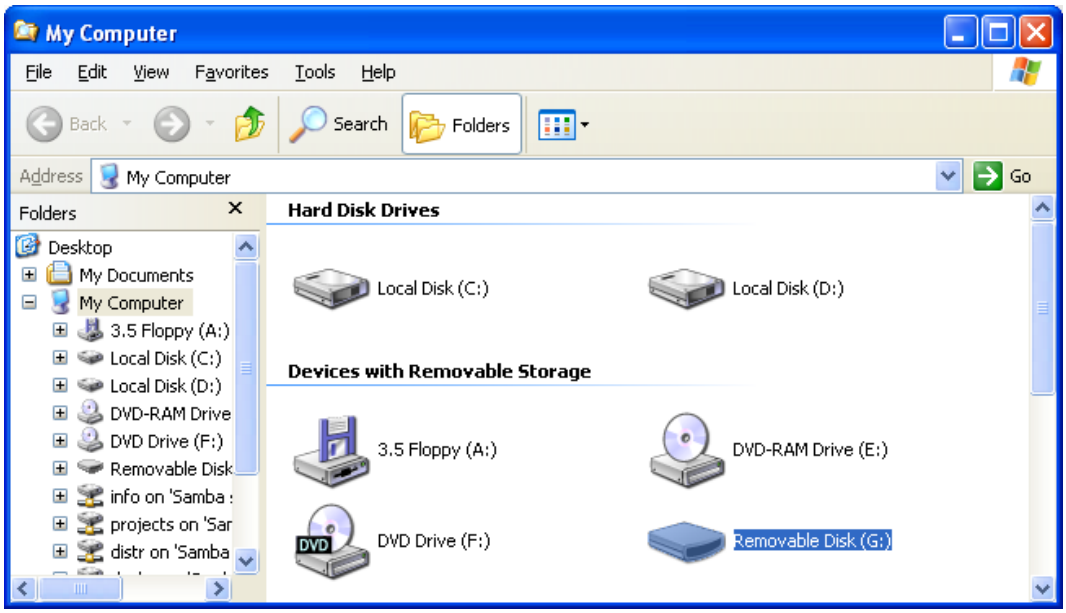

Рисунок 10 – Отображение диска СН в окне файлового менеджера

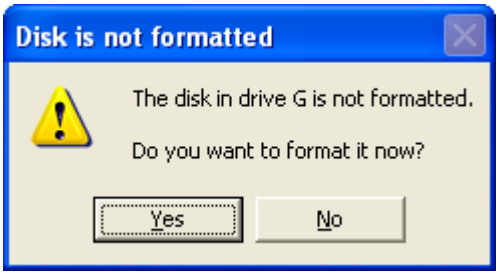

Рисунок 11 – Запрос на форматирование диска СН при первом получении доступа

Следует нажать кнопку <Да> (<Yes>). На экран выводится окно форматирования диска.

В случае отсутствия настоятельной необходимости в выполнении процедуры полного форматирования, в целях экономии времени **рекомендуется выполнять быстрое форматирование диска СН**, установив в окне форматирования галочку «Быстрое» («Quick Format») и нажав кнопку <Старт> (<Start>) (рисунок 12).

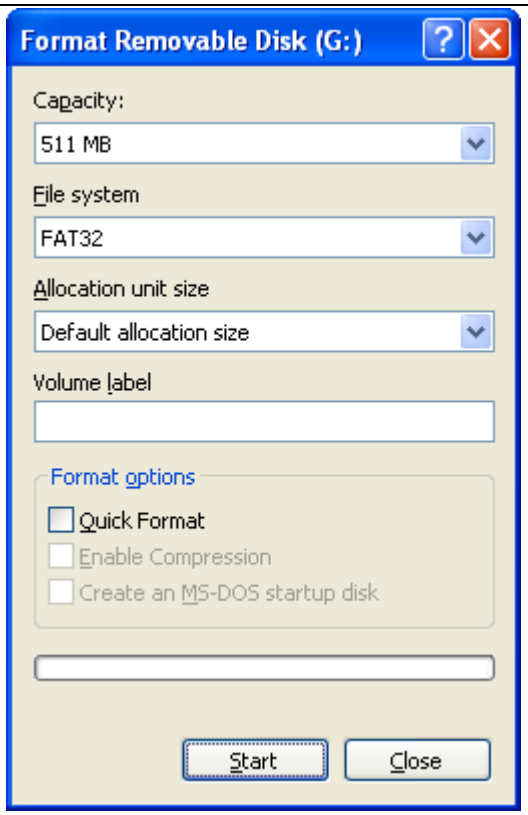

Рисунок 12 – Окно форматирования диска

В появившемся далее окне с предупреждением о том, что после форматирования все записанные на диске данные будут потеряны, следует нажать кнопку <OK> (рисунок 13).

Рисунок 13 – Предупреждающее сообщение

Начнется процесс форматирования диска CH, после успешного завершения которого на экран выводится соответствующее сообщение (рисунок 14).

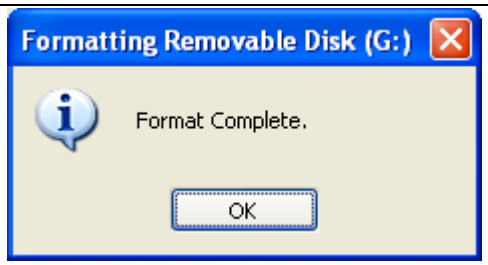

Рисунок 14 – Сообщение об успешном завершении процедуры форматирования диска

После успешного выполнения описанной последовательности действий доступ к диску СН может быть получен.

Если по каким-либо причинам уже после подключения «Секрета» к компьютеру, доступ к данным пользователя необходимо отложить, можно нажать кнопку <Отмена> (рисунок 7) и выполнить процедуру позднее описанным ниже образом.

Главное окно приложения «Секретный Агент» может быть активировано по двойному щелчку левой кнопкой мыши на значке в трее (рисунок 6). Внешний вид главного окна приведен на рисунке 15.

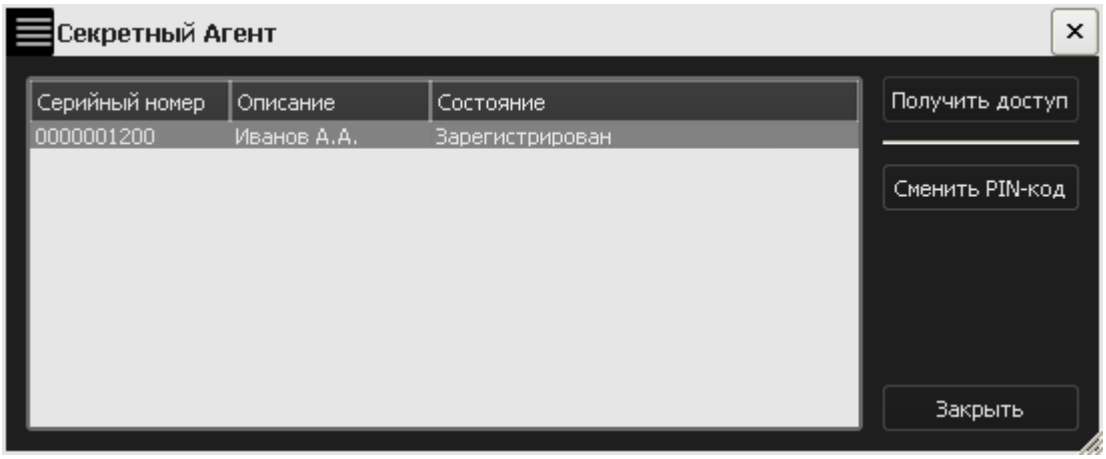

Рисунок 15 - Главное окно приложения «Секретный Агент»

Главное окно «Секретного Агента» содержит список подключенных СН с указанием имени, серийного номера и статуса. Доступ к данным в «Секрете» можно получить, выбрав соответствующий «Секрет» в списке и нажав кнопку <Получить доступ>.

Кнопка <Получить доступ> неактивна (и, следовательно, невозможен доступ к данным в «Секрете») в том случае, если СН не зарегистрирован на данной РС (на это указывает статус «Не зарегистрирован»).

После нажатия кнопки <Получить доступ> на экране появляется окно с предложением ввода PIN-кода, показанное на рисунке 7. Главное окно «Секретного агента» может быть скрыто посредством нажатия кнопки <Закрыть>.

Оперативное выполнение функций «Секретного Агента» может быть осуществлено из контекстного меню приложения, вызываемого по щелчку правой кнопки мыши на значке в трее (рисунок 16).

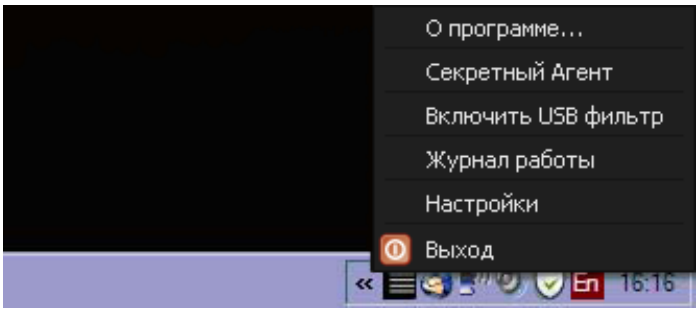

Рисунок 16 - Контекстное меню приложения «Секретный Агент»

Контекстное меню «Секретного Агента» содержит:

- пункт <О программе…> для вызова окна, содержащего информацию о «Секретном Агенте»;
- пункт <Секретный Агент> для вызова главного окна «Секретного Агента»;
- пункт включения/выключения фильтра USB устройств[1];
- пункт для вызова журнала регистрации событий (подробнее о журнале регистрации событий см. в подразделе 4.2);
- пункт «Настройки» (только при наличии аутентификации в системе с правами администратора);
- пункт для завершения работы приложения «Секретный Агент».

При выборе в контекстном меню пункта <О программе> на экран выводится информационное окно приложения «Секретный Агент», содержащее сведения об используемой версии ПАК «Секрет Фирмы», а также контактные данные службы технической поддержки.

При выборе в контекстном меню пункта <Секретный Агент> на экране отображается главное окно приложения «Секретный Агент».

При выборе в контекстном меню пункта <Включить USB фильтр> запрещается использование в системе всех устройств USB Mass Storage за исключением устройств «Секрет». Пользователь может отключить фильтр, выбрав в контекстном меню пункт <Выключить USB фильтр>.

Пункт <Настройки> контекстного меню предназначен для указания сетевых настроек (см. подраздел 3.2.2).

Работа приложения «Секретный Агент» может быть завершена посредством выбора в контекстном меню пункта <Выход>.

[1] Для отображения этого пункта в Windows XP необходимо запустить приложение «Секретный Агент» под учетной записью пользователя, входящего в группу «Администраторы». В ОС Windows 7 и выше необходимо запустить приложение «Секретный Агент» с опцией «run as administrator» и пройти процедуру идентификации в качестве Администратора ОС.

4.2 Журнал регистрации событий

Для отслеживания процесса работы с «Секретами» все производимые действия с СН, зарегистрированными на данной РС, записываются в журнал регистрации событий.

Журнал регистрации может быть использован для установления причин при возникновении ошибок в процессе работы с СН. В случае возникновения неполадок в работе СН следует обратиться к администратору СА.

Порядок работы с журналом регистрации событий описан в «Руководстве Администратора» (11443195.4012.032 90).

5 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

6 Методы устранения неполадок в работе ПАК «Секрет Фирмы»

При работе на ПЭВМ, оснащенной ПАК «Секрет Фирмы», могут возникать ситуации, при появлении которых комплекс выдает сообщения.

Выводимые на экран монитора сообщения, причины их появления и порядок действий пользователя по ним приведены в таблице 1.

Таблица 1 - Сообщения программных средств комплекса и порядок действий администратора

Сообщение на экране	Возможные причины появления сообщения	Порядок действий
«Не удалось выполнить аутентификацию Секрета [Имя: %1]»	Неверно введен PIN-код СН	Ввести верный PIN-код СН
	Неисправность устройства	Повторить операцию. В случае если PIN-код СН введен верно, но сообщение на экране появляется снова, следует вызвать Администратора ПАК «Секрет Фирмы»
	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) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор проверит, запущен ли СА (компьютер, на котором установлено ПО СА) и проверит наличие сетевого

Сообщение на экране	**Возможные причины появления сообщения**	**Порядок действий**
		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	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор удалит данный хост из черного списка на СА.
	Хост, с которого выполняется доступ к Секрету, отсутствует в белом списке на СА	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор добавит 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.	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор выполнит загрузку КИ СНСА в СА.
	СНСА отключен от СА	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор выполнит подключение СНСА к СА и выполнит загрузку КИ СНСА в СА.
	Закрыто приложение «АРМ Администратора»	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор запустит приложение «АРМ Администратора» и выполнит загрузку КИ СНСА в СА.
«Секрет не зарегистрирован на Сервере Аутентификации»	Данный СН отсутствует в базе зарегистрированных СН.	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) С помощью администратора зарегистрировать СН на данном СА.
«Прервана передача данных на Сервер Аутентификации»	Соединение было разорвано	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор устранит причину разрыва соединения.
«Невозможно выполнить доступ к Секрету. Служба доступа к Серверу Аутентификации не установлена»	Некорректно установлено ПО РС	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор выполнит переустановку ПО РС.
«Невозможно выполнить доступ к Секрету. Служба доступа к Серверу Аутентификации не запускается»	Некорректно установлено ПО РС	1) Вызвать Администратора ПАК «Секрет Фирмы». 2) Администратор выполнит переустановку ПО РС.