ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс защищенного хранения информации «Секрет Особого Назначения» (версия 1.0)

Руководство администратора

11443195.4012.033-90

Листов 43

Москва
2012

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса «Секрет Особого Назначения» v.1.0 (далее по тексту – ПАК «Секрет Особого Назначения», либо «Секрет Особого Назначения»), предназначенного для защищенного хранения корпоративной или личной информации конфиденциального характера и обеспечивающего контролируемый доступ к защищаемой информации со стороны авторизованного пользователя в соответствии с политиками доступа, установленными администратором.

ПАК «Секрет Особого Назначения» предназначен как для корпоративного, так и для личного использования.

При корпоративном использовании функции Администратора ПАК «Секрет Особого Назначения» выполняются назначенным должностным лицом, обладающим необходимыми знаниями и полномочиями.

В случае личного использования владелец одновременно является и Пользователем (оператором), и Администратором ПАК «Секрет Особого Назначения».

В документе описан порядок установки и настройки ПАК «Секрет Особого Назначения», а также приведено описание функций, связанных с его администрированием.

Перед установкой и эксплуатацией ПАК «Секрет Особого Назначения» необходимо внимательно ознакомиться с настоящим руководством.

Применение ПАК «Секрет Особого Назначения» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ.

СОДЕРЖАНИЕ

1. Общие сведения

1.1. Состав и назначение ПАК «Секрет Особого Назначения»

ПАК «Секрет Особого Назначения» включает:

1) специальный носитель «Секрет Особого Назначения» (СН);

2) программное обеспечение (ПО) рабочей станции (РС) «Секретный Агент», которое содержится на открытом разделе флеш-диска СН:

драйвер USB-устройства для работы в составе операционной системы (ОС);

приложения для управления доступом к данным СН.

СН представляет собой аппаратный модуль, выполненный по технологии флеш-диска с интерфейсом USB, предназначенный для хранения пользовательской информации (включая информацию конфиденциального характера). Основными элементами данного аппаратного модуля являются:

1) микроконтроллер со внутренней памятью, используемой для хранения внутреннего ПО СН и служебной информации;

2) физический датчик случайных чисел (ДСЧ);

3) энергонезависимая флеш-память, используемая для хранения пользовательской информации, а также журнала событий и ПО РС.

ПАК «Секрет Особого Назначения» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64).

ПАК «Секрет Особого Назначения» предназначен для защищенного хранения корпоративной или личной информации конфиденциального характера и обеспечивает контролируемый доступ к защищаемой информации со стороны авторизованного пользователя в соответствии с политиками доступа, установленными администратором. Основные особенности ПАК «Секрет Особого Назначения»:

- ПО РС «Секрета Особого Назначения» размещается на открытом диске СН и исполняется без установки на жесткий диск РС;
- предусмотрена возможность задания правил доступа к защищаемой информации посредством настройки политик;
- ведется журнал работы СН, содержащийся на закрытом разделе флеш-диска СН.

1.2. Технические условия применения комплекса

Для работы с ПАК «Секрет Особого Назначения» необходим следующий минимальный набор технических и программных средств:

- установленная на РС ОС Microsoft Windows XP SP3/Vista/7 SP1 (x32 или x64);
- свободный разъем USB.

ВНИМАНИЕ! Для подключения к ПЭВМ двух или более СН может использоваться USB-хаб. В этом случае USB-хаб должен быть оснащен внешним источником питания.

1.3. Комплектность поставки ПАК «Секрет Особого Назначения»

ПАК «Секрет Особого Назначения» поставляется в составе:

- СН;
- гарантийный талон;
- комплект упаковки.

2. Установка и настройка ПАК «Секрет Особого Назначения»

2.1. Подключение СН

Подключение осуществляется установкой СН в свободный USB-разъем системного блока РС[1]. При этом допускается использование USB -хаба с внешним источником питания (см. 1.2).

2.2. Установка системного драйвера СН

При первом подключении СН к USB-порту ОС обнаруживает новое устройство (рисунок 1).

Рисунок 1 - Оповещение об обнаружении СН

Далее происходит установка системного драйвера:

- если на РС установлена ОС Windows Vista/7, системный драйвер, как правило, устанавливается автоматически;
- если на РС установлена ОС Windows XP, необходимо установить обновление Microsoft для устройства чтения карт USB (KB967048-v2). Его можно получить с использованием механизмов, предусмотренных Microsoft для распространения обновлений, а в случае отсутствия такой возможности – запустить с открытого раздела диска СН.

2.3. Запуск ПО РС

ПО РС записывается на открытый диск СН при изготовлении. Для работы с ПО не требуется его установка на РС.

Внутреннее ПО СН разрешает доступ к открытому диску только для чтения.

В состав ПО РС входят два приложения:

- консоль администратора;
- консоль пользователя.

При подключении СН к USB-разъему РС автоматически монтируется открытый диск СН (рисунок 2). После этого консоль администратора может быть запущена администратором на исполнение.

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

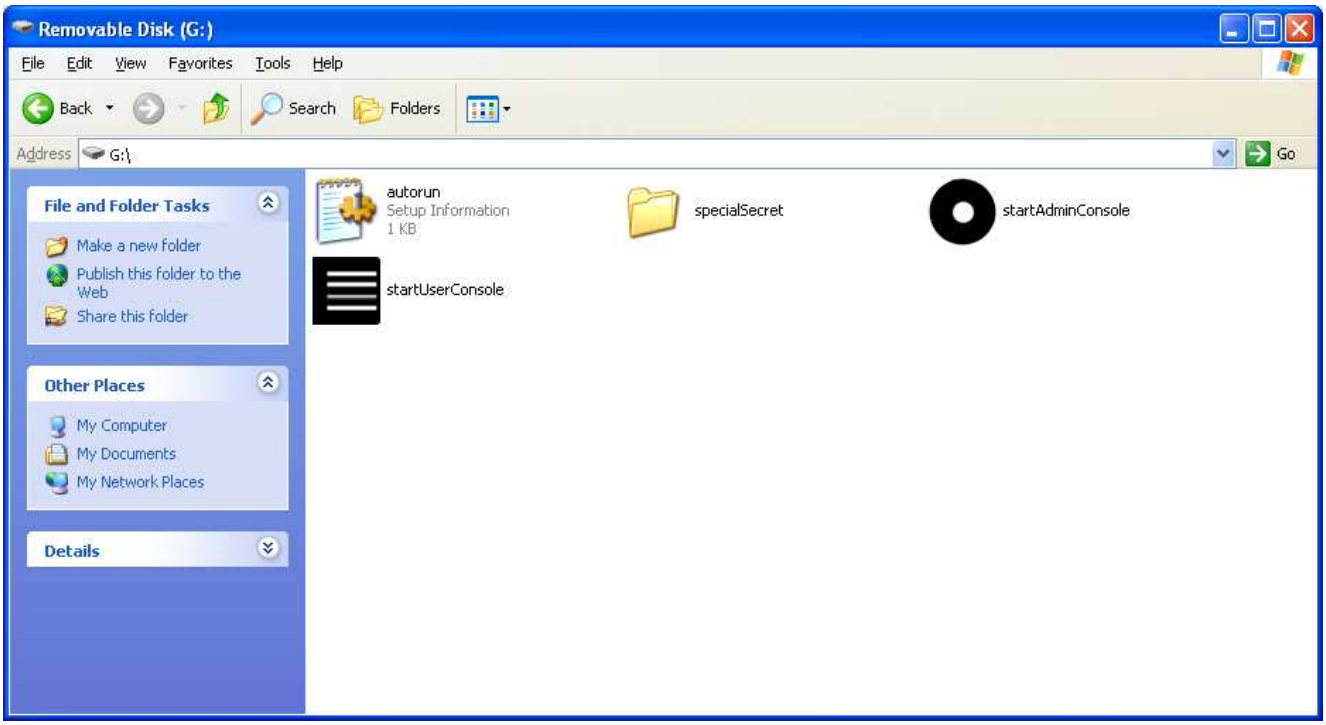

Рисунок 2 – Содержимое открытого раздела флеш-диска СН

2.4. Начало работы

До начала использования ПАК «Секрет Особого Назначения» на РС должно быть выполнено подключение СН (допускается использование USB–хаба с внешним источником питания, см. подраздел 2.1), произведена установка системного драйвера СН (см. подраздел 2.2).

ВНИМАНИЕ! Для корректного совместного функционирования ПАК «Секрет Особого Назначения» и СЗИ НСД «Аккорд» необходимо в редакторе ПРД (утилита ACED32.exe из состава ПО ПАК «Аккорд-Win32» (Аккорд-Win64)) добавить СН (устройство с VID 17E4 и PID 0017) в список разрешенных USB-устройств: либо прописать VID 17E4 и PID 0017 СН вручную, либо снять галку «Показывать только подключенные устройства». В последнем случае СН будет виден в списке всех USB-устройств системы, и появится возможность добавить СН в список разрешенных USB-устройств посредством нажатия кнопки <Добавить> (подробнее см. подраздел 6.15. документа «ПАК СЗИ НСД «АККОРД-Win32». Установка правил разграничения доступа. Программа ACED32» или подраздел 6.15 документа «ПАК СЗИ НСД «АККОРД-Win32». Установка правил разграничения доступа. Программа ACED32»).

Следующий шаг – запуск ПО РС (консоли администратора) (см. 2.3). Консоль администратора не может быть запущена на исполнение в рамках терминальной сессии.

Далее выполняются процедуры регистрации администратора (см. 3.1) и пользователя СН (см. «Руководство пользователя» 11443195.4012.033-34), в результате выполнения которых формируются пароль администратора и код

авторизации пользователя (КА). Эти процедуры выполняются один раз, в рабочем режиме повторять их не требуется.

ВНИМАНИЕ! Консоль пользователя и консоль администратора не могут быть запущены на исполнение одновременно! При попытке запустить консоль пользователя при работающей консоли администратора на экране появляется следующее сообщение (рисунок 3):

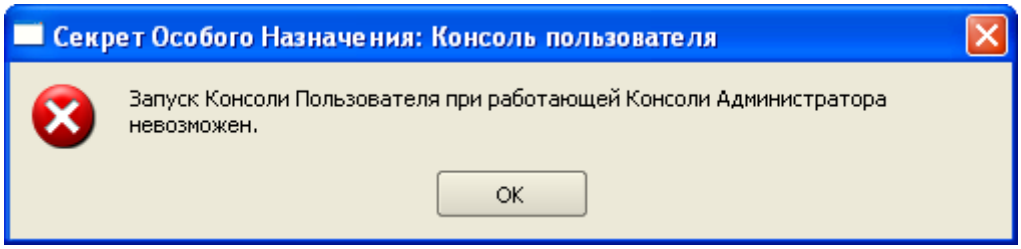

Рисунок 3 – Сообщение о невозможности запуска консоли пользователя при работающей консоли администратора

Пароль администратора необходим для выполнения любых процедур в рамках администрирования ПАК «Секрет Особого Назначения», включая смену пароля администратора.

Следует запомнить или надежно сохранить пароль администратора. В случае необходимости (например, при компрометации) пароль может быть изменен. Для выполнения этой операции потребуется знание старого пароля (подробнее см. 3.6).

Код авторизации пользователя, который формируется в результате выполнения регистрации пользователя (подробнее см. «Руководство пользователя», подраздел 3.1), необходим для выполнения следующих функций:

- авторизация пользователя при доступе к данным, хранящимся на флеш-диске СН;
- смена КА.

В случае нескольких последовательных неудачных попыток ввода КА при авторизации пользователя (максимально допустимое количество неудачных попыток определяется администратором, см. подраздел 3.2.3) СН блокируется и на экран выводится соответствующее сообщение.

ВНИМАНИЕ! В случае блокирования СН пользователь может разблокировать СН с помощью PUK – кода. Если значение PUK – кода утеряно, разблокировать СН может только администратор с помощью функции «Аннулировать регистрацию пользователя…». Важно помнить, что после выполнения данной операции пользовательская информация, хранящаяся на закрытом разделе флеш-диска СН, стирается!

Следует отметить, что регистрация администратора не относится к числу обязательных процедур. Для получения доступа к пользовательским данным, хранящимся на флеш-диске СН, достаточно зарегистрировать

пользователя и выполнять перед получением доступа процедуру авторизации.

После регистрации администратора дополнительно появляется возможность выполнения процедур управления ПАК «Секрет Особого Назначения»:

- настройка политик использования СН;
- редактирование списка разрешенных РС;
- просмотр журнала событий СН;
- аннулирование регистрации пользователя СН.

3. Управление ПАК «Секрет Особого Назначения»

3.1. Регистрация администратора

Для регистрации администратора необходимо запустить консоль администратора (исполняемый файл startAdminConsole.exe или исполняемый файл adminConsole.exe в папке specialSecret), хранящуюся на открытом разделе флеш-диска СН (см. подраздел 2.3). После этого в трее появляется значок ПАК «Секрет Особого Назначения» (рисунок 4).

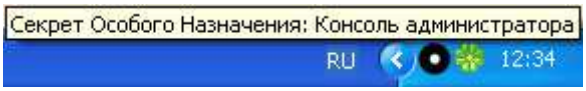

Рисунок 4 – Значок ПАК «Секрет Особого Назначения»в трее

По нажатии правой кнопкой мыши на значок СН в трее на экране появляется меню (рисунок 5), которое содержит следующие пункты:

- «О программе» – выводит сведения о ПО ПАК «Секрет Особого Назначения»;
- «Консоль администратора» – позволяет открыть консоль администратора;
- «Выход» - осуществляет выход из программы.

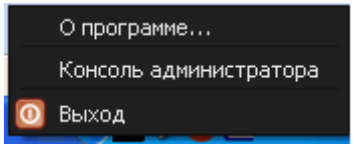

Рисунок 5 – Контекстное меню значка ПАК «Секрет Особого Назначения»в трее

Если процедура регистрации администратора ранее не выполнялась, при запуске консоли администратора активна только функция регистрации администратора (рисунок 6). Однако если в СН зарегистрирован пользователь (но не зарегистрирован администратор), то при первом запуске консоли администратора кроме функции регистрации администратора, активна функция общего сброса СН (рисунок 7).

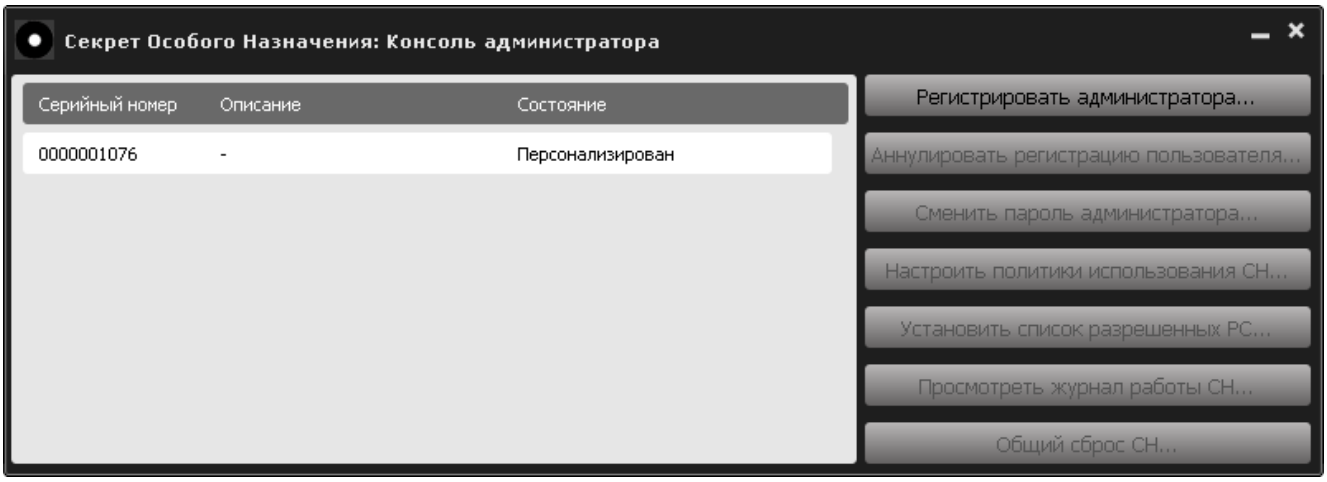

Рисунок 6 - Консоль администратора (в СН не зарегистрирован ни администратор, ни пользователь)

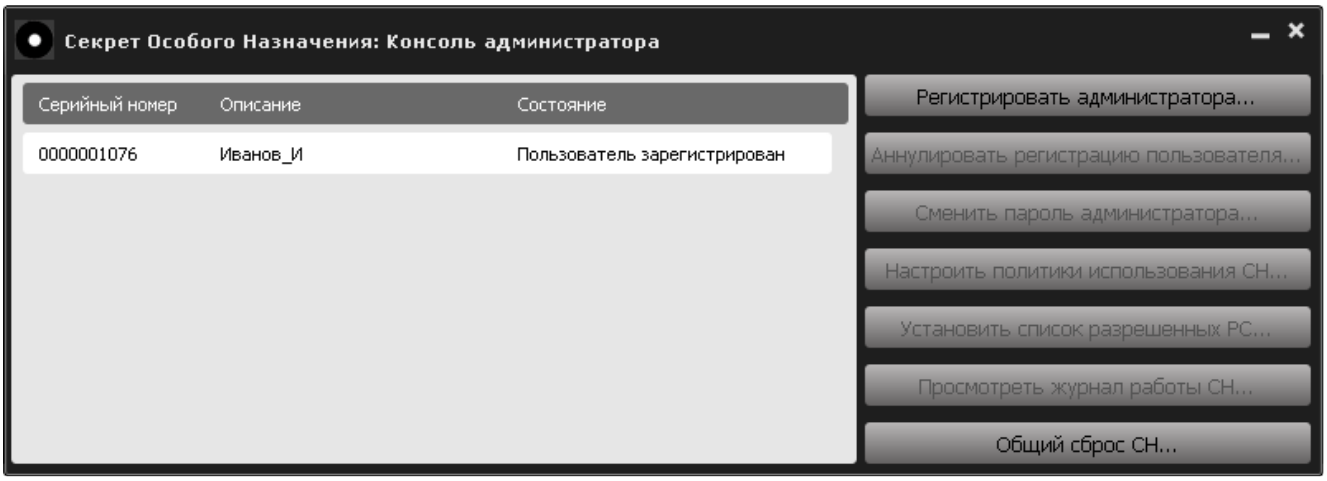

Рисунок 7 – Консоль администратора (в СН зарегистрирован пользователь)

Чтобы зарегистрировать администратора, необходимо нажать кнопку <Регистрировать администратора…>. Далее на экране появляется окно регистрации администратора (рисунок 8).

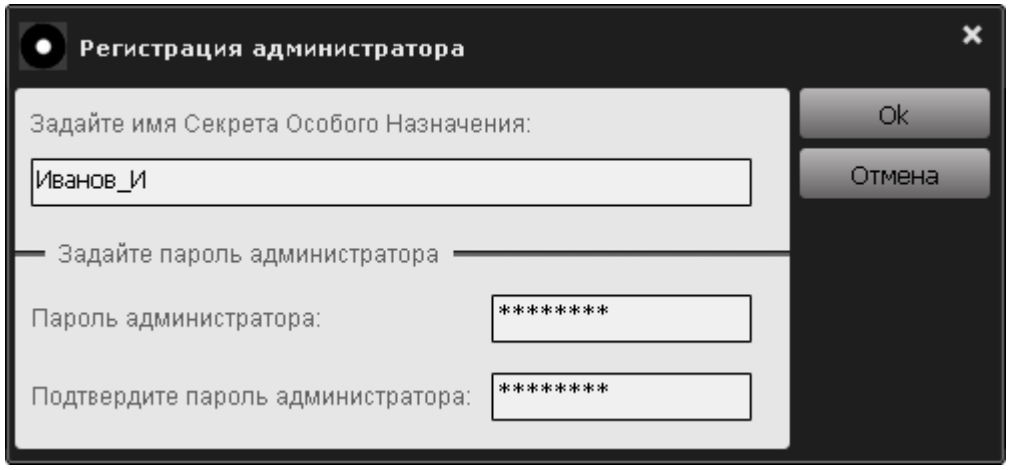

Рисунок 8 - Регистрация администратора

В появившемся диалоговом окне необходимо задать имя СН (имя СН уже могло быть задано ранее при регистрации пользователя, и в этом случае

администратор имеет возможность его изменить) и установить пароль администратора с подтверждением. Для завершения операции нужно нажать кнопку <Ok>, для отмены операции – кнопку <Отмена>. После ввода пароль администратора и имя СН передаются в СН и сохраняются во внутренней памяти устройства.

Регистрационные параметры СН:

- имя «Секрета Особого Назначения». Представляет собой строку, длина которой ограничена 34 произвольными символами. В качестве имени целесообразно использовать одно или несколько слов, характеризующих принадлежность СН (имя владельца, или должность, и т. д.) или его назначение (это может быть удобно, если в наличии имеется несколько СН, используемых для различных целей. В этом случае их легко отличить друг от друга – «для отчетов», «оборудование» и т. д.). Имя «Секрета Особого Назначения» не связано с защитными функциями и задается только для удобства пользователя, поэтому не нужно стремиться к тому, чтобы оно было сложным или чтобы о нем было трудно догадаться;
- пароль администратора. Представляет собой строку, минимальная длина которой составляет 6 произвольных символов, а максимальная длина – 16 произвольных символов.

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить пароль администратора, знание которого позволяет получать доступ к функциям администрирования ПАК «Секрет Особого Назначения». Важно помнить о необходимости сохранения пароля администратора недоступным для третьих лиц!

Кнопка <OK> окна регистрации недоступна, если:

- имя «Секрета Особого Назначения» не задано;
- не заданы значения в полях <Пароль администратора> или <Подтвердите пароль администратора>.

После того как будут введены имя устройства и пароль администратора с подтверждением, нужно нажать кнопку <Ok>, для отмены операции – кнопку <Отмена>.

Если вводимое количество символов пароля администратора меньше установленного минимального значения (6 символов), на экране появится следующее предупреждение (рисунок 9).

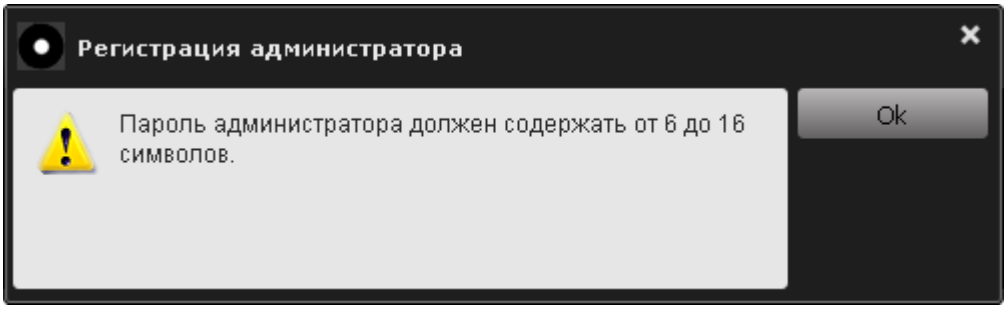

Рисунок 9 - Предупреждение о том, что пароль администратора должен содержать от 6 до 16 символов

В этом случае следует нажать кнопку <Ok> и ввести корректный пароль администратора.

Если пароль подтвержден неверно, после нажатия кнопки <ОК> на экран выводится соответствующее предупреждение (рисунок 10).

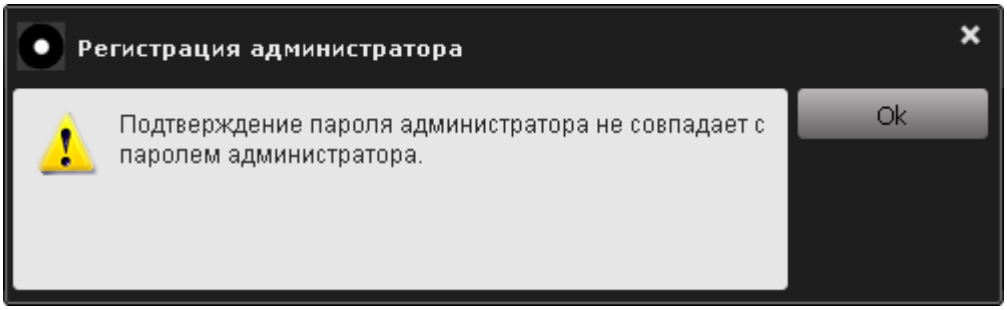

Рисунок 10 - Предупреждение об ошибке при подтверждении пароля администратора

В этом случае следует ввести корректное подтверждение пароля в поле <Подтвердите пароль администратора> (рисунок 8) и нажать кнопку <Ok>.

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

Если описанная последовательность действий выполнена верно, на экран выводится сообщение об успешной регистрации администратора (рисунок 11).

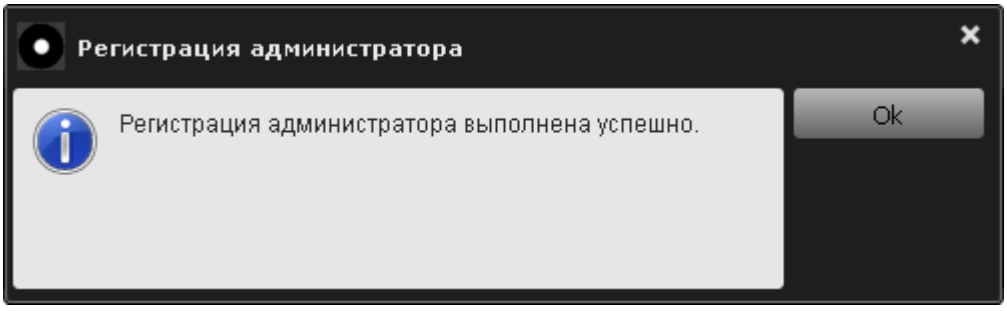

Рисунок 11 - Сообщение об успешной регистрации администратора

Далее функция регистрации администратора блокируется, в графе «Описание» отображается имя СН и становятся доступными остальные функции администрирования (рисунок 12).

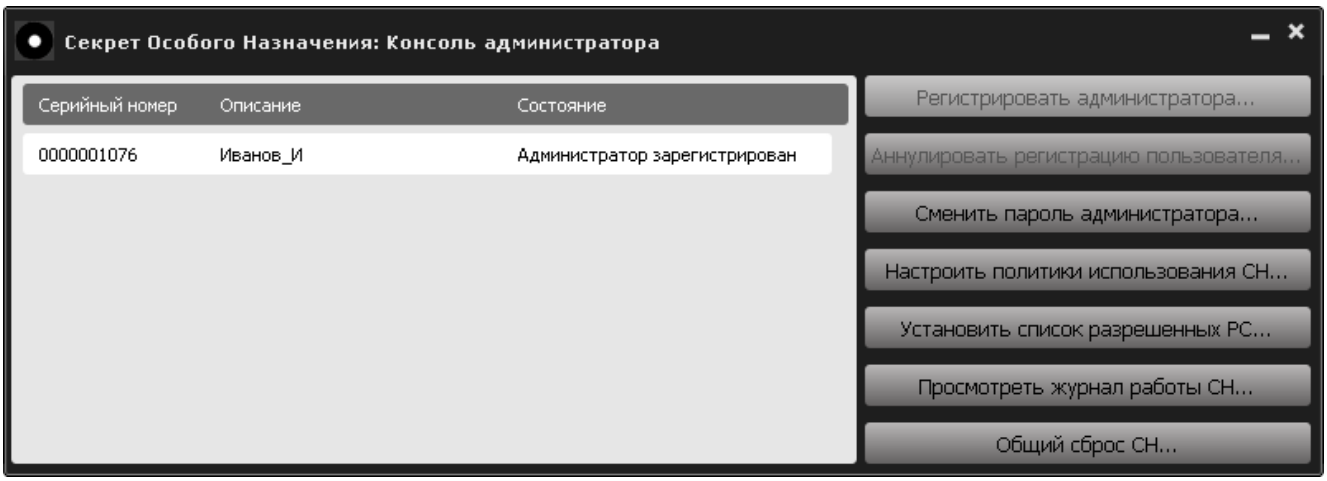

Рисунок 12 - Консоль администратора с доступными опциями

Если в СН зарегистрирован администратор, то в графе «Состояние» отображается: «Администратор зарегистрирован» (рисунок 12). После регистрации пользователя в колонке «Состояние» консоли администратора отображается: «Пользователь зарегистрирован» и становится доступной функция «Аннулировать регистрацию пользователя…» (рисунок 13).

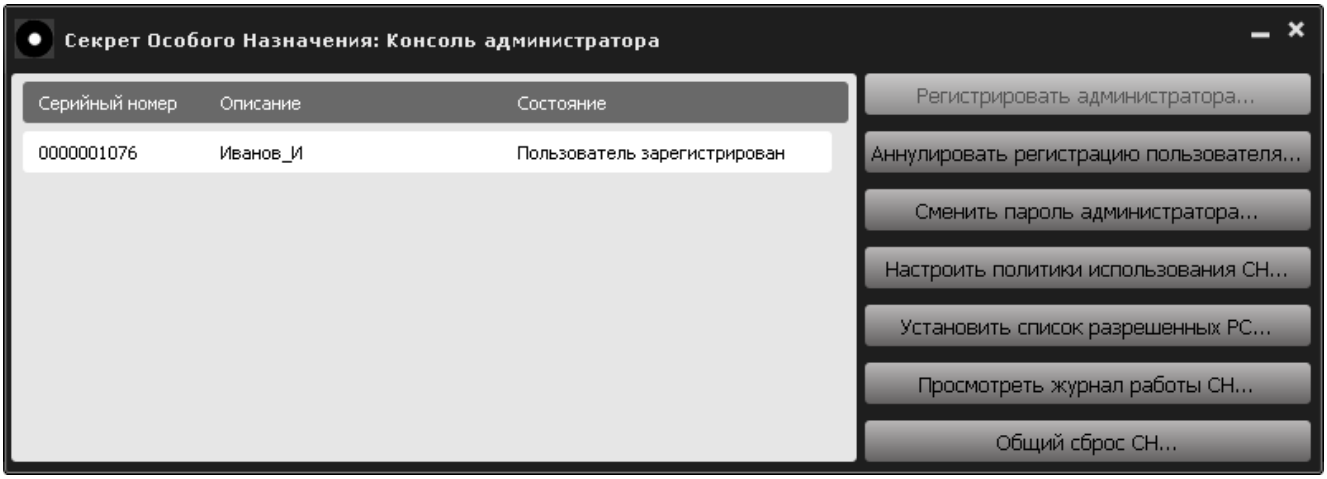

Рисунок 13 – Консоль администратора после регистрации пользователя

Если до выполнения процедуры регистрации администратора на СН была выполнена процедура регистрация пользователя, то в консоли администратора в графе «Состояние» будет отображаться «Пользователь зарегистрирован», а в графе «Описание» отображается заданное имя СН.

3.2. Настройка политик использования СН

До изменения настроек действуют политики по умолчанию:

- политика доступа к СН на РС: «Доступ без ограничения»;
- политика заполнения журнала: «Перезаписывать циклически»;
- политика использования КА: минимальное значение КА равно 6, максимальное – 16, число попыток авторизации пользователя равно 3.

В консоли администратора (рисунок 12) следует выбрать функцию «Настроить политики использования СН…». На экране появляется окно настройки политик СН (рисунок 14).

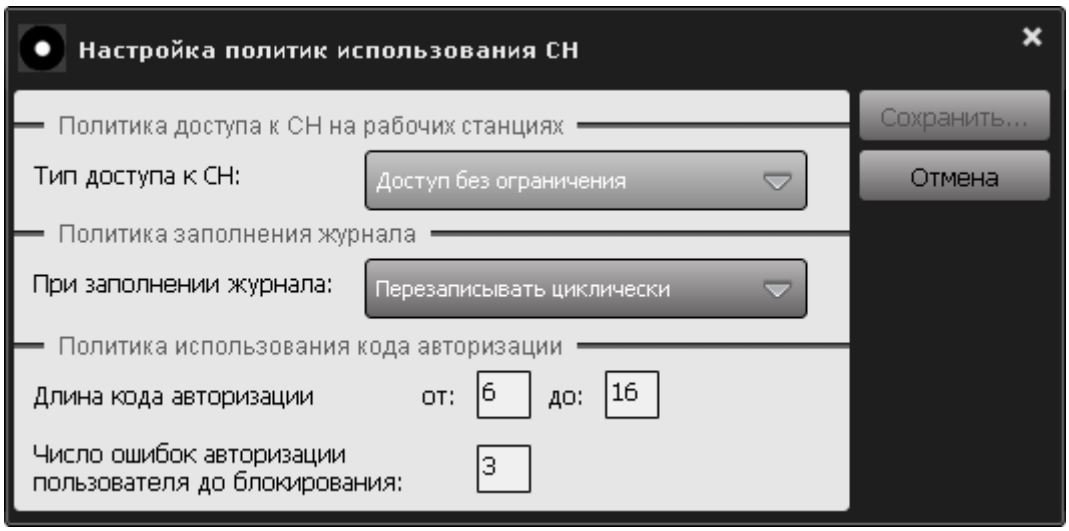

Рисунок 14 - Настройка политик СН

Экран настройки политик использования СН позволяет задать следующие параметры СН:

- тип доступа к СН на рабочих станциях;
- реакция при заполнении объема, выделенного для хранения журнала;
- длина КА и условия блокировки СН.

3.2.1. Настройка политики доступа к СН на РС

Экран настройки политик доступа к СН на РС позволяет выбрать одно из следующих значений: «Доступ без ограничения», «Доступ с ограничением по доменам и рабочим станциям» (рисунок 15).

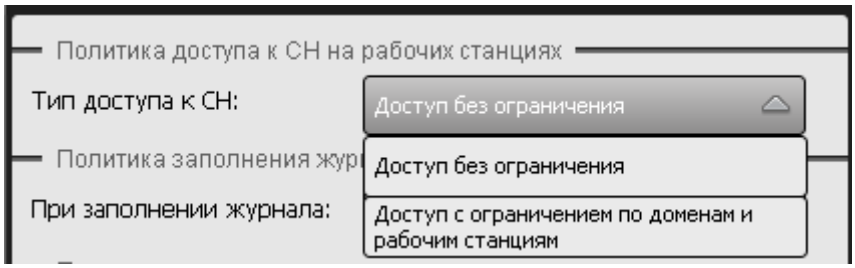

Рисунок 15 - Политика доступа к СН на рабочих станциях

Если необходимо, чтобы доступ к СН осуществлялся на любых РС, следует выбрать значение «Доступ без ограничения». Если необходимо, чтобы доступ к СН осуществлялся только на разрешенных администратором РС, следует выбрать опцию «Доступ с ограничением по доменам и рабочим станциям».

При выборе последнего варианта можно указать конкретные домены Active Directory, а также конкретные РС, на которых будет разрешена работа с данным СН. При добавлении РС в список разрешенных указываются отдельные РС домена (также допустимо указывать РС, не включенные в домены). Порядок задания перечня разрешенных РС описан в 3.3.

При авторизации пользователя СН получает от ПО РС идентификатор домена и идентификатор РС в домене, и на основании полученных данных

устройство разрешает доступ или отказывает в авторизации пользователю при нарушении политики доступа к РС.

3.2.2. Настройка реакции при заполнении объема, выделенного для хранения журнала

Экран настройки действий при возможном переполнении журнала событий СН (рисунок 16) позволяет выбрать одно из следующих значений:

- перезаписывать циклически;
- блокировать при переполнении.

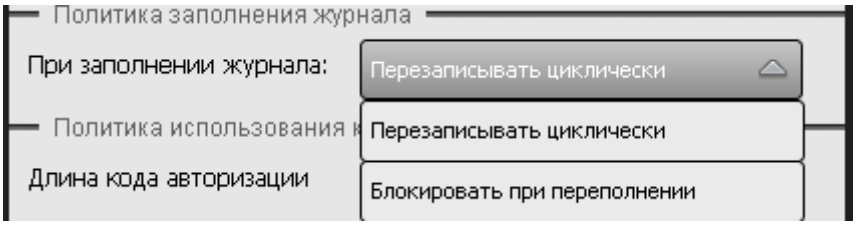

Рисунок 16 - Политика заполнения журнала

В первом случае при заполнении выделенного для хранения журнала объема (512 Мб) события будут записываться в журнал СН со стиранием самых старых записей. Во втором случае при достижении этой границы внутреннее ПО СН блокирует выполнение всех пользовательских функций СН до тех пор, пока администратор не выполнит очистку журнала событий (см. 3.5).

3.2.3. Настройка политики использования КА

ВНИМАНИЕ! Функция настройки политики использования КА доступна только в том случае, если в СН не зарегистрирован пользователь.

Экран настройки политик использования кода авторизации СН позволяет выбрать:

- минимальную и максимальную длину КА (значения границ варьируются в диапазоне от 6 до 16 произвольных символов; по умолчанию используются значения границ 6 и 16 (рисунок 17));
- максимальное число неудачных попыток авторизации: после достижения этого порога СН блокируется, разблокировка возможна только по предъявлению PUK-кода. Это число может варьироваться в пределах от 1 до 255 (по умолчанию установлено значение 3) (рисунок 17).

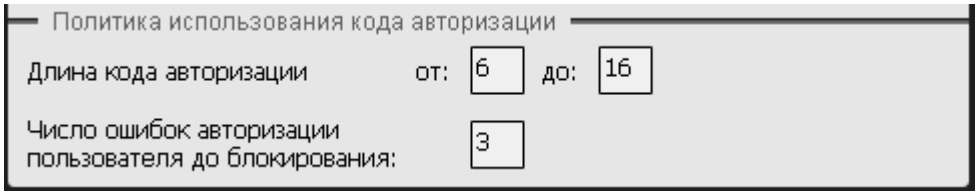

Рисунок 17 - Окно настройки политики использования кода авторизации

3.2.4. Сохранение политик СН

После внесения необходимых изменений в политики СН следует нажать кнопку <Сохранить…>, а для отмены внесенных изменений необходимо нажать кнопу <Отмена>.

После нажатия кнопки <Сохранить…> на экране появляется окно запроса пароля администратора (рисунок 18):

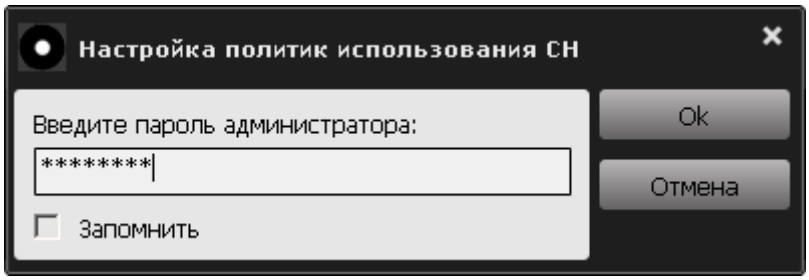

Рисунок 18 - Окно запроса пароля администратора

Для того чтобы завершить операцию настройки политик СН, следует нажать кнопку <Ok>. Если требуется запомнить пароль администратора на время работы с СН, нужно отметить пункт «Запомнить».

Если пароль администратора введен неверно, на экране отображается сообщение об ошибке в процессе ввода пароля (рисунок 19).

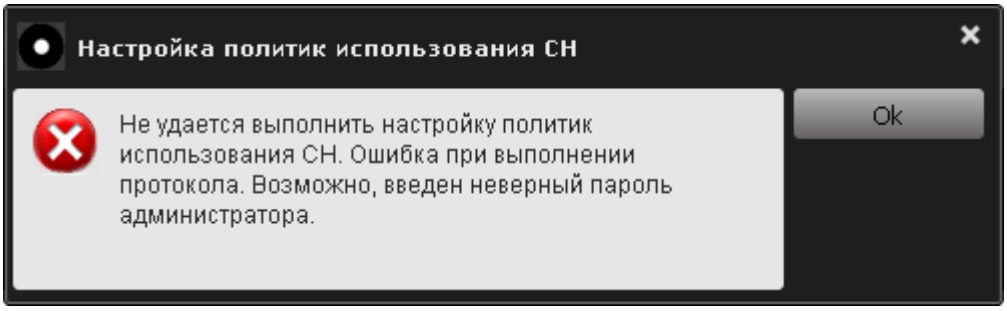

Рисунок 19 - Сообщение об ошибке в процессе ввода пароля

В этом случае следует нажать кнопку <Ok> и ввести корректный пароль администратора.

ВНИМАНИЕ! В случае трех подряд неудачных попыток ввода пароля администратора ПО СН функции администрирования блокируются для выполнения. Чтобы выйти из этого состояния, следует повторно подключить СН и перезапустить консоль администратора.

Если пароль администратора введен корректно, на экране появляется сообщение об успешном выполнении настройки политик СН (рисунок 20).

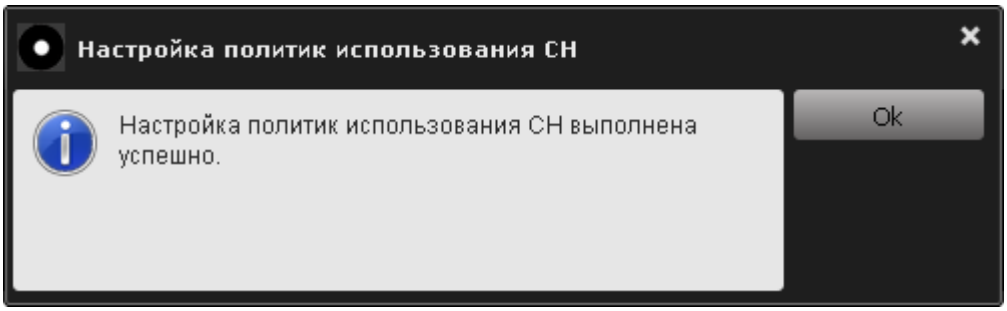

Рисунок 20 - Сообщение об успешном выполнении настройки СН

Для продолжения работы с консолью администратора (рисунок 12) следует нажать кнопку <Ok>.

3.3. Добавление РС в список разрешенных

Для того чтобы задать список рабочих станций, на которых должен быть разрешен доступ к СН, в консоли администратора (рисунок 12) необходимо выбрать функцию «Установить список разрешенных РС…». После этого на экране появляется окно установки списка разрешенных РС (рисунок 21).

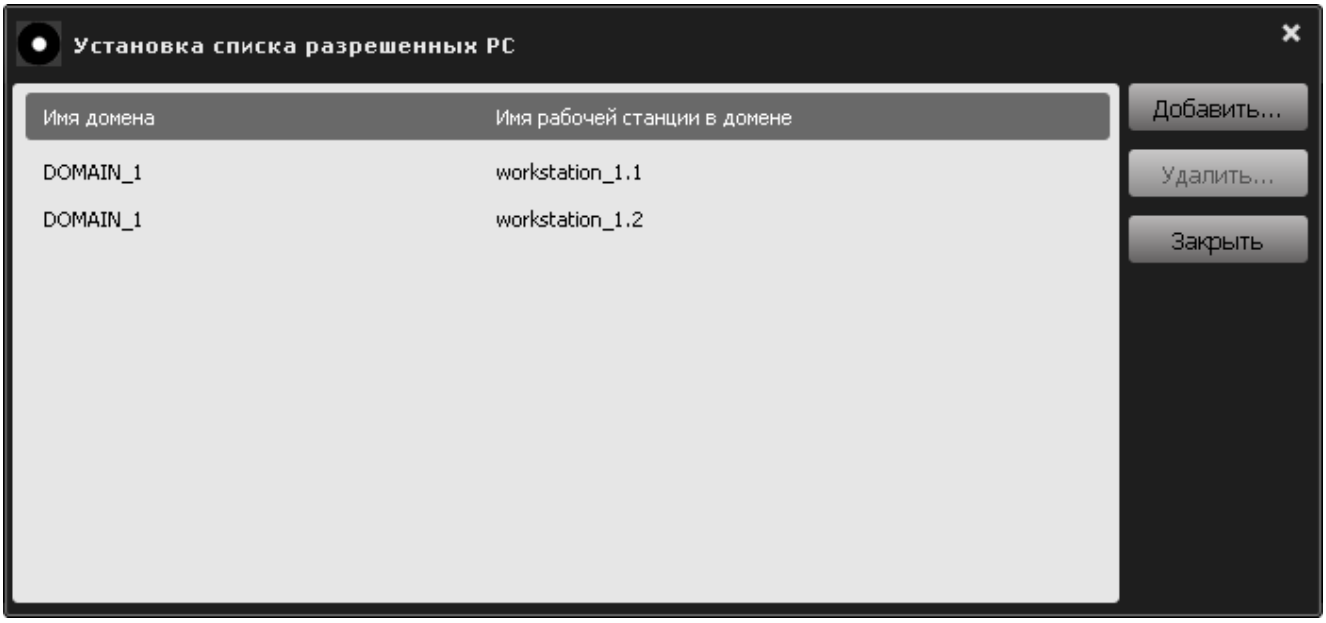

Рисунок 21 - Установка списка разрешенных станций

По нажатии кнопки <Добавить…> на экране появляется окно выбора рабочей станции (рисунок 22):

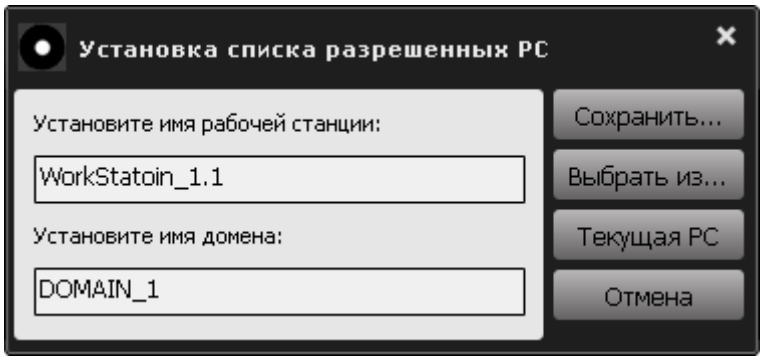

Рисунок 22 - Окно установки имени и домена рабочей станции

В верхнее поле данного окна следует ввести имя PC, в нижнее – имя домена (рабочей группы), в котором находится данная PC, а затем нажать кнопку <Сохранить…>.

ВНИМАНИЕ! Имя домена необходимо вводить в формате NetBIOS.

Если рабочая станция с заданным именем в сети не найдена, то на экране появляется сообщение (рисунок 23):

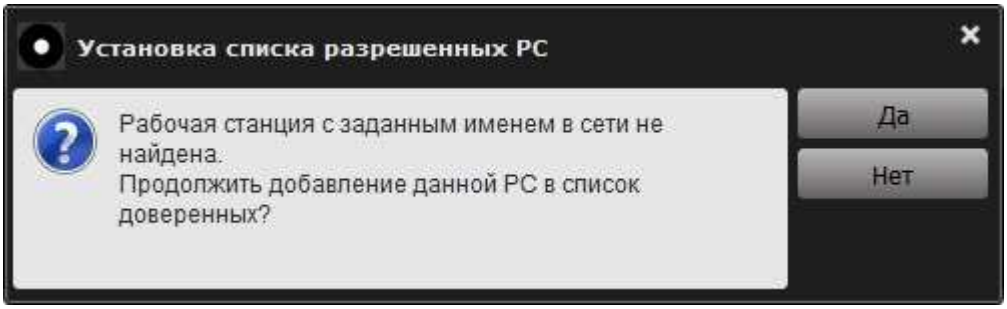

Рисунок 23 - Оповещение о том, что рабочая станция с заданным именем не найдена в сети

Для подтверждения текущей операции следует нажать кнопку <Да>, для отмены операции – кнопку <Нет>.

По нажатии кнопки <Да> на экране появляется окно для ввода пароля (рисунок 24).

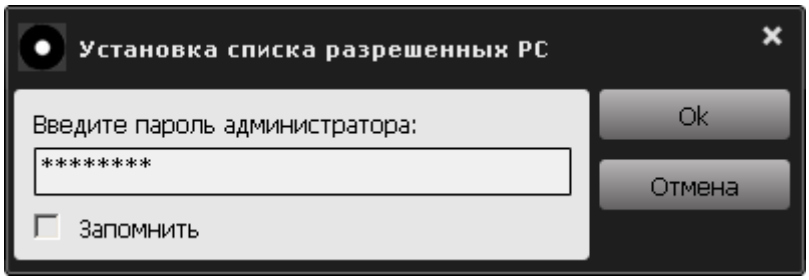

Рисунок 24 – Окно ввода пароля

Если домена с заданным именем в сети не найден, то на экране появляется сообщение (рисунок 25):

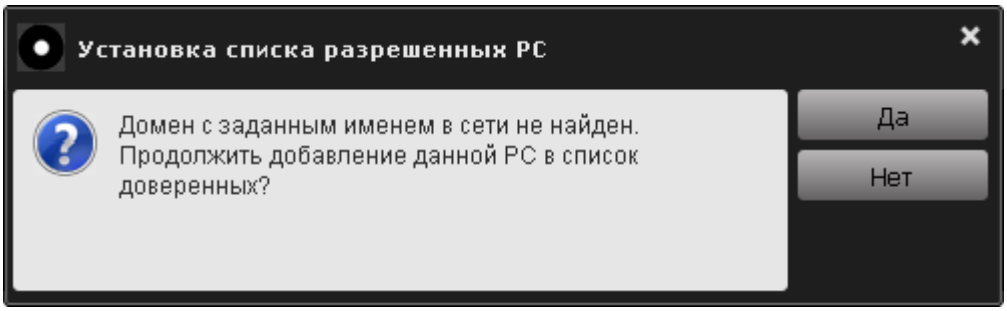

Рисунок 25 – Оповещение о том, что домен с заданным именем не найден в сети

Для подтверждения текущей операции следует нажать кнопку <Да>, для отмены операции – кнопку <Нет>.

По нажатии кнопки <Да> на экране появляется окно для ввода пароля (рисунок 24). Необходимо ввести пароль администратора и нажать кнопку <Ok>. Либо кнопку <Отмена> для прерывания текущей операции.

По нажатии кнопки <Текущая PC> (рисунок 22) на экране появляются имя и домен PC, на которой в данный момент времени работает пользователь СН.

По нажатии кнопки <Выбрать из…> (рисунок 22) на экране отображается окно с доступными доменными именами PC (рисунок 26).

Рисунок 26 - Список доменных имен PC

Следует нажать на кнопку ⊞, чтобы увидеть список имен различных рабочих станций находящихся в доменах (рисунок 27).

Рисунок 27 - Выбор имени разрешенной рабочей станции

Необходимо отметить нужное имя и нажать кнопку <Выбрать> (рисунок 27). Для отмены текущей операции следует нажать кнопку <Отмена>.

После выбора нужной PC на экран вновь выводится окно установки имени и домена разрешенных PC (рисунок 22), но в полях этого окна будут записаны имя и домен выбранной PC (рисунок 28).

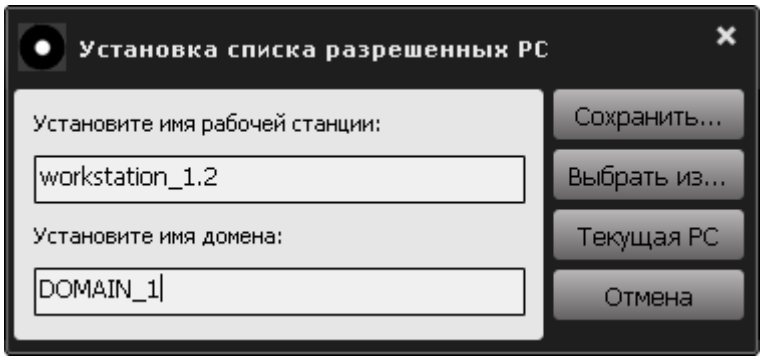

Рисунок 28 - Окно установки списка разрешенных PC с введенными именем и именем домена PC

Следует нажать кнопку <Сохранить…> для внесения данной PC в список разрешенных и кнопку <Отмена> для отмены текущей операции.

По нажатии кнопки <Сохранить…> на экране появляется окно для ввода пароля (рисунок 29).

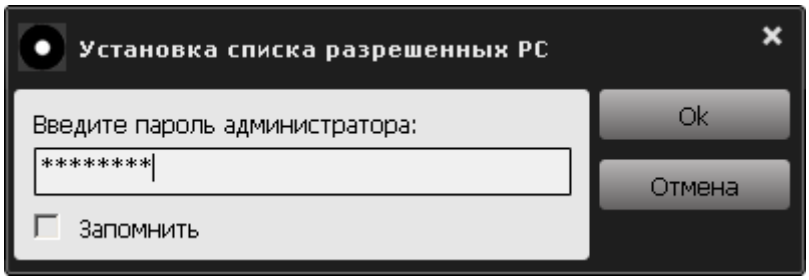

Рисунок 29 - Окно ввода пароля

Необходимо ввести пароль администратора и нажать кнопку <Ok>, для прерывания текущей операции следует нажать кнопку <Отмена>.

Если пароль введен некорректно, то на экране появляется сообщение об ошибке при установке списка разрешенных PC (рисунок 30).

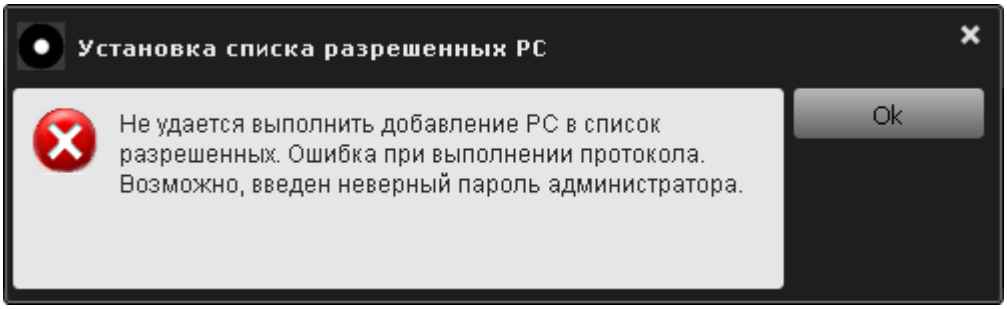

Рисунок 30 - Сообщение об ошибке в процессе ввода пароля администратора

В этом случае в данном сообщении нужно нажать кнопку <Ok>, далее ввести корректный пароль администратора.

Если операция установки списка разрешенных PC выполнена корректно, то на экране отображается сообщение об успешном завершении установки списка разрешенных PC (рисунок 31).

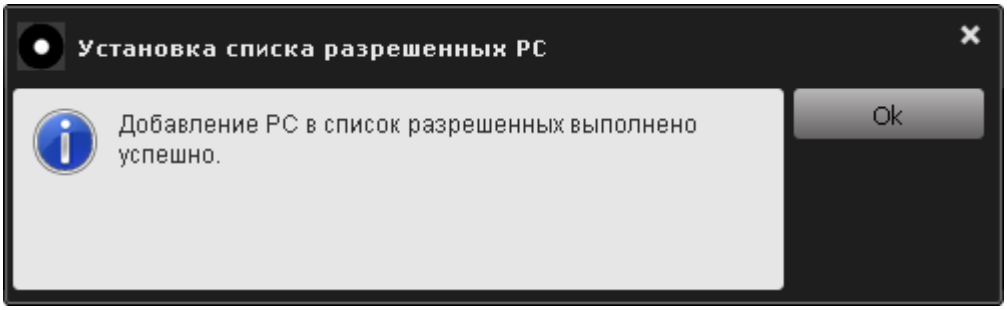

Рисунок 31 - Сообщение об успешном выполнении установки разрешенных PC

Следует нажать кнопку <Ok> для дальнейшей работы с консолью администратора.

При необходимости следует повторить описанную процедуру столько раз, сколько PC необходимо добавить в список разрешенных.

При первом подключении СН к PC из числа разрешенных внутреннее ПО СН производит считывание и сохранение внутри устройства информации о параметрах оборудования данной PC. В дальнейшем эта информация

используется при принятии решения о предоставлении доступа к пользовательской информации СН на РС.

ВНИМАНИЕ! При корпоративном применении ПАК «Секрет Особого Назначения» в целях безопасности рекомендуется, чтобы первое подключение СН к РС выполнял администратор.

Если в настройках политики доступа к РС был выбран тип доступа к РС: «Доступ без ограничений», то после выполнения процедуры добавления РС в список разрешенных на экране появляется оповещение (рисунок 32) о том, что внесенные изменения вступят в силу после установки типа доступа к РС «Доступ с ограничением по доменам и рабочим станциям».

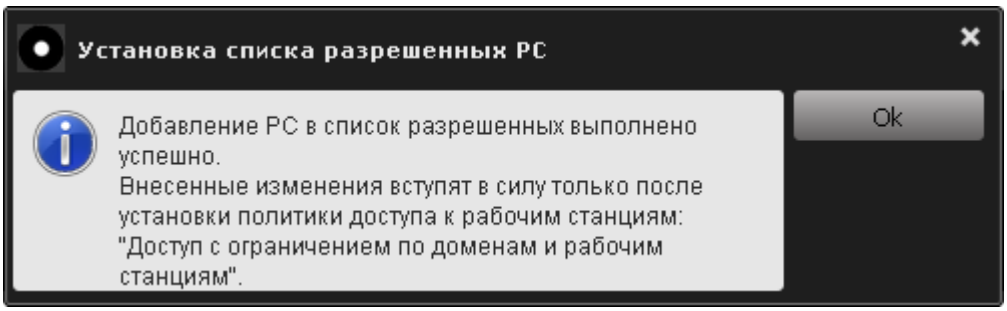

Рисунок 32 – Сообщение о внесенных изменениях

3.4. Удаление РС из списка разрешенных

Если необходимо удалить РС из числа разрешенных, в списке разрешенных РС следует выбрать нужную запись и нажать кнопку <Удалить…> (рисунок 33).

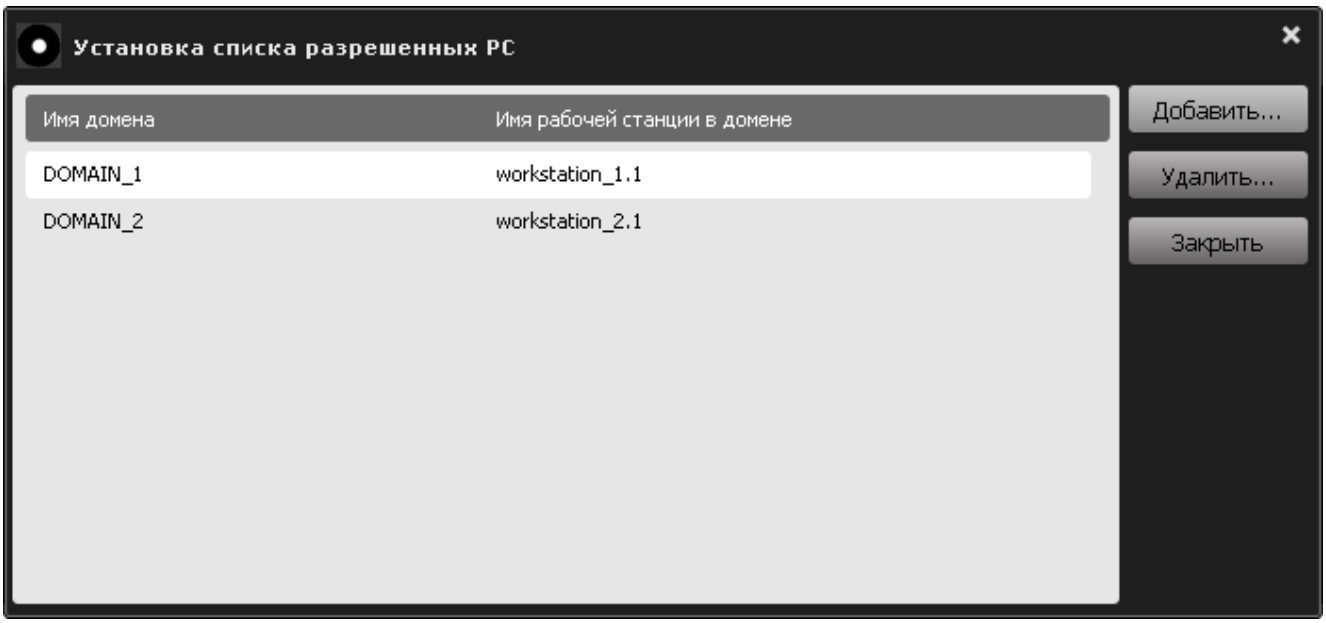

Рисунок 33 - Список разрешенных РС

После этого на экране появляется окно запроса пароля администратора, как показано на рисунке 34:

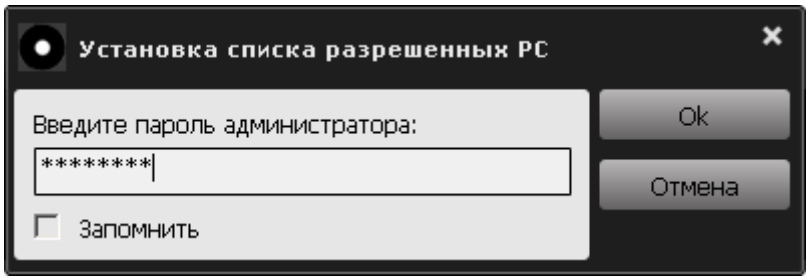

Рисунок 34 - Окно ввода пароля администратора

В поле данного окна нужно ввести пароль и нажать кнопку <Ok>, для отмены операции следует нажать кнопку <Отмена>.

Если пароль администратора введен некорректно, на экране появляется сообщение об ошибке при выполнении операции удаления PC из списка разрешенных (рисунок 35):

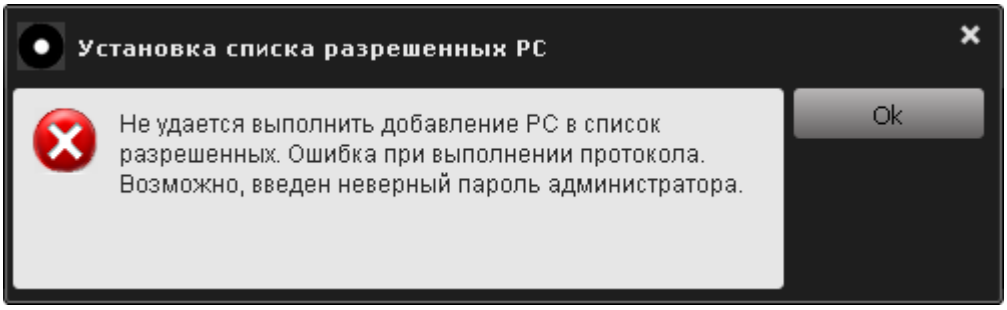

Рисунок 35 - Сообщение об ошибке при выполнении операции удаления разрешенной PC

В таком случае следует нажать кнопку <Ok> ввести корректный пароль администратора.

Если операция удаления разрешенной PC выполнена корректно, на экране отображается сообщение об успешном удалении PC из списка разрешенных (рисунок 36):

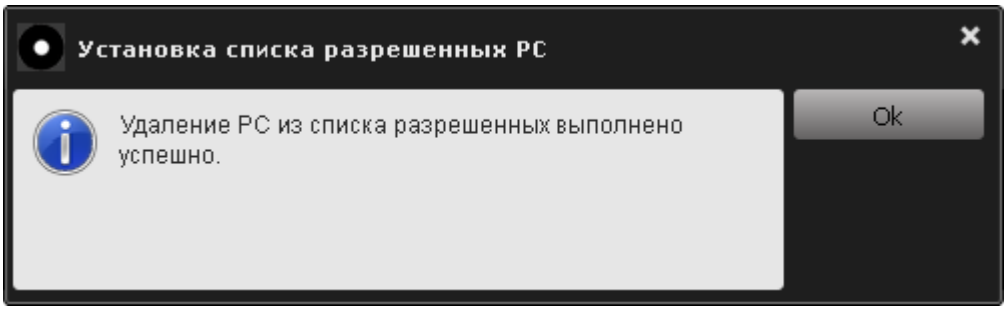

Рисунок 36 - Сообщение об успешном удалении PC из списка разрешенных PC

После завершения всех необходимых операций со списком разрешенных PC в окне задания списка разрешенных PC (рисунок 21) нужно нажать кнопку <Закрыть>.

Если в настройках политики доступа к PC был выбран тип доступа к PC: «Доступ без ограничений», то после выполнения процедуры удаления PC из списка разрешенных на экране появляется сообщение (рисунок 37), оповещающее о том, что внесенные изменения вступят в силу после

установки типа доступа к РС «Доступ с ограничением по доменам и рабочим станциям».

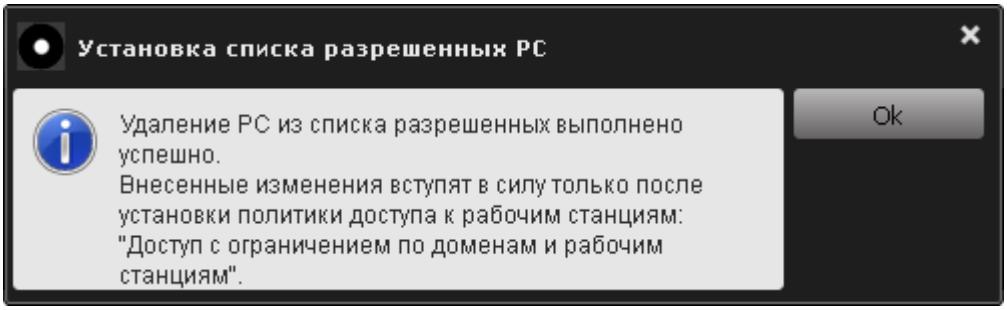

Рисунок 37 - Сообщение о внесенных изменениях

3.5. Просмотр журнала событий СН

ВНИМАНИЕ! Доступ к журналу событий ПАК «Секрет Особого Назначения» имеет только администратор устройства. Пользователь имеет доступ к журналу событий только при личном использовании СН.

Для того чтобы посмотреть журнал событий СН, необходимо нажать кнопку «Просмотреть журнал работы СН…» на панели консоли администратора (рисунок 12).

После выбора данной функции на экране появляется окно с запросом пароля администратора СН для доступа к журналу работы СН (рисунок 38). В поле данного окна следует ввести пароль администратора и нажать кнопку <Ok>.

В рамках одного сеанса работы с СН введение пароля администратора для доступа к журналу событий устройства требуется только один раз.

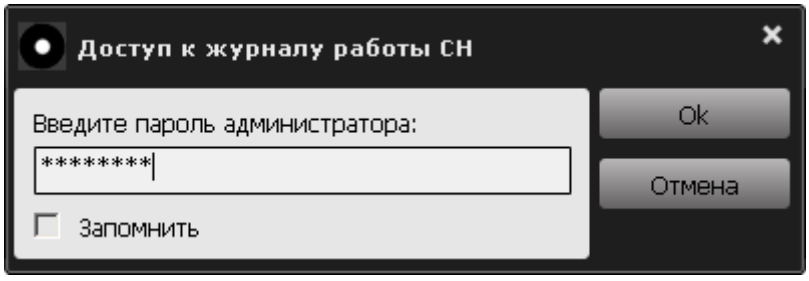

Рисунок 38 - Запрос пароля администратора СН для доступа к журналу работы СН

Если пароль введен некорректно, то на экране отображается сообщение об ошибке при вводе пароля администратора (рисунок 39):

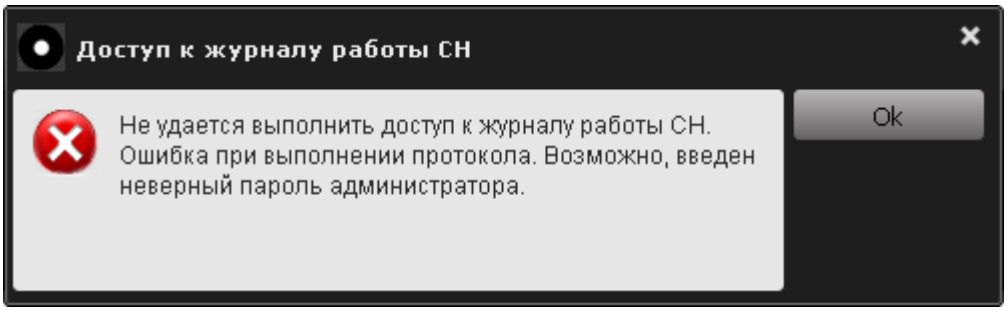

Рисунок 39 – Ошибка при выполнении доступа к протоколу работы СН

Если пароль введен корректно, на экране появляется сообщение об успешном доступе к протоколу работы СН (рисунок 40).

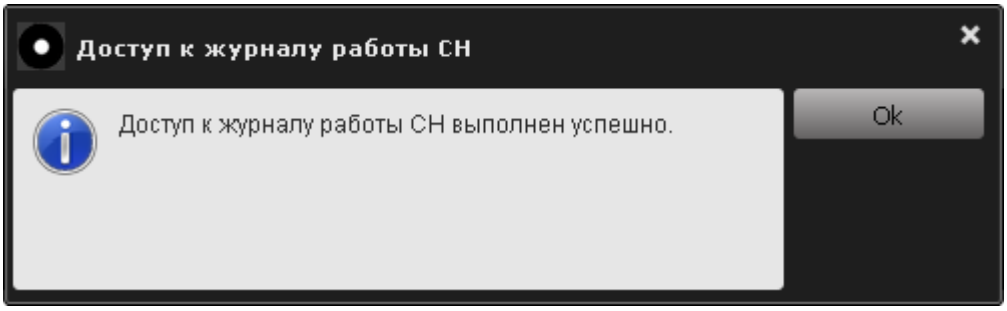

Рисунок 40 - Сообщение об успешном доступе к протоколу работы СН

По нажатии кнопки <Ok> на экране появляется журнал регистрации событий СН (рисунок 41), который содержит информацию о событиях, зафиксированных в процессе работы с ПАК «Секрет Особого Назначения» на данной РС (следует отметить, что при каждом подключении СН к компьютеру в журнале регистрируется соответствующее событие, предназначенное для фиксирования собственно факта подключения (подачи электропитания на устройство). Вследствие специфики данного события (оно регистрируется до начала взаимодействия СН с прикладным ПО, установленным в ОС компьютера) в журнал не записывается информация о дате и времени регистрации этого события).

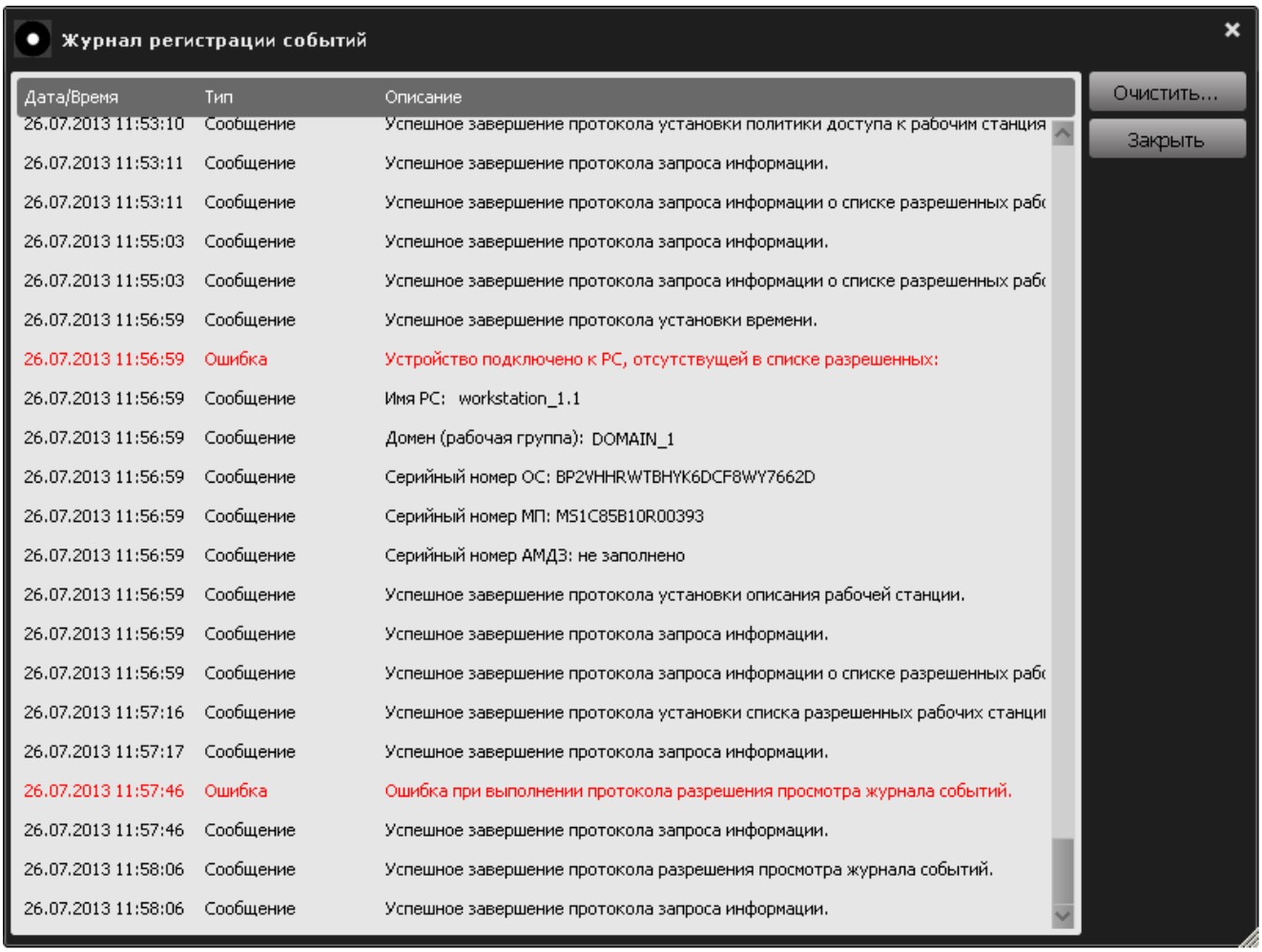

Рисунок 41 - Журнал регистрации событий СН

Если журнал СН переполнен (статус СН «Журнал переполнен» в главном окне консоли администрирования), необходимо провести очистку журнала регистрации событий. Для этого нужно нажать кнопку <Очистить> в журнале регистрации событий (рисунок 41).

ВНИМАНИЕ! Перед очисткой журнала рекомендуется выполнить копирование его содержимого на какой-либо сторонний носитель информации для возможности выполнения последующего анализа. Содержимое журнала регистрации событий хранится в текстовых файлах, размещенных на закрытом разделе СН (рисунок 42)).

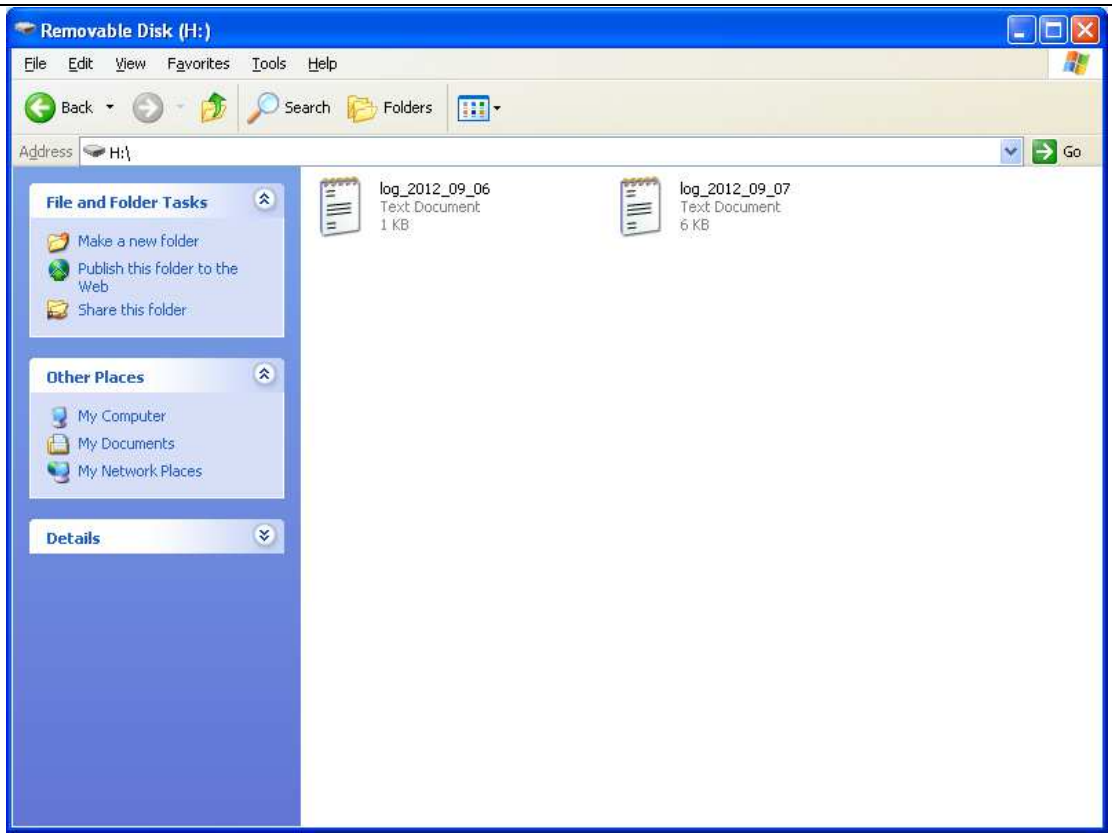

Рисунок 42 – Текстовые файлы журнала событий СН

Далее запрашивается пароль администратора для доступа к журналу работы СН (рисунок 43).

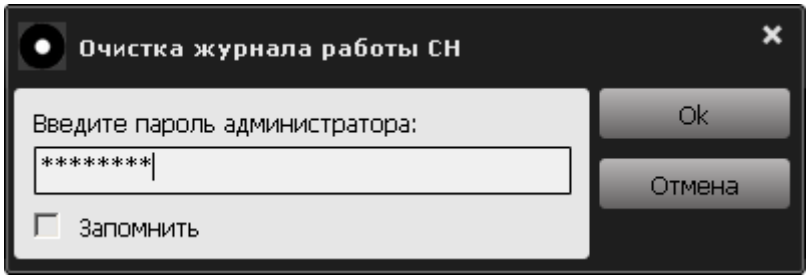

Рисунок 43 – Запрос пароля администратора СН для очистки журнала работы СН

В случае если пароль введен некорректно, на экране появляется оповещение об ошибке (рисунок 44):

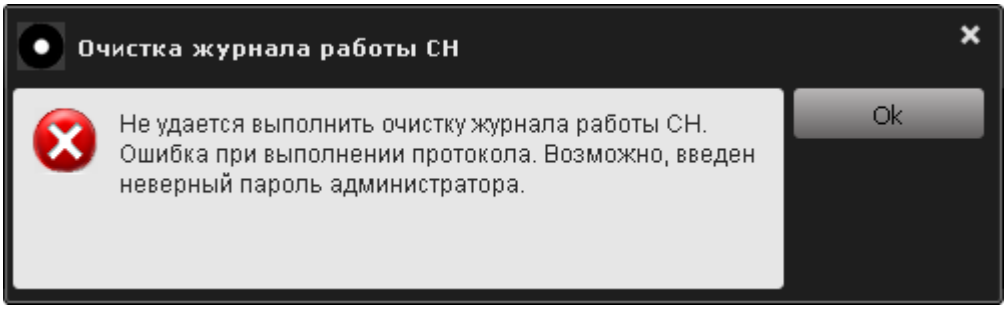

Рисунок 44 - Оповещение о невозможности доступа к протоколу работы СН

В этом случае в данном сообщении нужно нажать кнопку <Ok> и ввести корректный пароль администратора.

Если пароль введен корректно, на экране отображается следующее сообщение (рисунок 45).

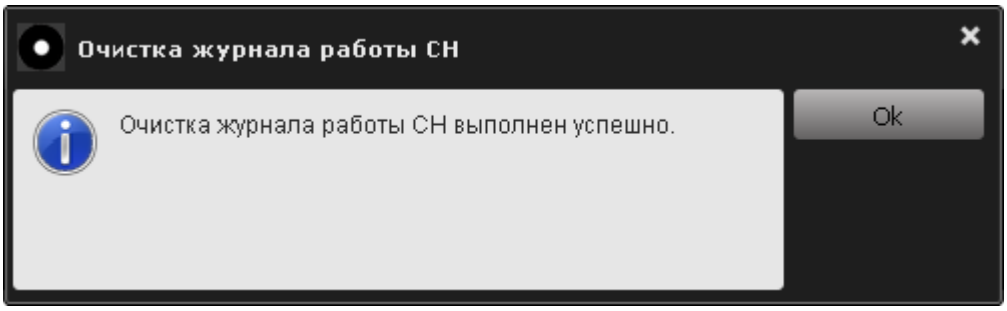

Рисунок 45 - Сообщение об успешном выполнении сброса протокола работы СН

После выполнения всех необходимых действий с журналом регистрации событий СН, можно нажать кнопку <Закрыть>. (Описание возможных сообщений, фиксируемых в журнале событий СН см. в разделе 6).

3.6. Смена пароля администратора

В случае необходимости смены пароля администратора (например, в случае его компрометации) в консоли администратора (рисунок 12) следует нажать кнопку «Сменить пароль администратора…». После выбора этой функции на экране появляется окно, показанное на рисунке 46.

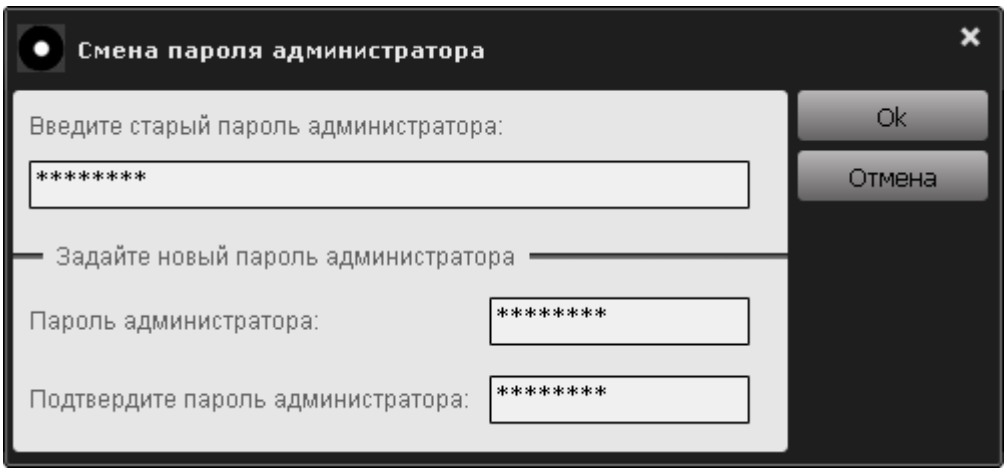

Рисунок 46 - Окно смены пароля администратора

Для восстановления возможности выполнения административных функций ПАК «Секрет Особого Назначения» в случае утраты пароля администратора необходимо выполнить процедуру общего сброса СН (подробнее см. пункт 3.8)

В верхнем поле данного окна необходимо ввести старый пароль администратора, в нижних полях – ввести новый пароль с подтверждением. После этого следует нажать кнопку <Ok> - для завершения текущей операции и кнопку <Отмена> - для ее отмены.

Кнопка <Ok> недоступна, если:

- не введен старый пароль администратора;
- не заданы допустимые значения в полях <Пароль администратора> и <Подтвердите пароль администратора>.

Следует ввести старый и новый пароль с подтверждением в соответствующие поля и нажать кнопку <Ok>.

Если вводимое количество символов нового пароля администратора меньше установленного минимального значения (6 символов), на экране появится следующее предупреждение (рисунок 47).

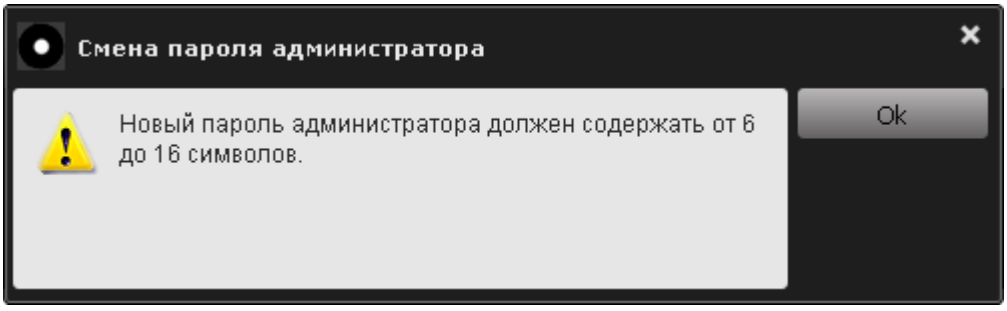

Рисунок 47 - Предупреждение о том, что новый пароль администратора должен содержать от 6 до 16 символов

В этом случае следует нажать кнопку <Ok> и ввести корректный пароль администратора.

Если подтверждение пароля введено некорректно, на экране появляется предупреждение (рисунок 48):

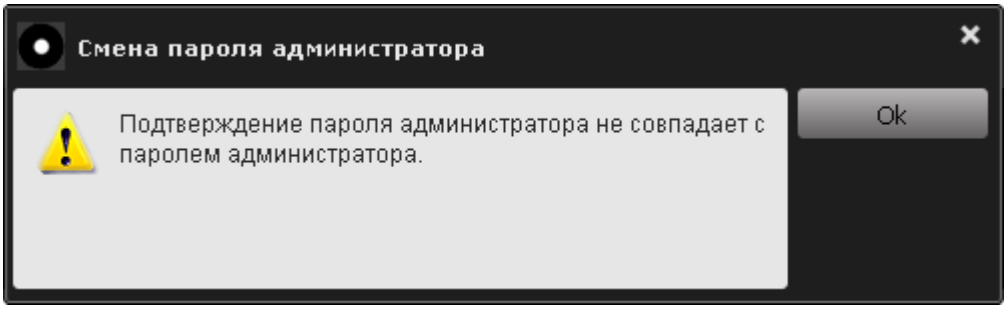

Рисунок 48 - Предупреждение о том, что подтверждение пароля администратора не совпадает с паролем администратора

В этом случае необходимо нажать кнопку <Ok> и ввести пароль с подтверждением еще раз.

Если же старый пароль введен некорректно, на экране появляется сообщение о вводе некорректного пароля (рисунок 49).

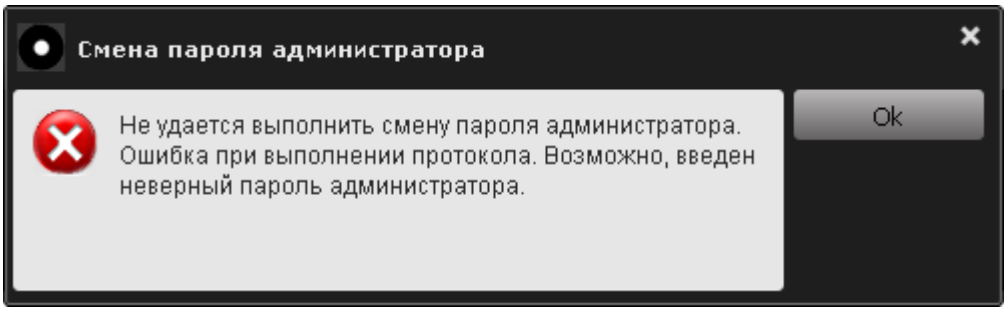

Рисунок 49 - Сообщение о вводе некорректного старого пароля

В этом случае следует нажать кнопку <Ok> и повторить описанную выше операцию смены пароля заново.

Если операция смены пароля администратора выполнена успешно, на экране отображается оповещение об успешной смене пароля (рисунок 50):

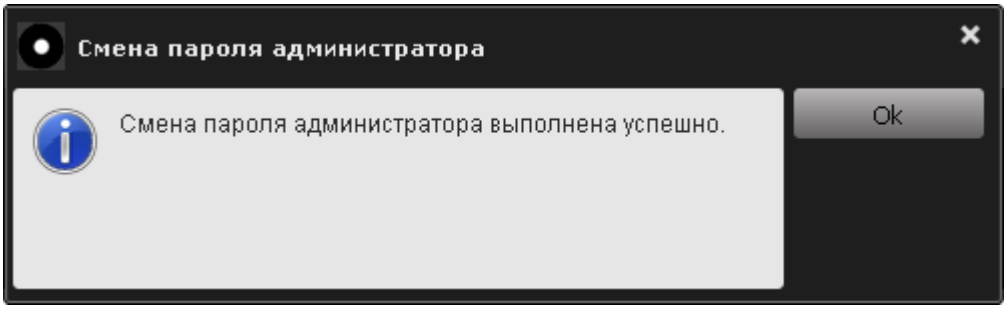

Рисунок 50 - Оповещение об успешной смене пароля

Необходимо проводить как регулярную (в соответствии с внутренней политикой безопасности организации), так и экстренную (в случае подозрения о компрометации) смену пароля администратора.

3.7. Аннулирование регистрации пользователя СН

Данная операция доступна, если на СН ранее был зарегистрирован пользователь (подробнее см. «Руководство пользователя» пункт 3.1).

Как правило, данная операция выполняется в следующих случаях:

- СН необходимо передать другому пользователю;
- утрачен код авторизации и PUK-код.

ВНИМАНИЕ! При выполнении операции аннулирования регистрации пользователя производится стирание пользовательской информации СН.

Для выполнения операции аннулирования регистрации пользователя следует нажать кнопку <Аннулировать регистрацию пользователя…> в консоли администратора (рисунок 12).

После выбора соответствующей функции (рисунок 12) на экране появляется окно запроса пароля администратора (рисунок 51):

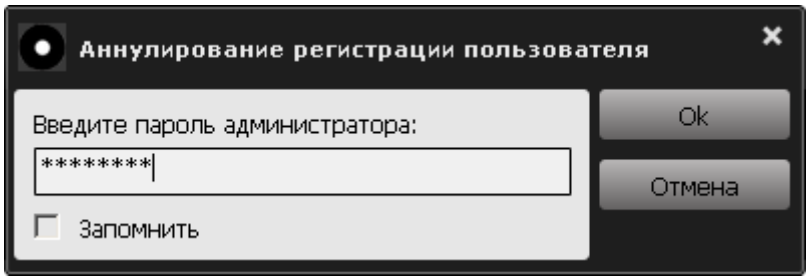

Рисунок 51 - Окно ввода пароля администратора

Следует ввести пароль и для завершения текущей операции необходимо нажать кнопку <Ok>, а для ее отмены – кнопку <Отмена>.

Если пароль введен некорректно, на экране появляется сообщение об ошибке в процессе ввода пароля (рисунок 52):

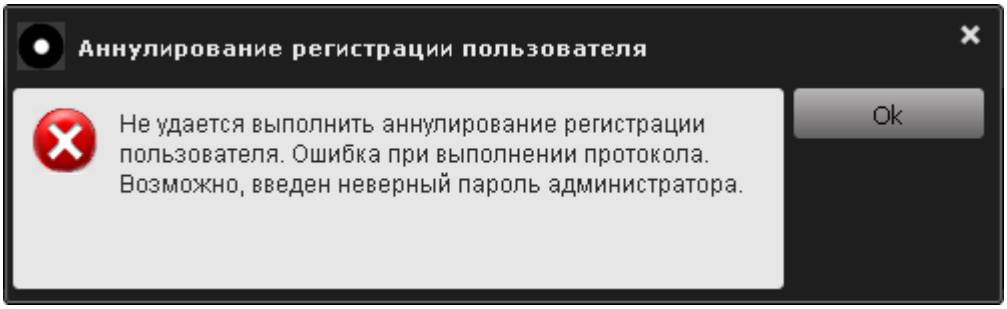

Рисунок 52 - Сообщение о невозможности выполнения аннулирования регистрации пользователя СН

В этом случае следует нажать кнопку <Ok> и повторить описанную выше операцию.

После корректного ввода пароля на экране отображается сообщение об успешном аннулировании регистрации пользователя СН (рисунок 53):

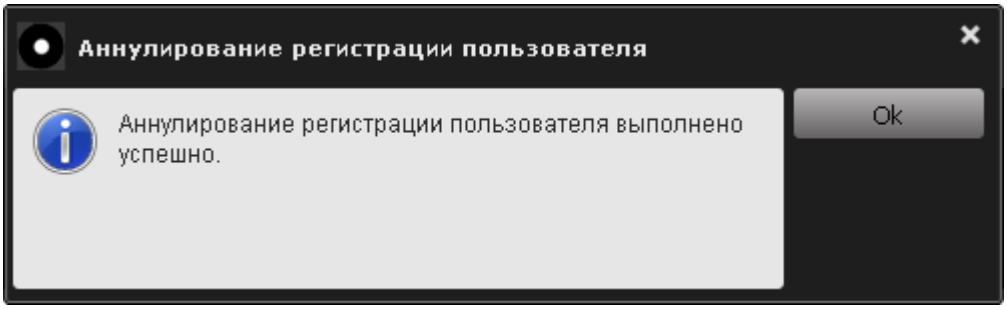

Рисунок 53 - Сообщение об успешном аннулировании регистрации пользователя СН

Для завершения операции необходимо нажать кнопку <Ok>.

ВНИМАНИЕ! Следует иметь в виду, что процесс стирания пользовательской информации может занять достаточно длительное время, и потеря питания СН до его завершения приведет только к стиранию части закрытого диска; при этом операция аннулирования может быть не выполнена должным образом. Поэтому необходимо обеспечить бесперебойную подачу питания на протяжении выполнения данной операции.

3.8. Общий сброс СН

В случае если пароль администратора утерян, может потребоваться выполнить общий сброс СН. Выполнение данной процедуры не является обязательным, поскольку остается возможность выполнения пользовательских функций СН даже в условиях, когда пароль администратора утрачен.

ВНИМАНИЕ! Важно помнить, что при выборе данной функции кроме аннулирования регистрации администратора также произойдет сброс всех настроек СН, журнала событий, аннулирование регистрации пользователя СН (см. 3.7) и удаление его информации.

Для выполнения операции сброса СН следует нажать кнопку <Общий сброс СН…> в консоли администратора (рисунок 12). После этого на экране появляется следующее сообщение (рисунок 54):

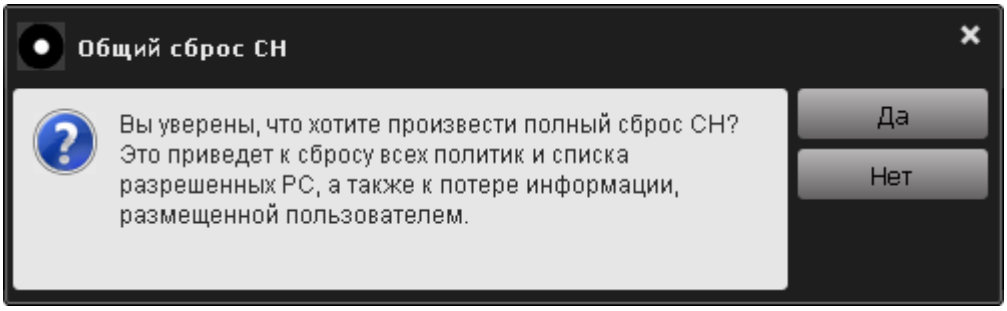

Рисунок 54 – Общий сброс СН

Для подтверждения текущей операции следует нажать кнопку <Да>, для отмены операции – кнопку <Нет>.

По нажатии кнопки <Да> на экране появляется сообщение об успешном выполнении общего сброса СН (рисунок 55).

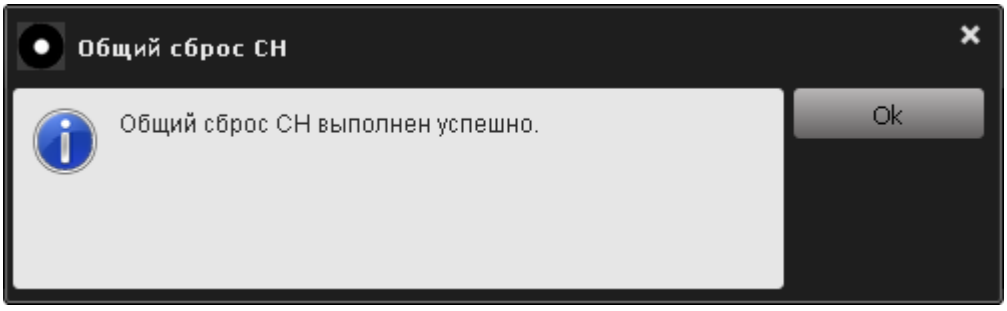

Рисунок 55 – Сообщение об успешном выполнении общего сброса СН

После общего сброса СН на консоли администратора будет доступна только одна функция: «Регистрировать администратора…», так как СН будет приведен в начальное состояние.

3.9. Разблокирование СН

В случае если количество попыток авторизации пользователя превысило допустимый порог, СН блокируется. Пользователь может

разблокировать СН с помощью PUK-кода. Если значение PUK-кода утеряно, разблокировать СН может только администратор с помощью функции аннулирования регистрации пользователя СН (см. подраздел 3.7). Подробное описание процедуры разблокирования СН приведено в «Руководстве пользователя» 11443195.4012.033-34.

3.10. Завершение работы

ВНИМАНИЕ! Перед извлечением СН из USB–порта рекомендуется сначала завершить работу ПО РС. Извлечение СН из USB–порта во время работы ПО РС может привести к некорректному завершению работы консоли пользователя.

Чтобы завершить работу с ПАК «Секрет Особого Назначения», необходимо нажать правой кнопкой мыши на значок СН в трее (рисунок 4) и выбрать в появившемся окне пункт «Выход» (рисунок 5). После этого на экране появляется следующее сообщение (рисунок 56):

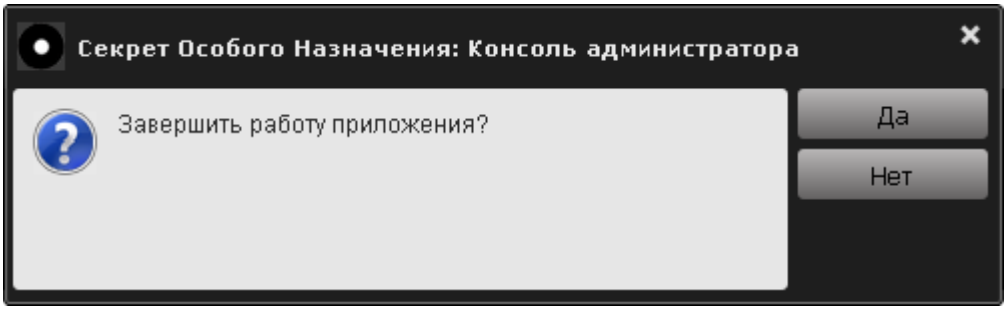

Рисунок 56 – Завершение работы СН

Для подтверждения текущей операции следует нажать кнопку <Да>, для отмены операции – кнопку <Нет>.

4. Рекомендации по организации безопасного применения ПАК «Секрет Особого Назначения»

4.1. Общие сведения

При применении ПАК «Секрет Особого Назначения» 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 Особого Назначения» 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.

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

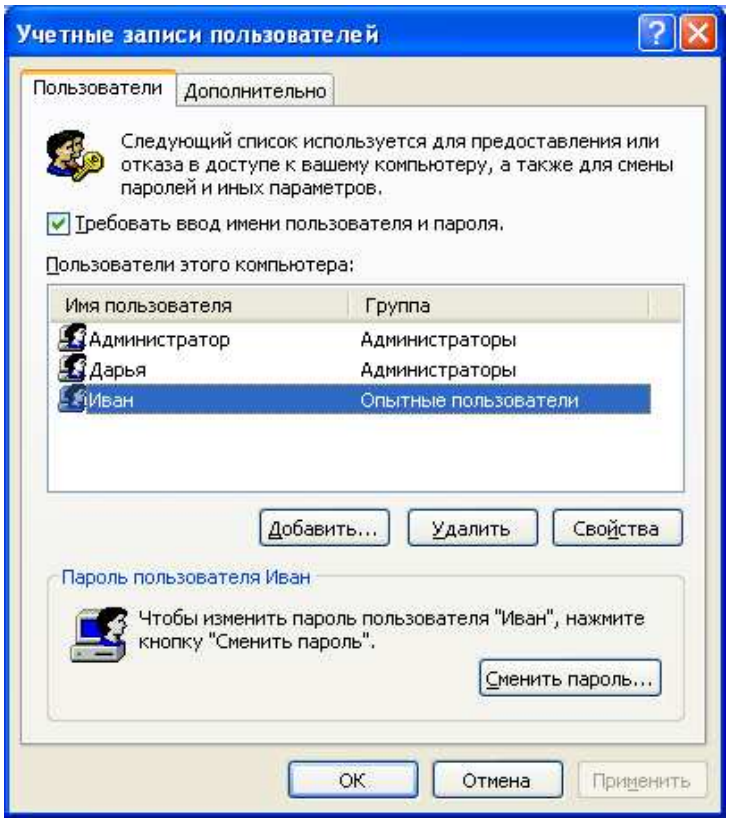

Рисунок 57 – Окно настроек учетных записей пользователей

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 58).

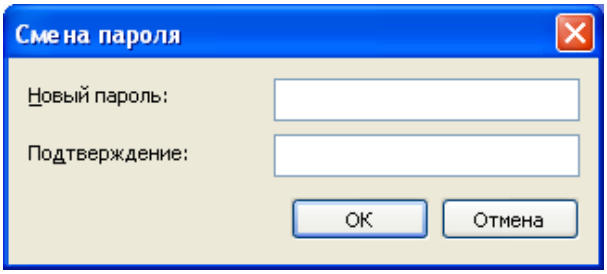

Рисунок 58 – Окно смены пароля пользователя для входа в ОС

4.3. 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 59).

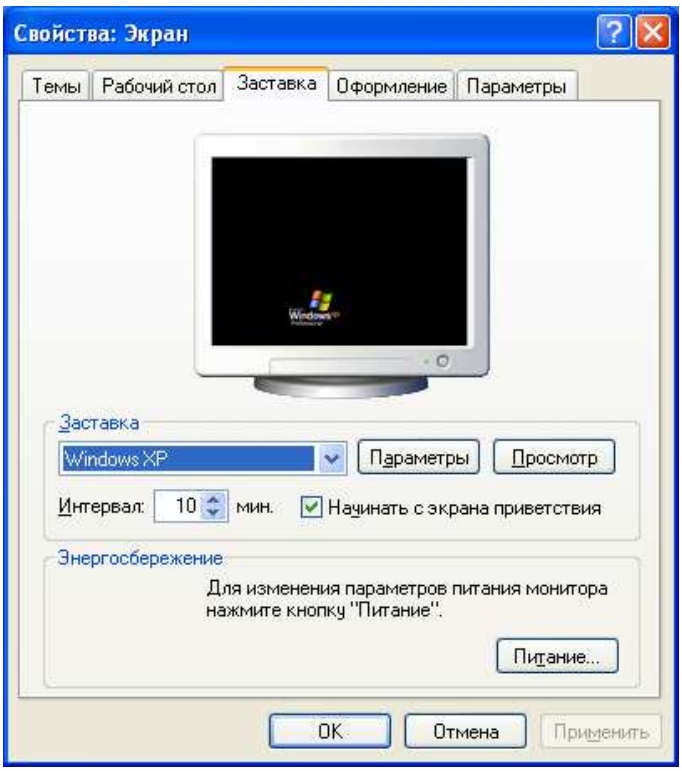

Рисунок 59 – Окно настройки заставки экрана в ОС Windows XP

•*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 60).

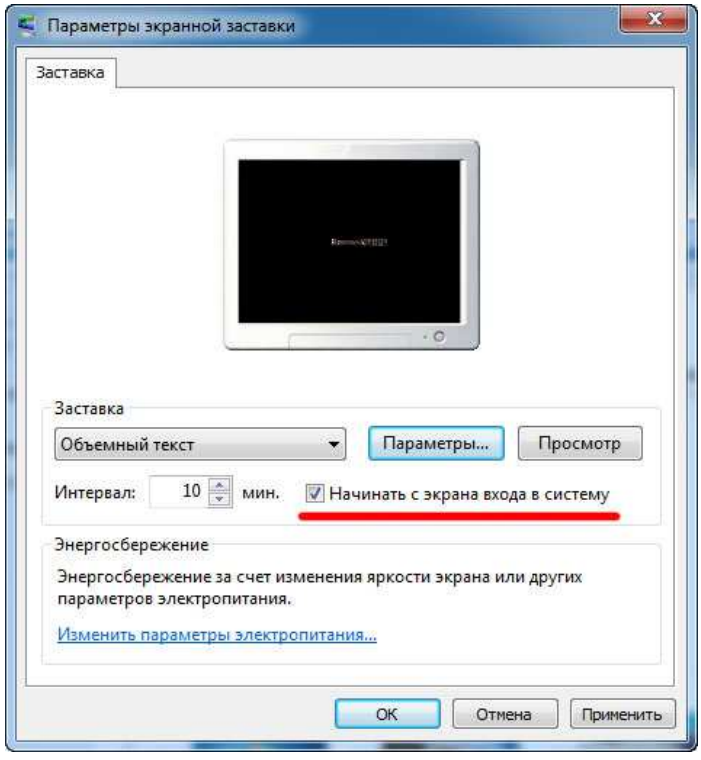

Рисунок 60 - Окно настройки заставки экрана в ОС Windows 7

5. Рекомендации по применению «Секрета Особого Назначения» в личных целях

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

В случае личного использования владелец «Секрета Особого Назначения» выполняет функции как администратора, так и пользователя СН. При этом выполнение процедуры регистрации администратора СН является необязательным (действуют политики доступа по умолчанию, см. 3.2).

«Секрет Особого Назначения» можно использовать для хранения и переноса конфиденциальной информации, только если в СН зарегистрирован пользователь (см. «Руководство пользователя» 11443195.4012.033-34). Доступ к хранимой информации пользователь может получить только после выполнения процедуры авторизации.

Для авторизации необходимо ввести верное значение КА. После успешного завершения процедуры авторизации ПО РС монтирует закрытый диск СН, который становится доступен операционной системе РС. На этом диске пользователь может хранить необходимую защищаемую информацию.

Если авторизация завершилась неудачей, монтирование закрытого диска не производится. В таком случае пользователь не может получить доступ к информации, хранящейся на СН.

В случае достижения предельно допустимого порога неудачных попыток авторизации (определяется политикой КА) СН блокируется. Дальнейшее штатное использование СН возможно только после успешного выполнения операции разблокирования.

Пользователь должен запомнить КА и PUK-код. В случае утраты этих параметров доступ к пользовательским данным, записанным на закрытый диск СН, блокируется. При этом для дальнейшего использования СН администратор СН должен выполнить процедуру аннулирования регистрации пользователя СН.

6. Возможные сообщения в журнале событий ПАК «Секрет Особого Назначения»

Виды возможных сообщений ПАК «Секрет Особого Назначения» и их описание приведены в таблицах 1, 2.

Таблица 1 - Возможные сообщения об ошибках в журнале событий СН и их описание

Сообщение об ошибке	Возможные причины возникновения ошибки	Порядок действий по устранению ошибки
«Ошибка при выполнении протокола установки времени»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола установки описания рабочей станции»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола запроса информации»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола запроса информации о списке разрешенных рабочих станций»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола регистрации администратора»	Неисправность устройства	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен пароль администратора	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола регистрации пользователя»	Неисправность устройства	Повторить операцию. В случае если код авторизации введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неверно введен код авторизации	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола смены ключа авторизации»	Неверно введен код авторизации	Повторить операцию. В случае если код авторизации введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки

Сообщение об ошибке	**Возможные причины возникновения ошибки**	**Порядок действий по устранению ошибки**
	Неисправность устройства	
«Ошибка при выполнении протокола разблокирования»	Неверно введен код авторизации	Повторить операцию. В случае если код авторизации введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола установки политики использования кода авторизации»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола установки политики доступа к рабочим станциям»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола смены пароля администратора»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола установки списка разрешенных рабочих станций»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола форматирования устройства»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола авторизации пользователя»	Неисправность устройства	Повторить операцию. В случае если код авторизации введен верно, но сообщение на экране появляется снова, следует обратиться в службу
	Неверно введен код авторизации	
	Программная ошибка в процессе выполнения операции	

Сообщение об ошибке	**Возможные причины возникновения ошибки**	**Порядок действий по устранению ошибки**
		технической поддержки
«Ошибка при выполнении протокола установки политики заполнения журнала»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола разрешения просмотра журнала событий»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола очистки журнала событий»	Неверно введен пароль администратора	Повторить операцию. В случае если пароль администратора введен верно, но сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола обновления программного обеспечения»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола сброса носителя»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении протокола персонализации носителя»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Неподдерживаемый тип протокола»	Неисправность устройства	Повторить операцию. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Достигнут предел неудачных попыток ввода пароля администратора.»	Достигнут предел неудачных попыток ввода пароля администратора	Извлечь и вновь подключить СН из USB – порта. В случае если сообщение на экране появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	

Таблица 2 – Возможные информационные сообщения в журнале событий СН и их описание

Информационное сообщение	Описание
«Успешное завершение протокола установки времени»	Запрос информации о списке разрешенных рабочих станций завершен успешно
«Успешное завершение протокола установки описания рабочей станции»	Регистрация администратора завершена успешно
«Успешное завершение протокола запроса информации»	Регистрация пользователя завершена успешно
«Успешное завершение протокола запроса информации о списке разрешенных рабочих станций»	Смена ключа авторизации завершена успешно
«Успешное завершение протокола регистрации администратора»	Разблокирование СН завершено успешно
«Успешное завершение протокола регистрации пользователя»	Установка политики использования кода авторизации завершена успешно
«Успешное завершение протокола смены ключа авторизации»	Установка политики доступа к рабочим станциям завершена успешно
«Успешное завершение протокола разблокирования»	Смена пароля администратора выполнена успешно
«Успешное завершение протокола установки политики использования кода авторизации»	Установка списка разрешенных рабочих станций завершена успешно
«Успешное завершение протокола установки политики доступа к рабочим станциям»	Форматирование устройства завершено успешно
«Успешное завершение протокола смены пароля администратора»	Авторизация пользователя завершена успешно
«Успешное завершение протокола установки списка разрешенных рабочих станций»	Установка политики заполнения журнала событий СН выполнена успешно
«Успешное завершение протокола форматирования устройства»	Доступ к журналу событий СН выполнен успешно
«Успешное завершение протокола авторизации пользователя»	Очистка журнала событий СН выполнена успешно
«Успешное завершение протокола установки политики заполнения журнала»	Обновление программного обеспечения завершено успешно
«Успешное завершение протокола разрешения просмотра журнала событий»	Сброс носителя выполнен успешно
«Успешное завершение протокола очистки журнала событий»	Идентификационная информация рабочей станции, на которой использовался СН
«Успешное завершение протокола обновления программного обеспечения»	Запрос информации о списке разрешенных рабочих станций завершен успешно
«Успешное завершение протокола сброса носителя»	Регистрация администратора завершена успешно
«Имя РС Серийный номер МП, Серийный номер ОС, Имя РС, Домен (рабочая группа), Серийный номер АМДЗ»	Регистрация пользователя завершена успешно

7. Перечень принятых сокращений и обозначений

АМДЗ	–	аппаратный модуль доверенной загрузки;
ДСЧ	–	датчик случайных чисел;
СН	–	специальный носитель;
КА	–	код авторизации;
НСД	–	несанкционированный доступ;
ОС	–	операционная система;
ПАК	–	программно-аппаратный комплекс;
ПО	–	программное обеспечение;
ПСП	–	псевдослучайная последовательность;
РС	–	рабочая станция;
NAND	–	флэш-память типа И-НЕ (NOT AND);
PUK	–	Personal Unblocking Key;
USB	–	Universal Serial Bus.