



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

**Программно-аппаратный комплекс
защищенного хранения информации
«Секрет Особого Назначения»**

Руководство администратора

37222406.26.20.40.140.094 90

Листов 61

**Москва
2025**

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса «Секрет Особого Назначения» (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	5
1.1. Состав и назначение ПАК «Секрет Особого Назначения»	5
1.2. Технические условия применения комплекса	6
1.3. Комплектность поставки и приемка ПАК «Секрет Особого Назначения»	6
2. Установка и настройка ПАК «Секрет Особого Назначения»	7
2.1. Подключение СН	7
2.2. Запуск ПО РС	7
2.3. Начало работы	8
3. Управление ПАК «Секрет Особого Назначения»	11
3.1. Регистрация администратора	11
3.2. Настройка политик использования СН	15
3.2.1. Настройка политики доступа к СН на РС	15
3.2.2. Временное снятие ограничений на доступ к СН на РС.....	16
3.2.3. Настройка реакции при заполнении объема, выделенного для хранения журнала	17
3.2.4. Настройка политики использования КА	18
3.2.5. Сохранение политик СН.....	18
3.3. Управление списком разрешенных РС	20
3.3.1. Общие сведения	20
3.3.2. Добавление текущей РС в список разрешенных	21
3.3.3. Добавление удаленной РС в список разрешенных.....	21
3.3.4. Сохранение РС в списке разрешенных	28
3.3.5. Удаление РС из списка разрешенных	29
3.4. Просмотр журнала событий СН	31
3.5. Смена пароля администратора.....	36
3.6. Аннулирование регистрации пользователя СН	38
3.7. Установка размеров журнала и закрытого раздела диска СН	39
3.8. Общий сброс СН	40
3.9. Установка внутреннего времени	42
3.10. Разблокирование СН.....	43
3.11. Изменение буквы открытого раздела ПАК «Секрет Особого Назначения»	43
3.12. Завершение работы	44
4. Рекомендации по организации безопасного применения ПАК «Секрет Особого Назначения»	45
4.1. Общие сведения	45
4.2. Установка входа пользователя в систему с обязательным вводом пароля	45

4.3.	Включение режима автоматической блокировки экрана.....	46
5.	Настройки для обеспечения работы ПАК «Секрет Особого Назначения» в режиме терминальной сессии.....	48
6.	Рекомендации по применению «Секрета Особого Назначения» в личных целях	53
7.	Возможные сообщения в журнале событий ПАК «Секрет Особого Назначения»	54
8.	Перечень принятых сокращений и обозначений	61

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), 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 с внутренней памятью, используемой для хранения внутреннего ПО СН и служебной информации;
- 2) физический датчик случайных чисел;
- 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 Windows 10 Professional и Astra Linux Special Edition (РУСБ.10015-01) (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.

Поскольку ПАК «Секрет Особого Назначения» оперирует в своей работе определенным набором команд фиксированного формата, а все данные, которые он использует в процессе работы, сохраняются в его внутренней памяти, никакие скрытые каналы не могут влиять на работу комплекса. Соответствующие результаты анализа скрытых каналов отражены в документе «Протокол анализа уязвимостей программно-аппаратного комплекса защищенного хранения информации «Секрет Особого Назначения» и среды его функционирования 37222406.26.20.40.140.094 ПАУ» п.3.4.

Основные особенности ПАК «Секрет Особого Назначения»:

- ПО РС «Секрета Особого Назначения» размещается на открытом диске СН и выполняется без установки на жесткий диск РС;
- предусмотрена возможность задания правил доступа к защищаемой информации посредством настройки политик;

- предусмотрена возможность задания размеров журнала событий СН и закрытого раздела диска СН, на котором хранится пользовательская информация;
- предусмотрена возможность добавления удаленных СВТ, на которых планируется использовать ПАК «Секрет Особого Назначения», в список разрешенных РС;
- ведется журнал работы СН, содержащийся на закрытом разделе флеш-диска СН. По достижении выделенного объема раздела диска СН, на котором хранятся файлы журнала СН, ПО РС информирует пользователя СН о том, что объем журнала событий СН заполнен.

1.2. Технические условия применения комплекса

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

- установленная на PC ОС Windows 10 Professional и Astra Linux Special Edition (РУСБ.10015-01) (x32 или x64);
- свободный разъем USB.

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 и приемка ПАК «Секрет Особого Назначения»

ПАК «Секрет Особого Назначения» поставляется в составе:

- СН;
- гарантийный талон;
- комплект упаковки.

При приемке администратор обязан заполнить таблицу раздела 9 Формуляра 37222406.26.20.40.140.094 ФО, внося в нее сведения о закреплении ПАК «Секрет Особого Назначения» при эксплуатации.

2. Установка и настройка ПАК «Секрет Особого Назначения»

2.1. Подключение СН

Подключение осуществляется установкой СН в свободный USB-разъем системного блока РС¹. При этом допускается использование USB -хаба с внешним источником питания (см. 1.2).

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



Рисунок 1 - Оповещение об обнаружении СН

Далее происходит автоматическая установка системного драйвера.

2.2. Запуск ПО РС

Для работы на РС ОС семейства Windows установка ПО не требуется: данное ПО записывается на открытый диск СН при изготовлении. При работе на РС ОС семейства Linux администратор устанавливает ПО в соответствии с «Руководством по установке» (37222406.26.20.40.140.094 98).

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.

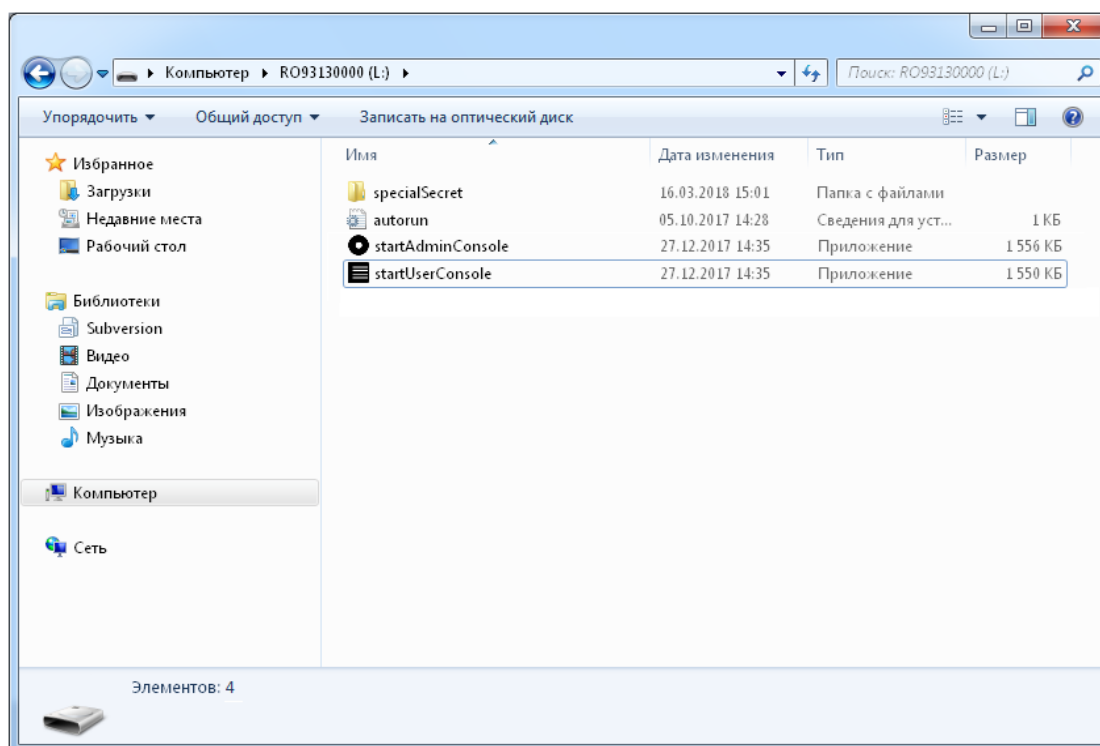


Рисунок 2 – Содержимое открытого раздела флеш-диска СН

2.3. Начало работы

До начала использования ПАК «Секрет Особого Назначения» на PC должно быть выполнено подключение СН (п. 2.1), произведена установка системного драйвера СН. 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. п. 6.15 документа «ПАК СЗИ НСД «АККОРД-Win32». Установка правил разграничения доступа. Программа ACED32» или п. 6.15 документа «ПАК СЗИ НСД «АККОРД-Win64». Установка правил разграничения доступа. Программа ACED32»).

Следующий шаг – запуск ПО PC (консоли администратора) (п. 2.2). Консоль администратора не может быть запущена на исполнение в рамках терминальной сессии.

Далее выполняются процедуры регистрации администратора (п. 3.1) и пользователя СН (см. «Руководство пользователя» 37222406.26.20.40.140.094 34), в результате выполнения которых формируются пароль администратора и код авторизации пользователя (КА). Эти процедуры выполняются однократно, 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 появляется следующее сообщение (рисунок 3):

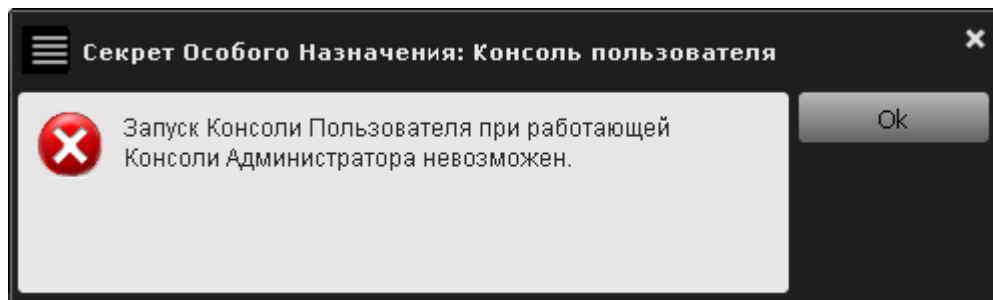


Рисунок 3 – Сообщение о невозможности запуска консоли пользователя при работающей консоли администратора

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 п. 3.5).

Код авторизации пользователя, который формируется в результате выполнения регистрации пользователя (подробнее см. «Руководство пользователя», п. 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. п. 3.2.4) 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;
- задание размеров журнала событий СН и закрытого раздела диска СН, на котором хранится пользовательская информация;
- смена пароля администратора;
- аннулирование регистрации пользователя СН;
- установка внутреннего времени СН (при условии, что используется СН с внутренними часами).

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 (п. 2.2). После этого в трее появляется значок ПАК «Секрет Особого Назначения» (рисунок 4).

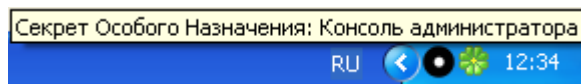


Рисунок 4 – Значок ПАК «Секрет Особого Назначения» в трее

При нажатии на значок СН в трее 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.

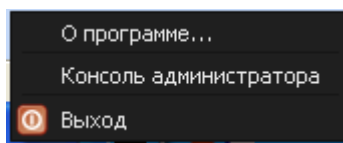


Рисунок 5 – Контекстное меню значка ПАК «Секрет Особого Назначения» в трее

Если процедура регистрации администратора ранее не выполнялась, при запуске консоли администратора активна только функция регистрации администратора (рисунок 6).

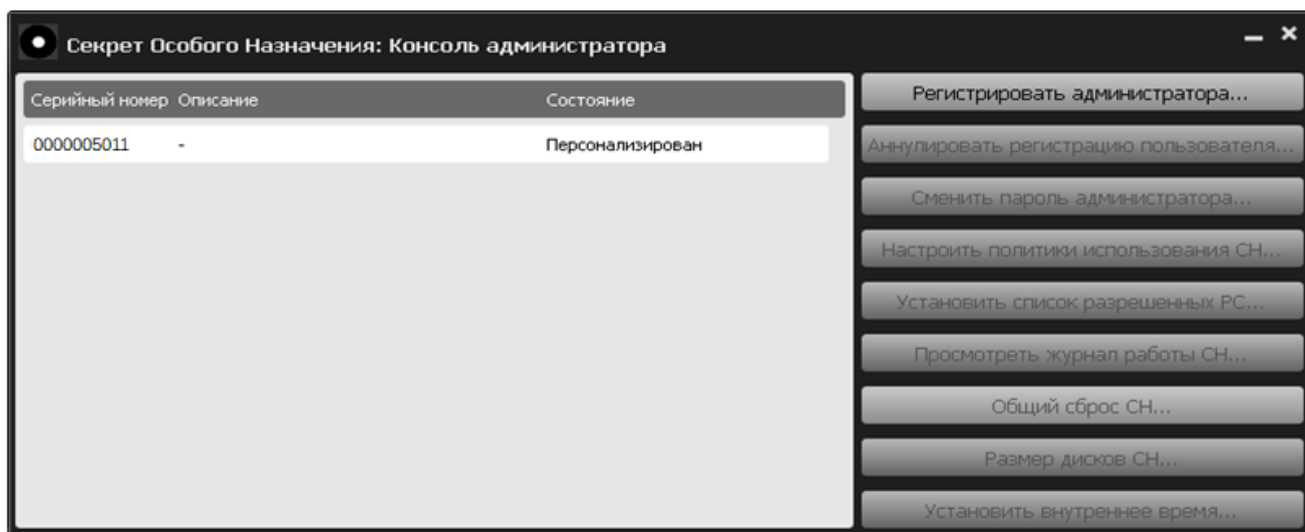


Рисунок 6 – Консоль администратора (в СН не зарегистрирован ни администратор, ни пользователь)

Чтобы зарегистрировать администратора, необходимо нажать кнопку <Регистрировать администратора...>. Появится окно, показанное на рисунке 7.

Рисунок 7 – 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 ввести пароль администратора с подтверждением. Для завершения операции следует нажать кнопку <Ok>, для отмены операции – кнопку <Отмена>. После завершения операции заданные параметры передаются в СН и сохраняются во внутренней памяти устройства.

Регистрационные параметры СН:

- имя «Секрета Особого Назначения». Представляет собой строку, длина которой ограничена 64 произвольными символами. В качестве имени устройства целесообразно использовать одно или несколько слов, характеризующих принадлежность СН (например, должность сотрудника) или его назначение (например, «для отчетов», «оборудование» и т. д.). Имя «Секрета Особого Назначения» необходимо для того, чтобы легко отличать устройства друг от друга. Оно не связано с защитными функциями и задается только для удобства пользователя, поэтому не нужно стремиться к тому, чтобы имя устройства 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. Параметр предназначен для доступа к функциям безопасности.

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить пароль администратора, а также сделать его недоступным для третьих лиц!

Кнопка <ОК> 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 все необходимые параметры, следует нажать кнопку <Ok>, для отмены операции – кнопку <Отмена>.

Если вводимое количество символов пароля администратора меньше установленного минимального значения (6 символов), появится следующее предупреждение (рисунок 8).

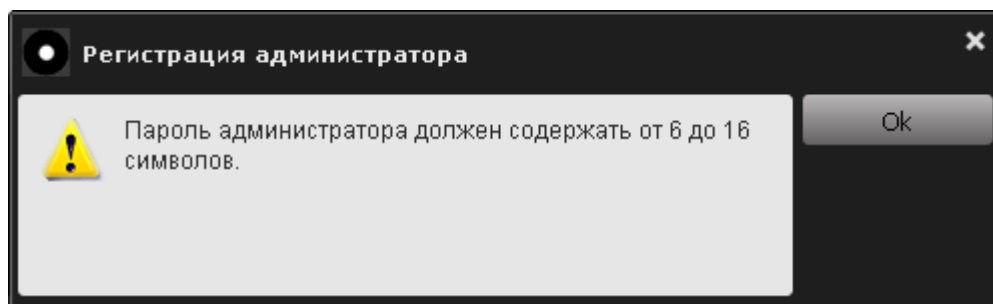


Рисунок 8 – Предупреждение о том, что пароль администратора должен содержать от 6 до 16 символов

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

Если пароль подтвержден неверно, после нажатия кнопки <Ok> выводится соответствующее предупреждение (рисунок 9).

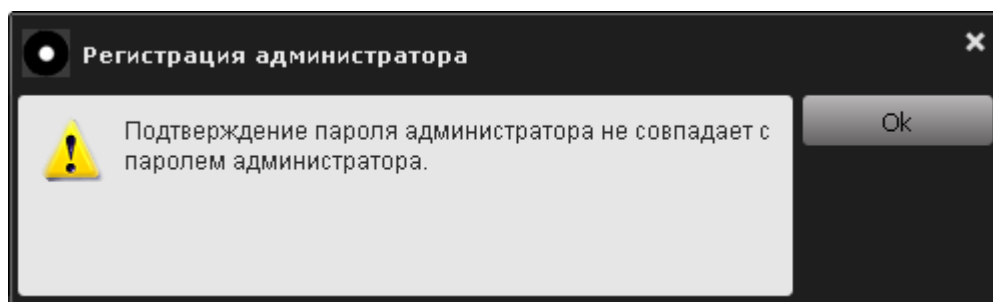


Рисунок 9 – Предупреждение об ошибке при подтверждении пароля администратора

В этом случае следует ввести корректное подтверждение пароля в поле <Подтвердите пароль администратора> (рисунок 7) и нажать <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 10).

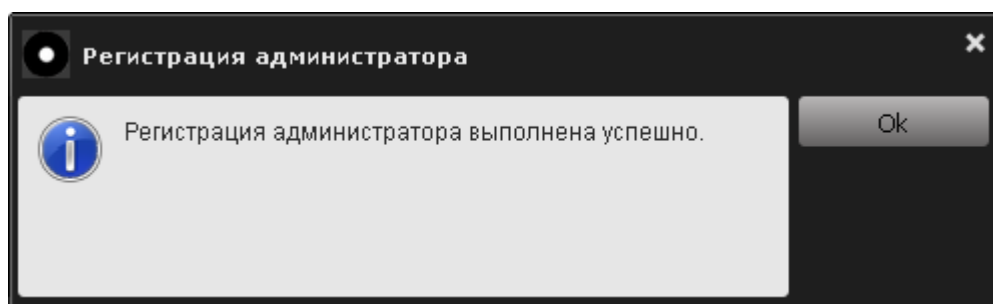


Рисунок 10 – Сообщение об успешной регистрации администратора

37222406.26.20.40.140.094 90

Далее функция регистрации администратора блокируется, в графе «Описание» отображается имя СН, и становятся доступными остальные функции администрирования (рисунок 11).

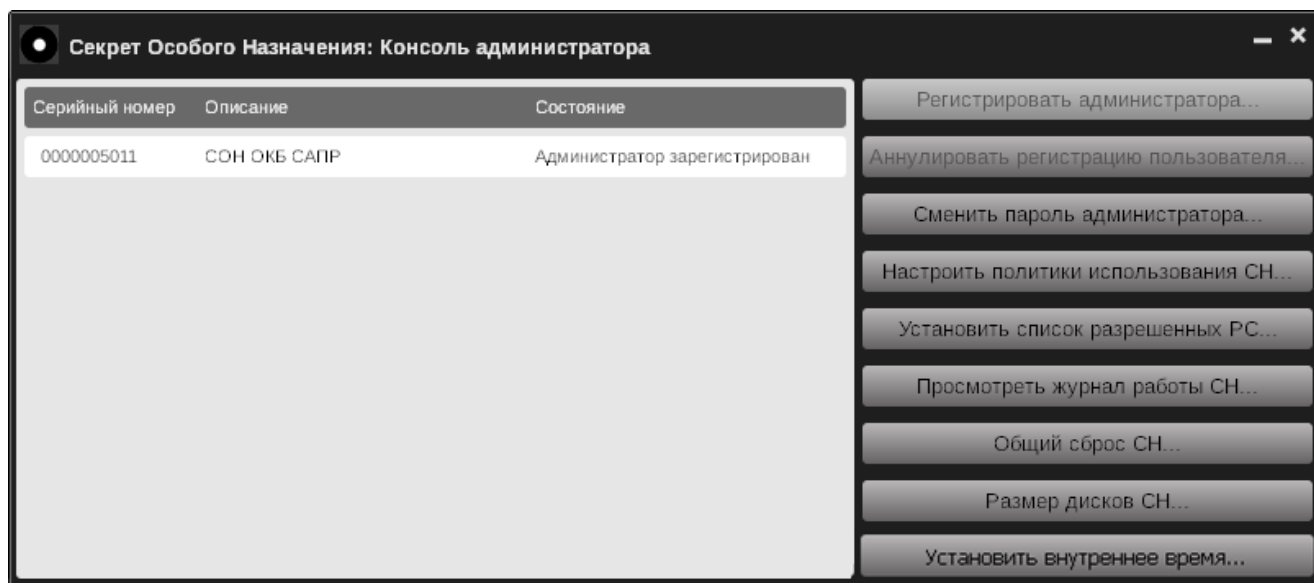


Рисунок 11 – Консоль администратора с доступными опциями

Если в СН зарегистрирован администратор, то в графе «Состояние» отображается «Администратор зарегистрирован» (рисунок 11). После регистрации пользователя в колонке «Состояние» консоли администратора отображается «Пользователь зарегистрирован», и становится доступной функция «Аннулировать регистрацию пользователя...» (рисунок 12).

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.

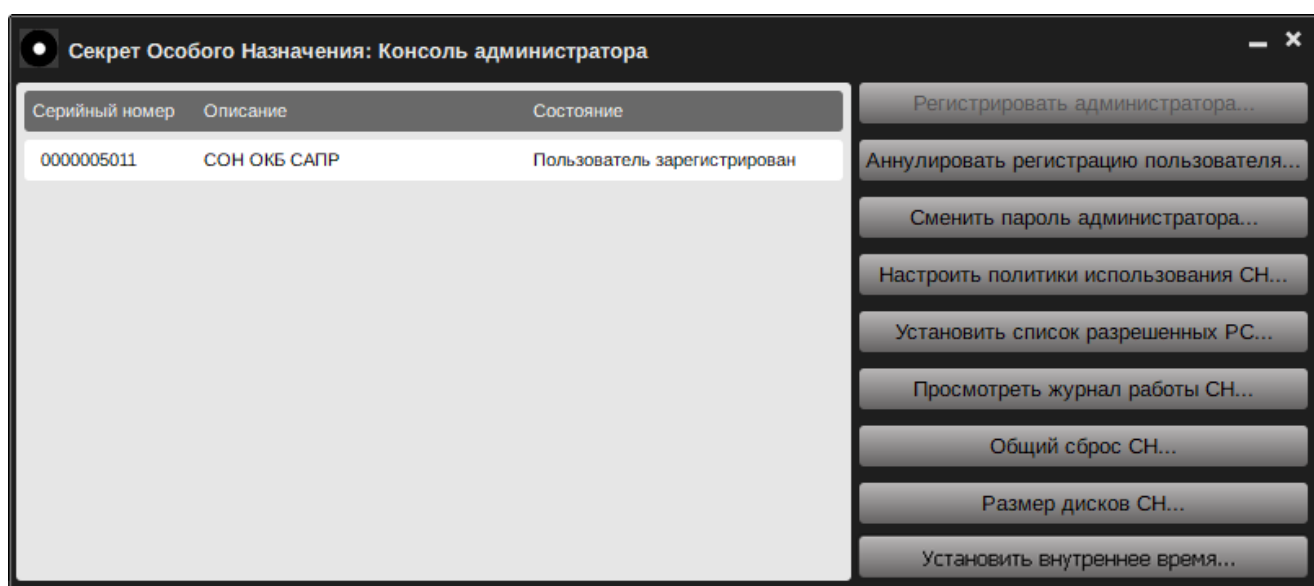


Рисунок 12 – Консоль администратора после регистрации пользователя

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 11) следует выбрать функцию «Настроить политики использования СН...». На экране появляется окно настройки политик СН (рисунок 13).

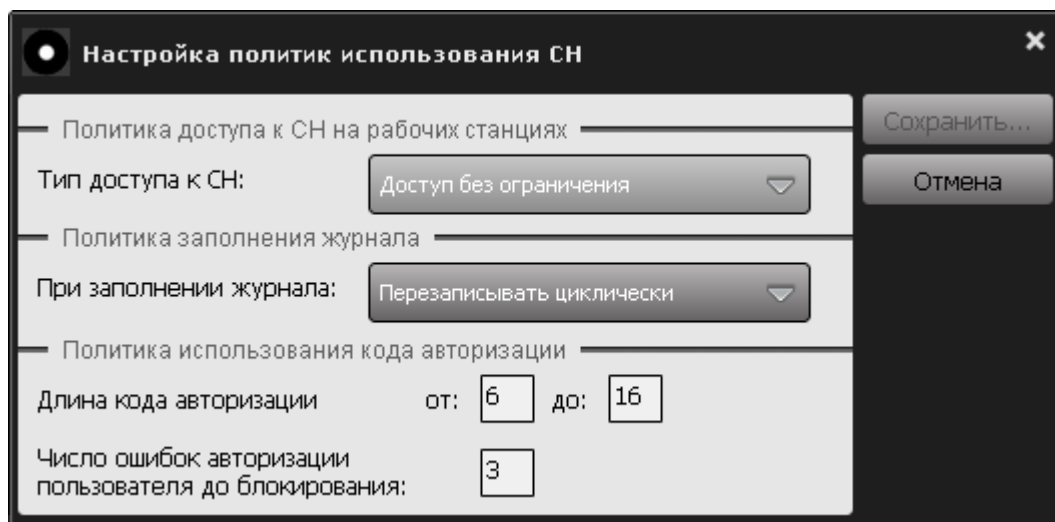


Рисунок 13 – Настройка политик СН

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;
- число ошибок авторизации пользователя до блокирования (минимальное значение параметра – 1, максимальное значение – 255).

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 14).

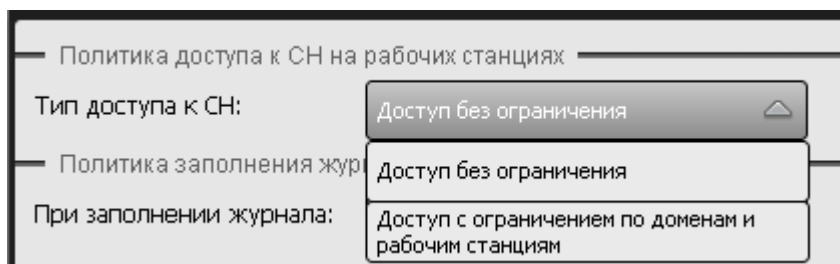


Рисунок 14 – Политика доступа к СН на рабочих станциях

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 3.3.2.

Также при выборе опции «Доступ с ограничением по доменам и рабочим станциям» становится доступной функция временного снятия ограничений на доступ к СН на РС. Функция позволяет задать временной интервал, в течение которого не требуется ограничивать доступ к СН на РС, и описана в п. 3.2.2.

3.2.2. Временное снятие ограничений на доступ к СН на РС

Для случаев, когда для СН установлен доступ с ограничением по доменам и РС, но предполагается его временное использование на компьютерах, не включенных в список разрешенных, в ПАК «Секрет Особого Назначения» предусмотрена функция временного снятия ограничений на доступ к СН на РС.

Границы временного интервала, в котором отсутствуют ограничения доступа к СН на РС, указываются в соответствующих строках при активном флаге «Временно отключить» (рисунок 15).

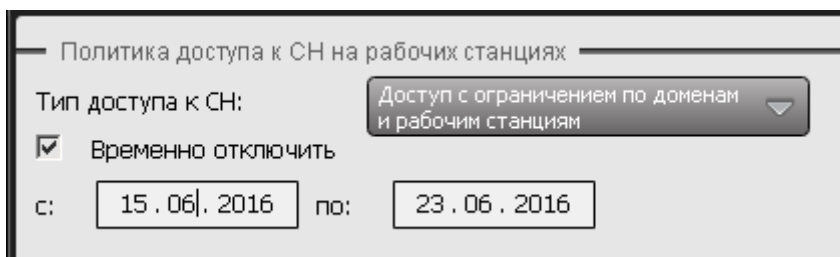


Рисунок 15 – Настройка временного интервала, в котором отсутствуют ограничения доступа к СН на РС

При этом ограничения на доступ к СН на РС перестают действовать на период с 00:00:00 даты начала временного снятия ограничений до 23:59:59 даты его окончания.

После установки временного интервала при каждом подключении СН выполняется проверка текущего времени. Если текущее время входит в интервал, в котором отсутствуют ограничения доступа, пользователю для доступа к закрытому диску СН достаточно пройти авторизацию. Иначе при попытке доступа к закрытому диску СН, помимо авторизации пользователя, выполняется также проверка параметров РС (серийный номер материнской платы, серийный номер ОС, имя РС, имя домена (рабочей группы), серийный номер АМДЗ), и на основании полученных данных устройство разрешает доступ или отказывает в авторизации пользователю при нарушении политики доступа к СН.

Информация о факте временного снятия ограничений на доступ к СН на РС и периоде его действия указана в окне с параметрами СН. Чтобы просмотреть параметры СН, необходимо навести курсор мыши на строку с СН в консоли администратора. При этом появляется окно, изображенное на рисунке 16.

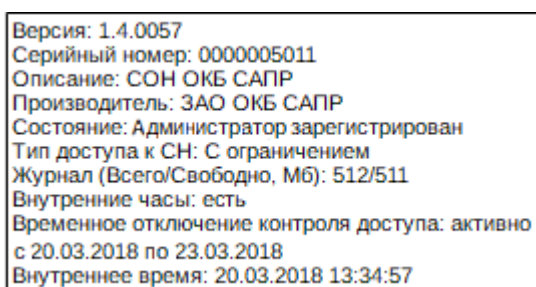


Рисунок 16 – Окно с параметрами СН

Если администратором установлен временной интервал, в котором не требуется ограничивать доступ к СН на РС, в строке «Временное отключение контроля доступа» стоит значение «Активно» и указаны границы временного интервала.

Стоит отметить, что в случае использования СН без внутренних часов в качестве текущего времени принимается системное время. Если СН снабжен внутренними часами, текущее время определяется с их помощью и не зависит от настроек ОС.

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

Экран настройки действий при возможном переполнении журнала событий СН (рисунок 17) позволяет выбрать одно из следующих значений:

- перезаписывать циклически;
- блокировать при переполнении.

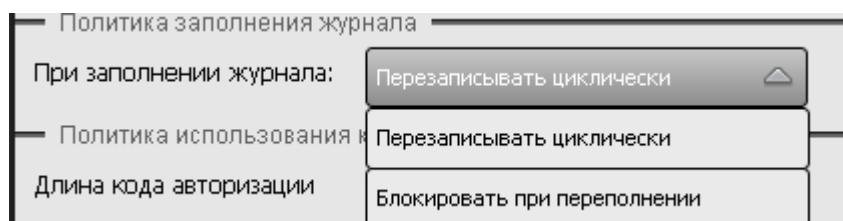


Рисунок 17 – Политика заполнения журнала

В первом случае при заполнении выделенного для хранения журнала объема (512 Мб или другого заданного администратором значения, подробнее см. п. 3.7) 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 (п. 3.4).

3.2.4. Настройка политики использования КА

ВНИМАНИЕ! Функция настройки политики использования КА доступна только в случае, если в СН не зарегистрирован пользователь. В случае корпоративного применения СН не рекомендуется регистрировать пользователя раньше регистрации администратора.

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 18));
- максимальное число неудачных попыток авторизации: при достижении этого порога СН блокируется, и разблокировка возможна только при предъявлении PUK-кода. Это число может варьироваться в пределах от 1 до 255 (по умолчанию установлено значение 3) (рисунок 18).

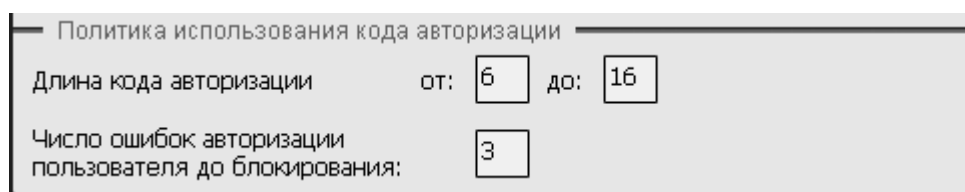


Рисунок 18 – Окно настройки политики использования кода авторизации

3.2.5. Сохранение политик СН

После внесения необходимых изменений в политики СН следует нажать кнопку <Сохранить...>, для отмены внесенных изменений - кнопку <Отмена>.

При нажатии кнопки <Сохранить...> появляется окно запроса пароля администратора (рисунок 19):

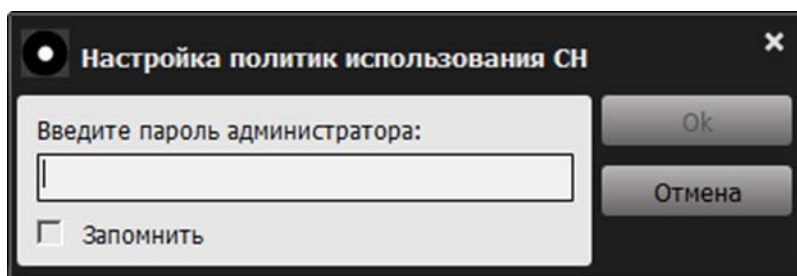


Рисунок 19 – Окно запроса пароля администратора

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

Если пароль администратора введен неверно, на экране отображается сообщение об ошибке (рисунок 20).

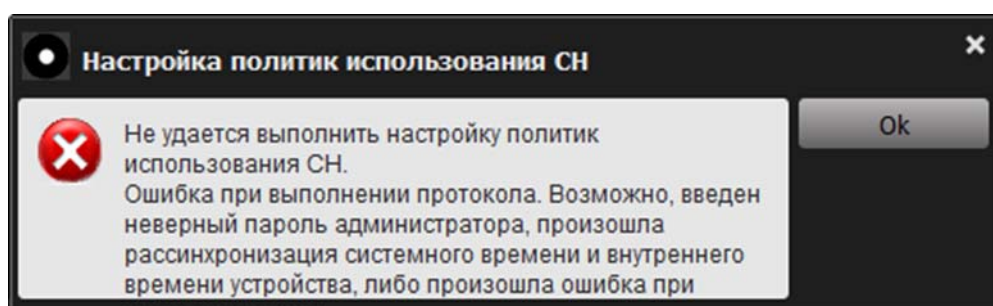


Рисунок 20 – Сообщение об ошибке при сохранении настроек политик использования

В этом случае следует нажать кнопку <Ok> и повторить операцию настройки политик использования СН.

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, появляется сообщение об успешном выполнении настройки политик СН (рисунок 21).

Для продолжения работы с консолью администратора следует нажать кнопку <Ok>.

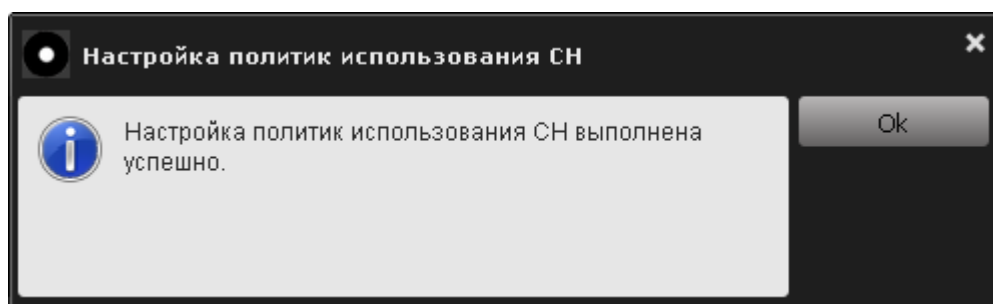


Рисунок 21 – Сообщение об успешном выполнении настройки СН

3.3. Управление списком разрешенных РС

3.3.1. Общие сведения

ПАК «Секрет Особого Назначения» позволяет добавлять в список разрешенных как текущую, так и удаленную РС.

Для каждого СН в список разрешенных РС может быть добавлено не более 32 рабочих станций. Если максимальное число разрешенных РС достигнуто, при попытке добавления в список разрешенных еще одной РС появляется окно, представленное на рисунке 22.

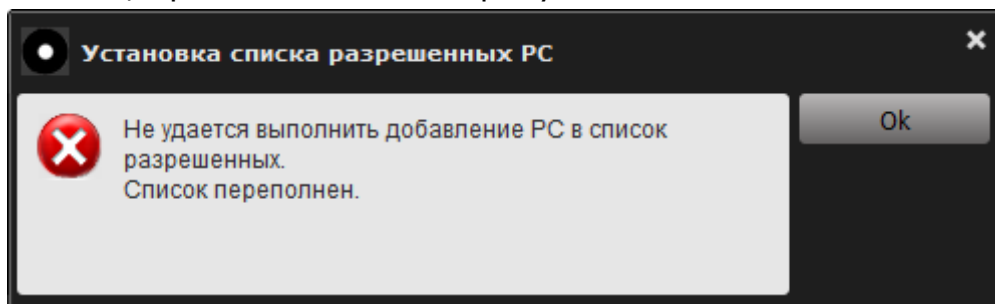


Рисунок 22 – Сообщение о переполнении списка разрешенных РС

Чтобы задать список рабочих станций, на которых должен быть разрешен доступ к СН, в консоли администратора (рисунок 11) необходимо выбрать функцию «Установить список разрешенных РС...». При этом если в списке разрешенных имеются РС, то при выборе функции «Установить список разрешенных РС...» (рисунок 11) появляется окно ввода пароля администратора.

После ввода данных появляется окно установки списка разрешенных РС (рисунок 23).

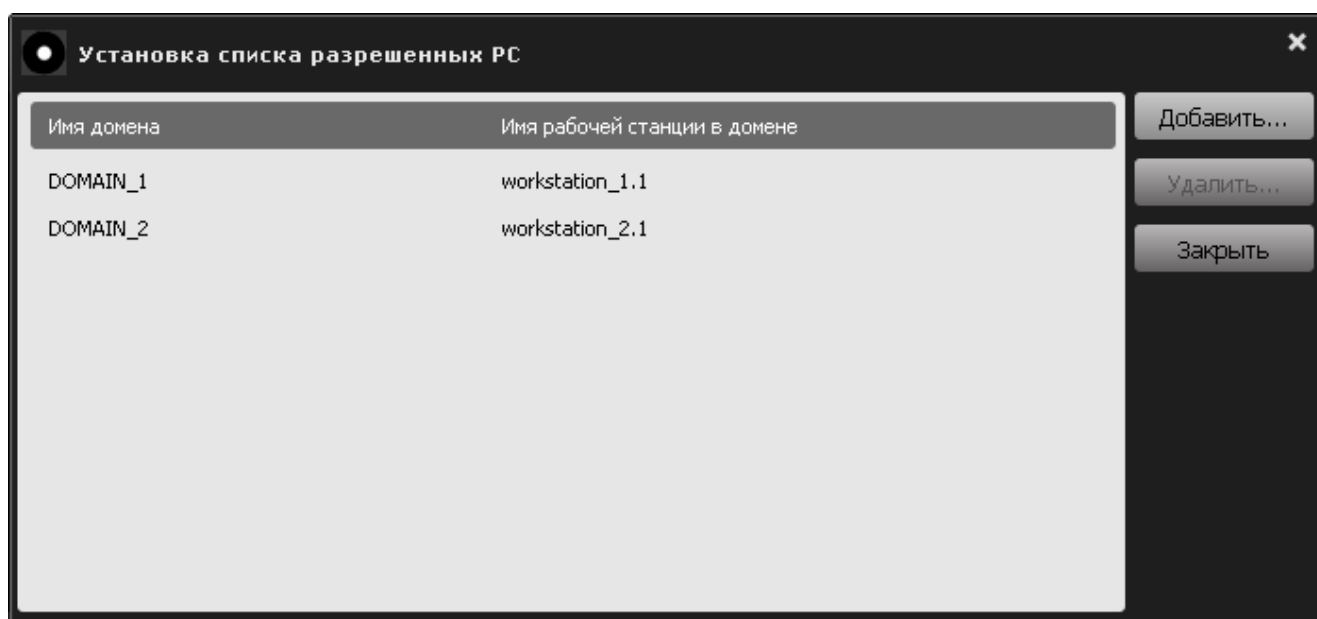


Рисунок 23 – Установка списка разрешенных станций

При нажатии кнопки <Добавить...> появляется окно установки списка разрешенных РС (рисунок 24).

Рисунок 24 – Окно установки списка разрешенных РС

Дальнейшие действия по добавлению РС в список разрешенных зависят от типа РС (текущая или удаленная).

3.3.2. Добавление текущей РС в список разрешенных

Для добавления текущей РС в список разрешенных необходимо нажать кнопку <Текущая РС> в окне, показанном на рисунке 24. При нажатии кнопки появляются имя и домен РС, на которой в данный момент времени работает администратор ПАК «Секрет Особого Назначения».

Администратор ПАК «Секрет Особого назначения» имеет возможность редактировать параметры РС перед ее добавлением в список разрешенных.

3.3.3. Добавление удаленной РС в список разрешенных

3.3.3.1. Добавление удаленной РС вручную

Для добавления удаленной РС в список разрешенных вручную следует в окне, изображенном на рисунке 24, ввести в верхнее поле данного окна имя РС, в нижнее – имя домена (рабочей группы), в котором находится данная РС, а затем нажать кнопку <Сохранить...>.

ВНИМАНИЕ! Имя домена необходимо вводить в формате NetBIOS.

Если рабочая станция с заданным именем в сети не найдена, то появляется следующее сообщение (рисунок 25):

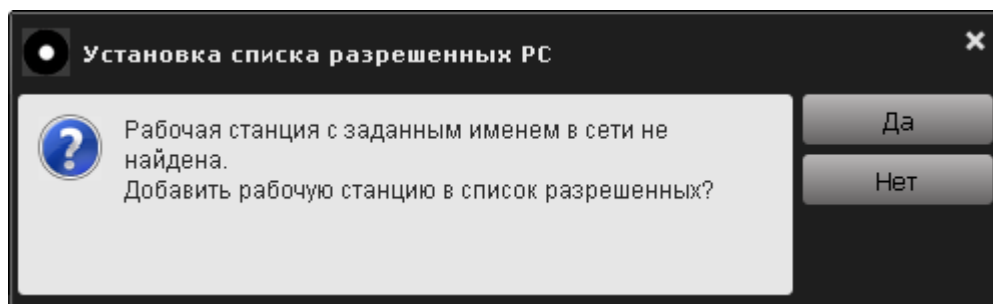


Рисунок 25 – Сообщение о том, что рабочая станция с заданным именем не найдена в сети

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

При нажатии кнопки <Да> появляется окно для ввода пароля (рисунок 26).

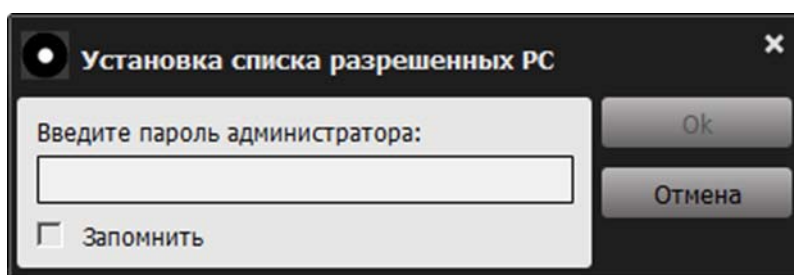


Рисунок 26 – Окно ввода пароля

Если домен с заданным именем в сети не найден, то появляется следующее сообщение (рисунок 27):

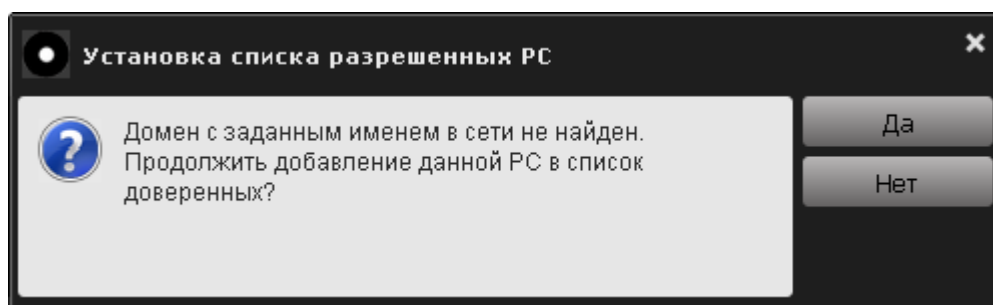


Рисунок 27 – Сообщение о том, что домен с заданным именем не найден в сети

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

При нажатии кнопки <Да> появляется окно для ввода пароля (рисунок 26). Необходимо ввести пароль администратора и нажать <Ok> либо <Отмена> для прерывания текущей операции.

Имя и домен рабочей станции можно выбрать из списка доступных. Для этого следует нажать кнопку <Выбрать из...> (рисунок 24), после чего отобразится окно с доступными доменными именами РС (рисунок 28).

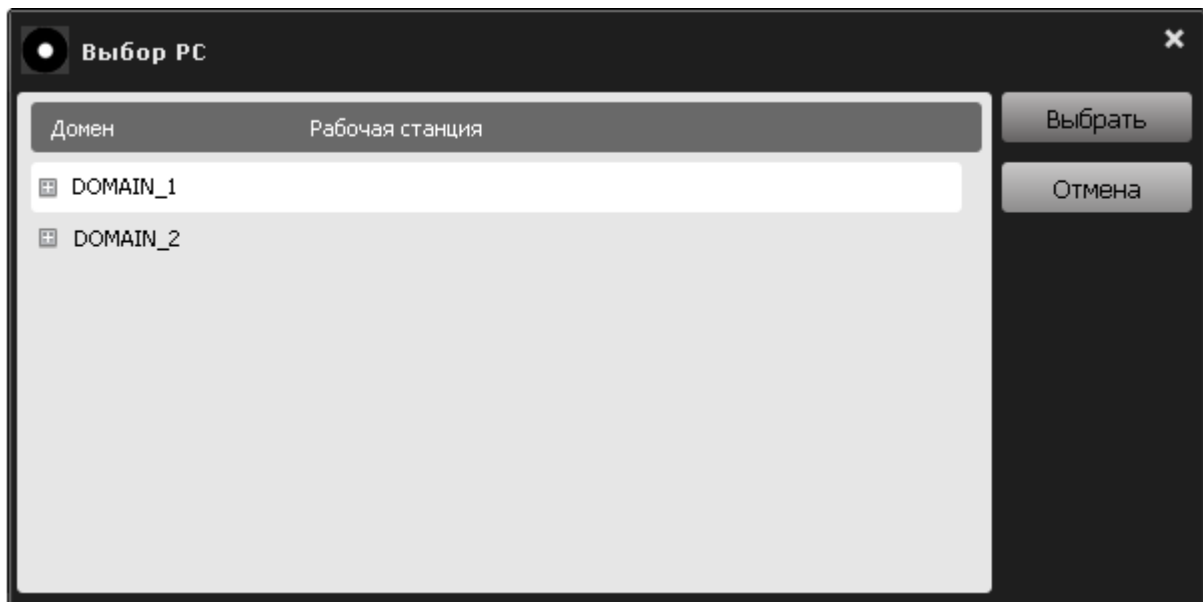


Рисунок 28 – Список доменных имен PC

Следует нажать на кнопку , чтобы увидеть список имен PC, находящихся в доменах (рисунок 29).

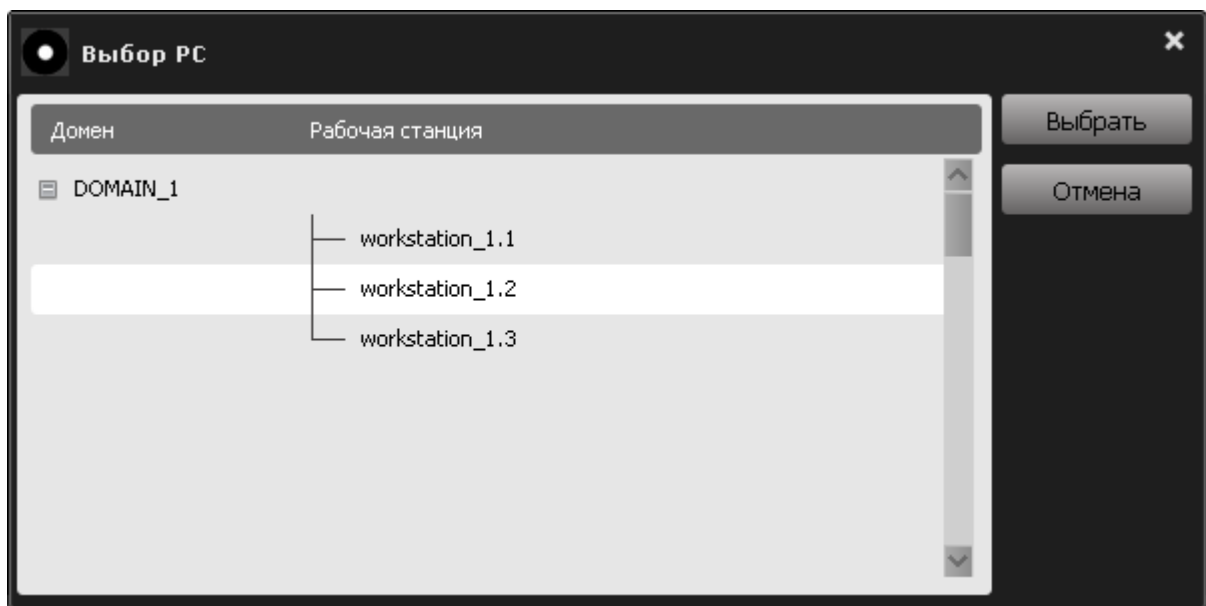


Рисунок 29 – Выбор имени разрешенной рабочей станции

Необходимо отметить нужное имя и нажать кнопку <Выбрать> (рисунок 29). Для отмены текущей операции нажать кнопку <Отмена>.

После выбора нужной PC вновь выводится окно установки списка разрешенных PC (рисунок 24), но в полях этого окна будут записаны имя и домен выбранной PC (рисунок 30).

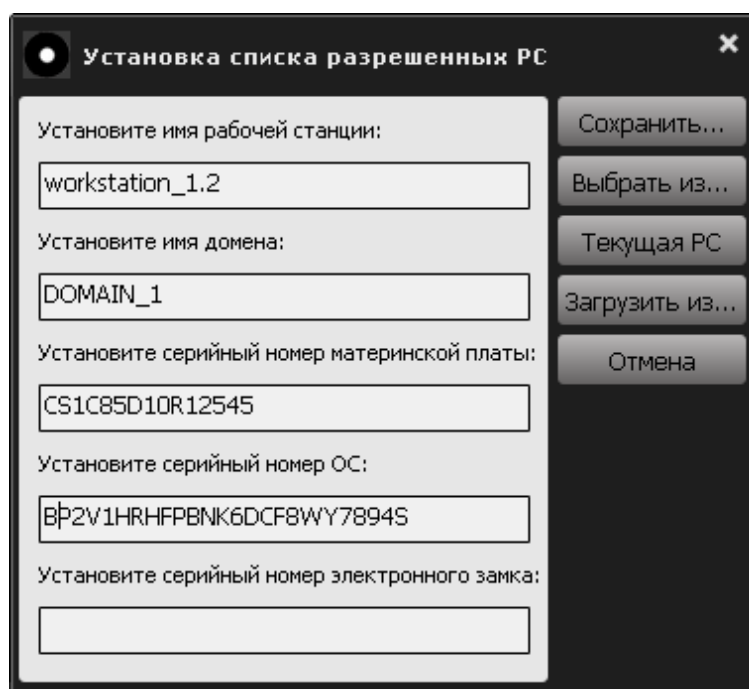


Рисунок 30 – Окно установки списка разрешенных PC с введенными именем и именем домена PC

3.3.3.2. Добавление удаленной PC с помощью утилиты экспорта информации

В ряде случаев возникает необходимость работы ПАК «Секрет Особого Назначения» на компьютерах, которые администратор СН не может добавить в список разрешенных из-за их расположения.

В ПО ПАК «Секрет Особого Назначения» реализована возможность получения информации об удаленных PC с целью добавления их в список разрешенных. Для этого необходимо выполнить следующие действия:

- экспортировать информацию об удаленной PC с помощью специальной утилиты из состава ПО ПАК «Секрет Особого Назначения»;
- передать файл с информацией о PC на СВТ, на котором администратор СН выполняет процедуру добавления PC в список разрешенных;
- добавить удаленную PC в список разрешенных кнопкой <Загрузить из...> окна установки списка разрешенных PC.

Для экспорта информации необходимо на удаленной PC запустить на исполнение утилиту pcInfo.exe, входящую в состав ПО ПАК «Секрет Особого Назначения».

ВНИМАНИЕ! С целью недопущения разглашения информации о PC рекомендуется, чтобы процедуру экспорта информации выполнял администратор PC.

После запуска pcInfo.exe появляется главное окно утилиты (рисунок 31).

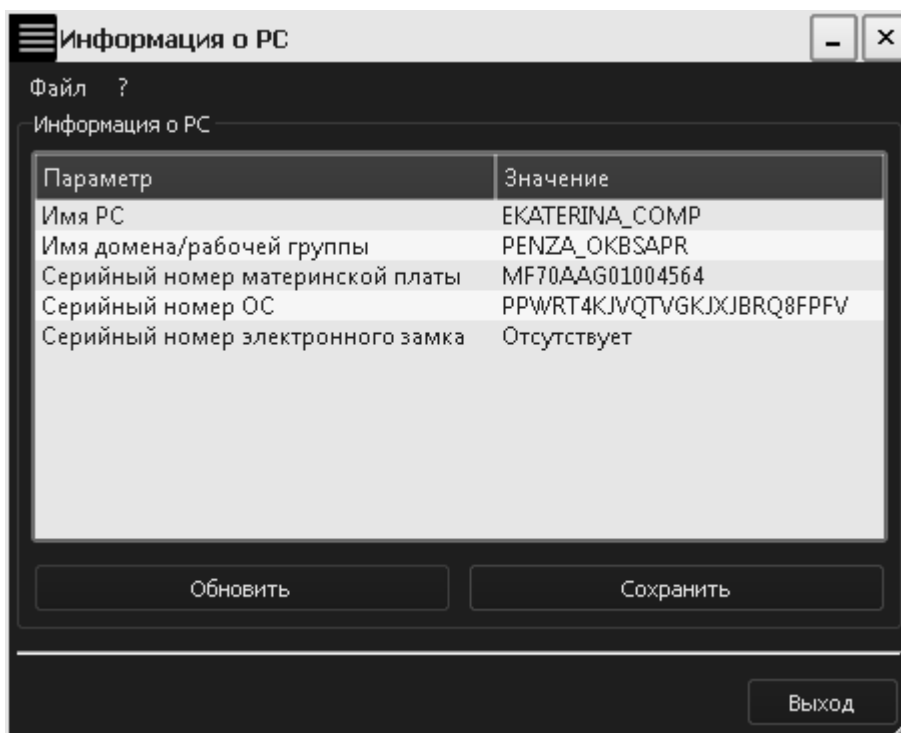


Рисунок 31 – Главное окно утилиты pcInfo.exe

Главное окно утилиты pcInfo.exe отображает следующую информацию о РС:

- имя РС;
- имя домена (рабочей группы);
- серийный номер материнской платы;
- серийный номер ОС;
- серийный номер электронного замка².

При необходимости следует обновить информацию о РС перед ее сохранением в файл.

Чтобы экспортировать информацию о РС в файл, необходимо нажать кнопку <Сохранить> в главном окне утилиты (рисунок 31). Появляется окно, в котором нужно ввести имя сохраняемого файла и нажать кнопку <Сохранить> (рисунок 32).

² При условии наличия на СВТ электронного замка.

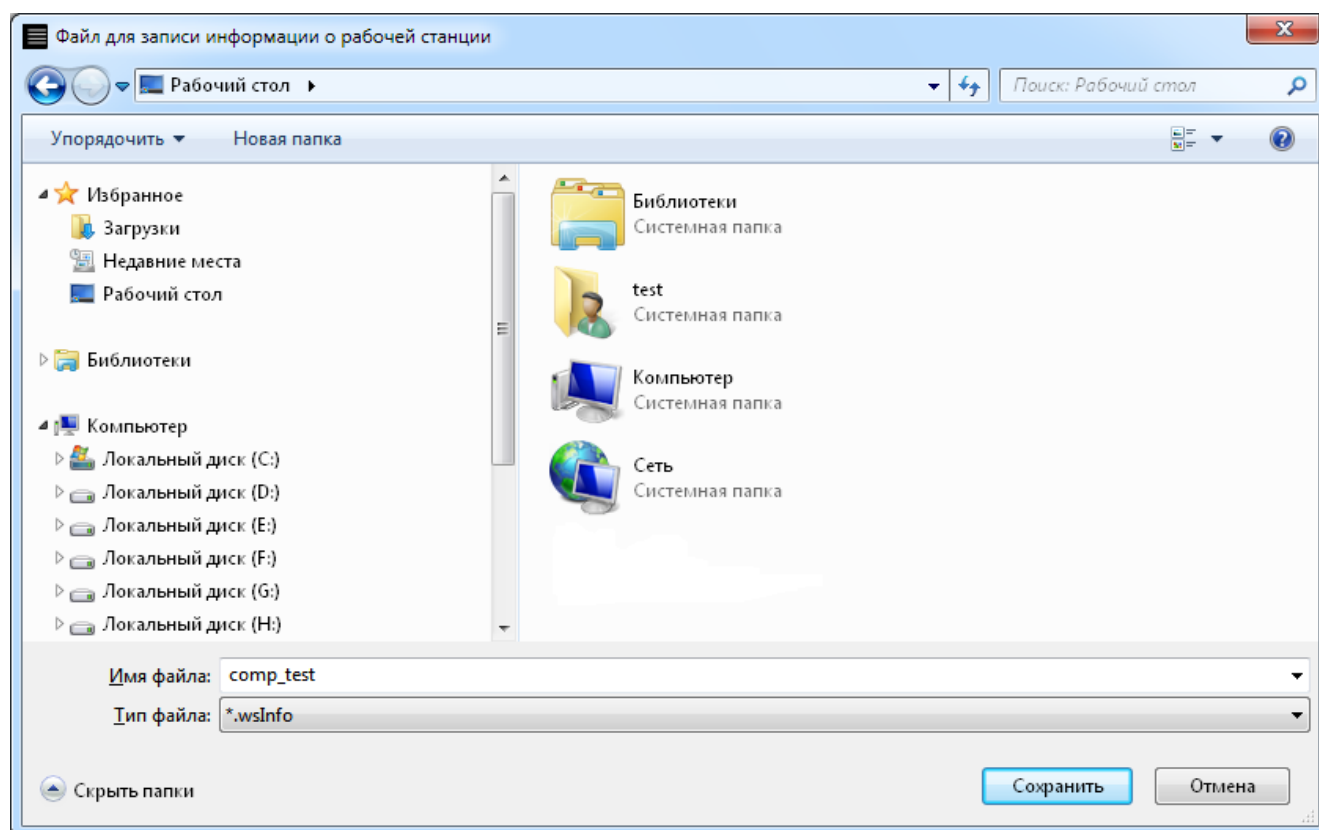


Рисунок 32 – Окно сохранения информации о PC

Если описанная последовательность действий выполнена верно, выводится сообщение об успешном сохранении информации о PC (рисунок 33).

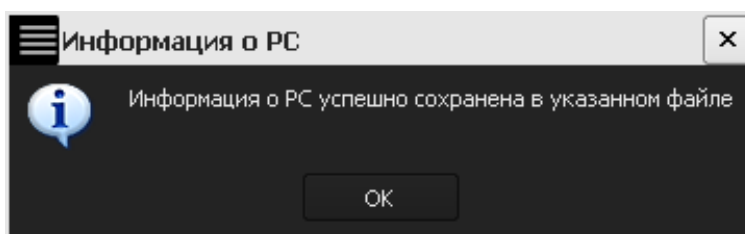


Рисунок 33 – Сообщение об успешном сохранении информации о PC

Для завершения работы с приложением нажать кнопку <Выход> в окне на рисунке 31 (либо выбрать команду Файл\Выход). На экране появится следующее сообщение (рисунок 34):

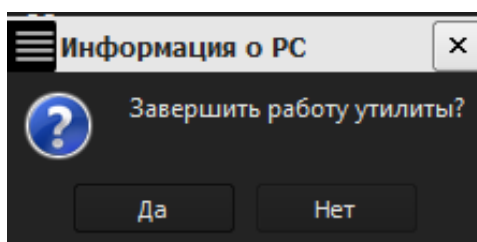


Рисунок 34 – Завершение работы утилиты pcInfo.exe

Затем файл с информацией о РС должен быть передан администратору ПАК «Секрет Особого Назначения». Выбор способа передачи файла оставляется на усмотрение эксплуатирующей организации.

Далее администратору ПАК «Секрет Особого Назначения» следует выполнить процедуру добавления информации об удаленной РС в список разрешенных:

- в консоли администратора (рисунок 11) выбрать функцию «Установить список разрешенных РС...»;
- в появившемся окне (рисунок 23) выбрать кнопку <Добавить...>;
- далее в окне выбора рабочей станции нажать кнопку <Загрузить из...>.

После этого появляется окно, в котором необходимо выбрать файл с информацией об удаленной РС и нажать кнопку <Открыть> (рисунок 35).

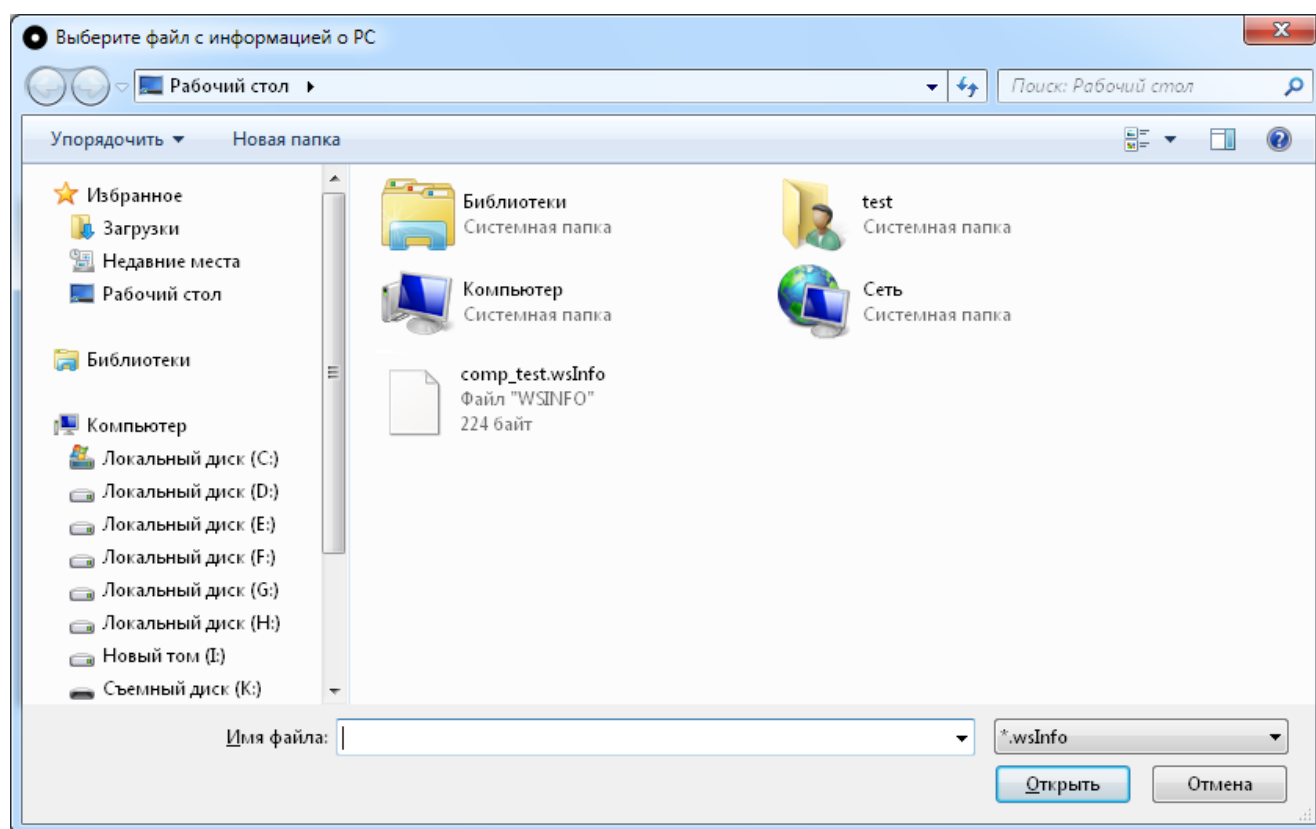


Рисунок 35 – Импорт информации об удаленной РС

При этом поля окна выбора РС заполняются импортированной информацией об удаленной РС (рисунок 36).

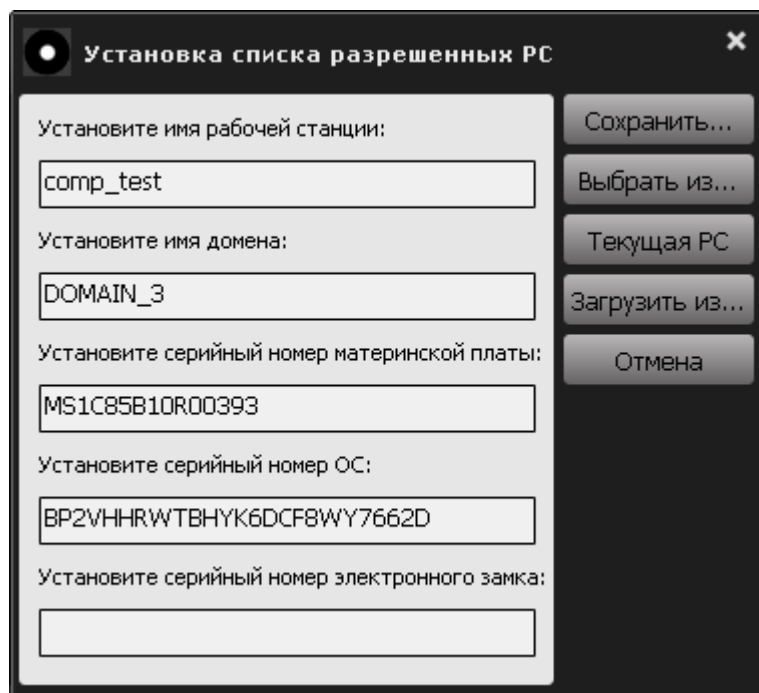


Рисунок 36 – Установка списка разрешенных PC: поля окна выбора рабочей станции заполнены импортированной информацией об удаленной PC

3.3.4. Сохранение PC в списке разрешенных

Для сохранения данных, введенных в окне установки списка разрешенных PC, следует нажать кнопку <Сохранить...>, для отмены операции нажать <Отмена>.

При нажатии кнопки <Сохранить...> появится окно ввода пароля администратора (рисунок 26); после его ввода нажать <Ok>, для прерывания текущей операции нажать <Отмена>.

Если пароль введен некорректно, появляется сообщение об ошибке при установке списка разрешенных PC (рисунок 37).

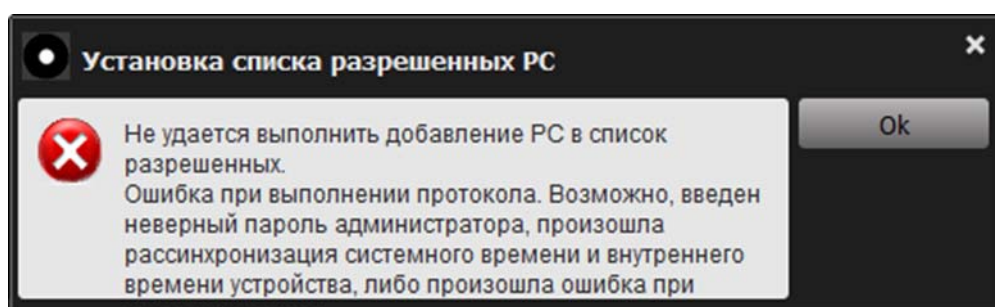


Рисунок 37 – Сообщение об ошибке в процессе добавления PC в список разрешенных

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

Если операция установки списка разрешенных PC выполнена корректно, то отображается сообщение об успешном завершении установки списка разрешенных PC (рисунок 38).

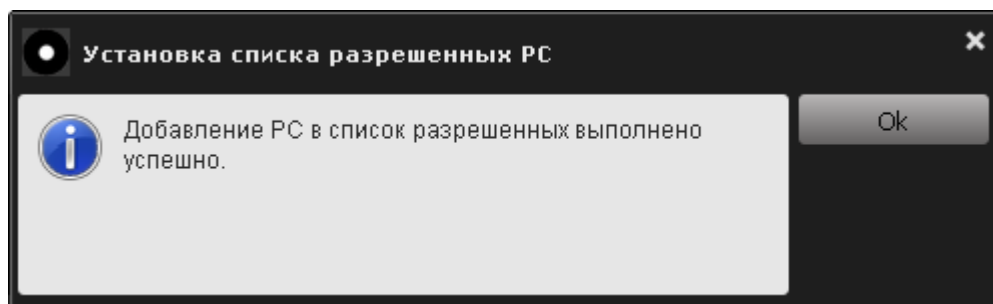


Рисунок 38 – Сообщение об успешном выполнении установки разрешенных РС

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

При необходимости добавления в список разрешенных нескольких РС следует повторить описанную процедуру для каждой РС.

При первом подключении СН к РС из числа разрешенных внутреннее ПО СН производит считывание и сохранение внутри устройства информации о параметрах оборудования данной РС. 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.

В целях обеспечения возможности использования ПАК «Секрет Особого назначения» в режиме терминальной сессии при включенной политике доступа с ограничением по доменам и рабочим станциям (п. 3.2.1) в список разрешенных РС необходимо добавить имя и домен (рабочую группу) терминального сервера.

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 появляется оповещение (рисунок 39) о том, что внесенные изменения вступят в силу после установки типа доступа к РС «Доступ с ограничением по доменам и рабочим станциям».

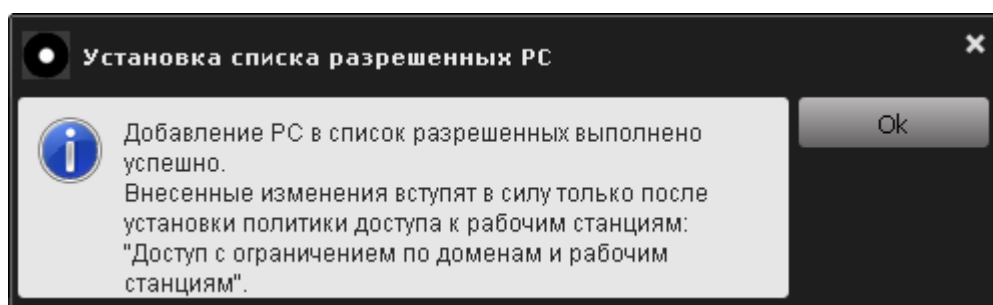


Рисунок 39 – Сообщение о внесенных изменениях

3.3.5. 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 40).



Рисунок 40 – Список разрешенных PC

После этого появляется окно, показанное на рисунке 26.

Нужно ввести пароль администратора, после чего нажать <Ok>, для отмены операции нажать <Отмена>.

Если пароль администратора введен некорректно, появляется сообщение об ошибке при выполнении операции удаления PC из списка разрешенных (рисунок 41).

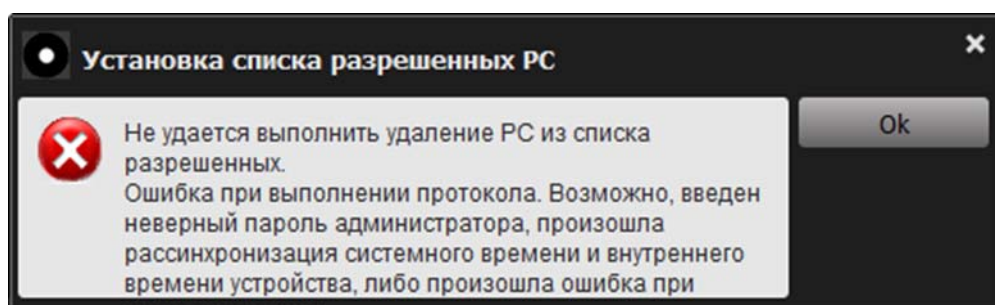


Рисунок 41 – Сообщение об ошибке при выполнении операции удаления разрешенной PC

В этом случае нажать <Ok> и повторить процедуру удаления PC из списка разрешенных.

Если операция удаления разрешенной PC выполнена корректно, отображается сообщение об успешном удалении PC из списка разрешенных (рисунок 42):

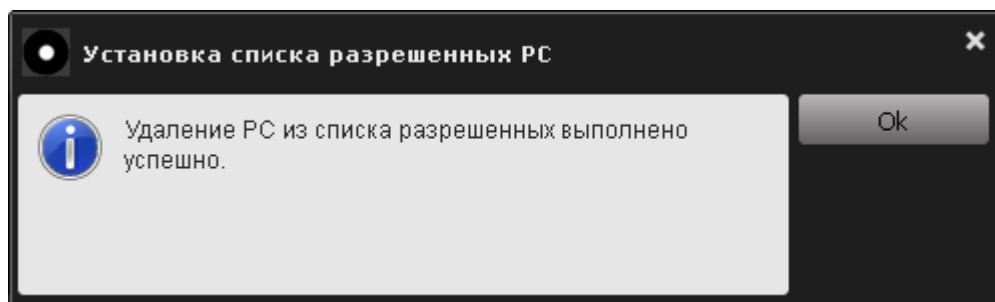


Рисунок 42 – Сообщение об успешном удалении PC из списка разрешенных PC

После завершения всех необходимых операций со списком разрешенных РС в окне задания списка разрешенных РС (рисунок 23) нажать кнопку <Заккрыть>.

Если в настройках политики доступа к РС был выбран тип доступа к РС «Доступ без ограничений», то после выполнения процедуры удаления РС из списка разрешенных появляется сообщение (рисунок 43), оповещающее о том, что внесенные изменения вступят в силу после установки типа доступа к РС «Доступ с ограничением по доменам и рабочим станциям».

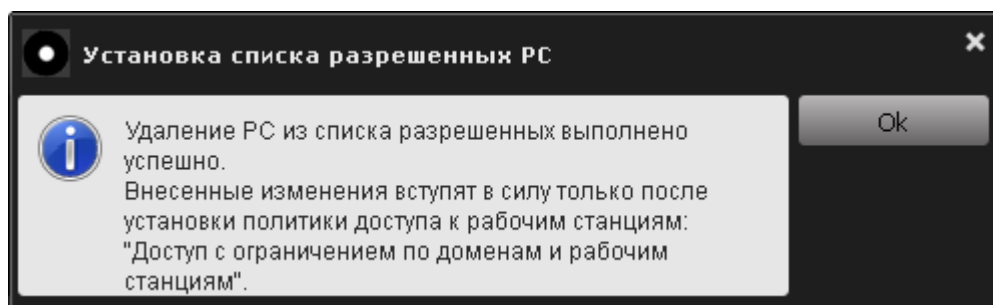


Рисунок 43 – Сообщение о внесенных изменениях

3.4. 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.

Чтобы посмотреть журнал событий СН, необходимо нажать кнопку «Просмотреть журнал работы СН...» на панели консоли администратора (рисунок 11).

После выбора данной функции появляется окно с запросом пароля администратора СН (рисунок 44). Для подтверждения введенного пароля нажать кнопку <Ok>.

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

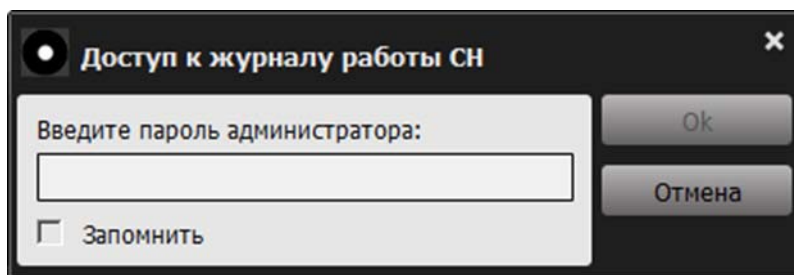


Рисунок 44 – Запрос пароля администратора СН для доступа к журналу работы СН

Если пароль введен некорректно, отображается сообщение об ошибке при получении доступа к журналу (рисунок 45):

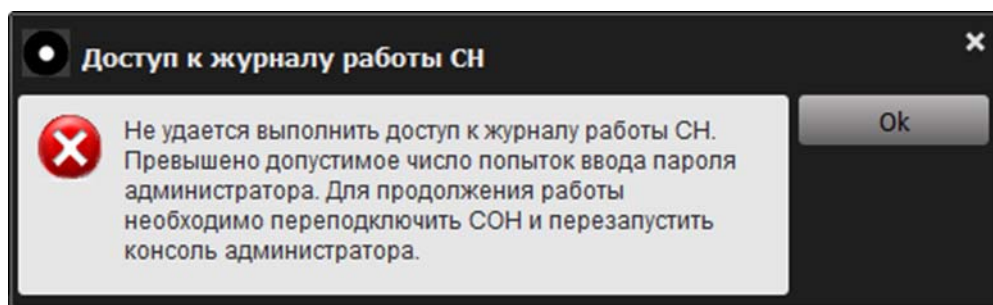


Рисунок 45 – Ошибка при выполнении доступа к протоколу работы СН

При корректном вводе пароля появляется сообщение об успешном доступе к протоколу работы СН (рисунок 46).

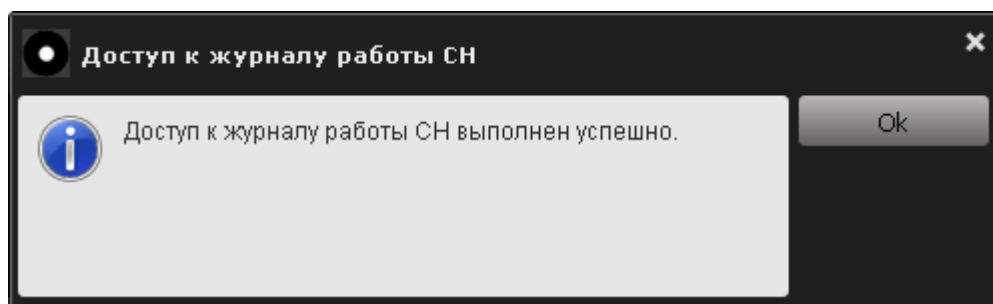


Рисунок 46 – Сообщение об успешном доступе к протоколу работы СН

При нажатии кнопки <Ok> появляется журнал регистрации событий СН (рисунок 50), который содержит информацию о событиях, зафиксированных в процессе работы с ПАК «Секрет Особого Назначения» на данной РС.

Следует обратить внимание, что при нажатии кнопки <Ok> также возможно возникновение некорректной ситуации, связанной с особенностями некоторых ОС, которые вызывают ошибку монтирования разделов журнала регистрации событий. Эта ситуация проявляется следующим образом:

- сначала выдается кратковременное сообщение об успешном доступе к журналу (рисунок 47);
- далее появляется окно с ошибкой монтирования (рисунок 48).

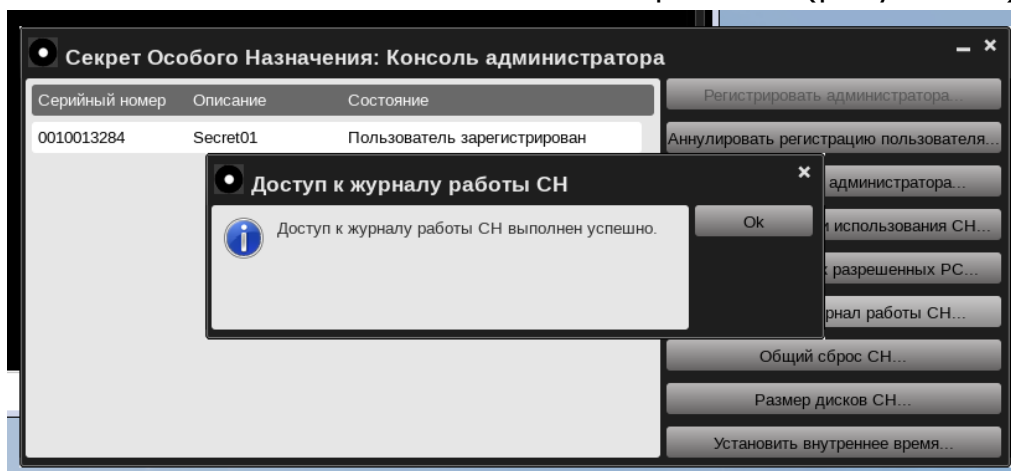


Рисунок 47 – Сообщение об успешном доступе к журналу регистрации событий

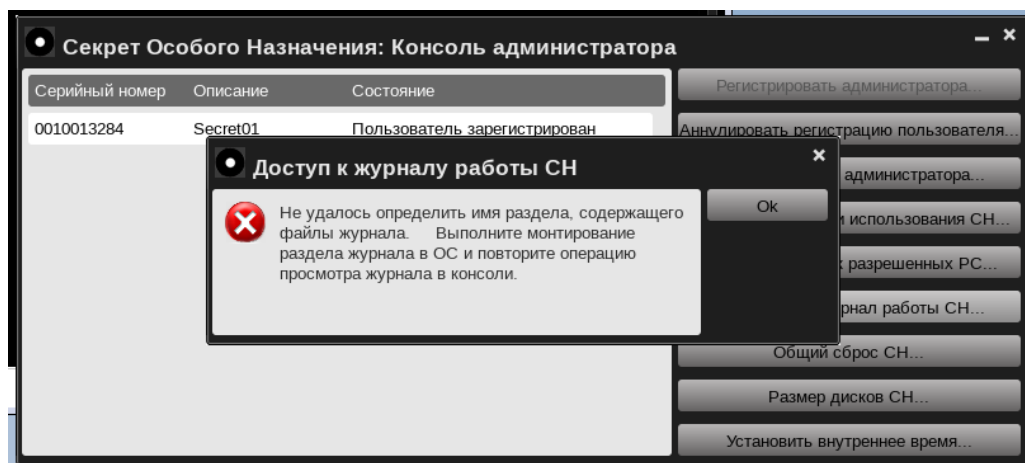


Рисунок 48 – Сообщение об ошибке монтирования разделов журнала

При подобных обстоятельствах проблема исправляется ручным монтированием разделов журнала – в терминале или в графическом интерфейсе (рисунок 49) – и повторном выборе пункта меню в консоли администрирования.

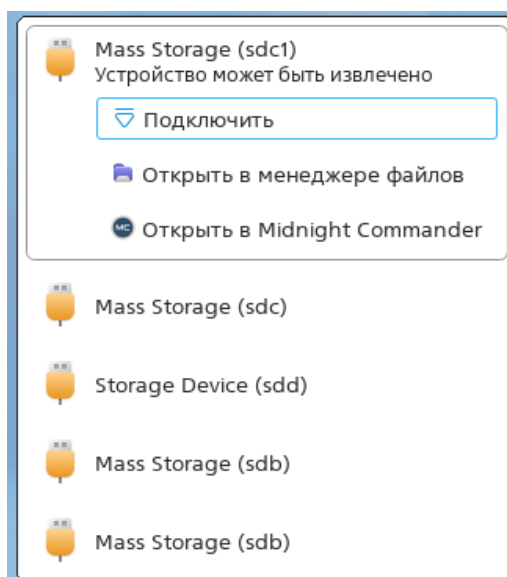


Рисунок 49 – Ручное монтирование разделов журнала в графическом интерфейсе

Следует отметить, что при каждом подключении СН к компьютеру в журнале регистрируется собственно факт 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.

ВНИМАНИЕ! В связи с особенностями работы ОС семейства Windows после получения доступа к закрытому диску СН записи о новых событиях работы не отображаются в журнале. При необходимости обновления журнала следует переподключать устройство после завершения работы с закрытым диском СН.

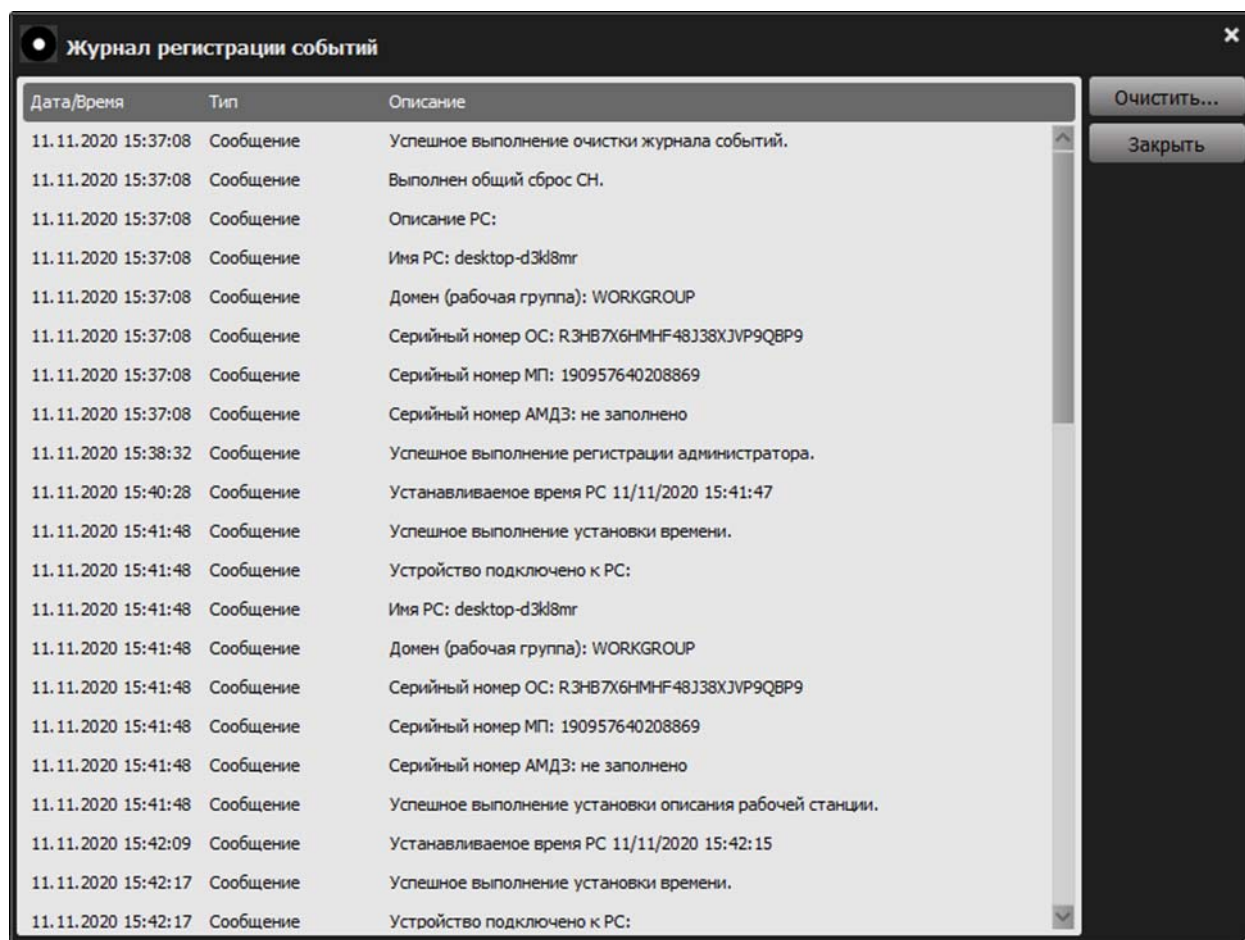


Рисунок 50 – Журнал регистрации событий СН

ВНИМАНИЕ! Если СН снабжен внутренними часами, события регистрируются в журнале в соответствии с установленным на них временем. Если внутренние часы отсутствуют, в журнале событий СН регистрируется время возникновения события в соответствии с системным временем ОС.

Запись в журнале с сообщением об ошибке содержит номер ошибки, позволяющий разработчикам продукта определить ее причину при обращении в техническую поддержку изготовителя.

Чтобы очистить журнал регистрации событий, необходимо нажать кнопку <Очистить> (рисунок 50). При нажатии кнопки запрашивается пароль администратора для доступа к журналу работы СН (рисунок 51).

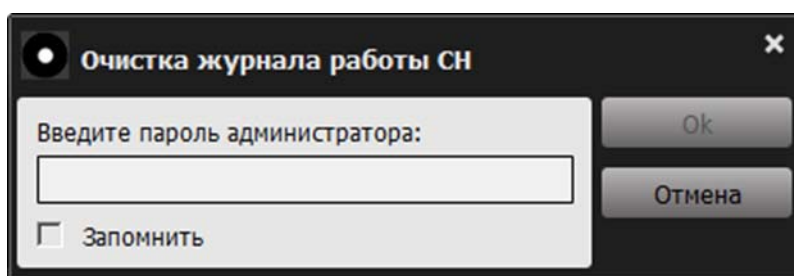


Рисунок 51 – Запрос пароля администратора СН для очистки журнала работы СН

Если пароль введен некорректно, появляется оповещение об ошибке (рисунок 52):

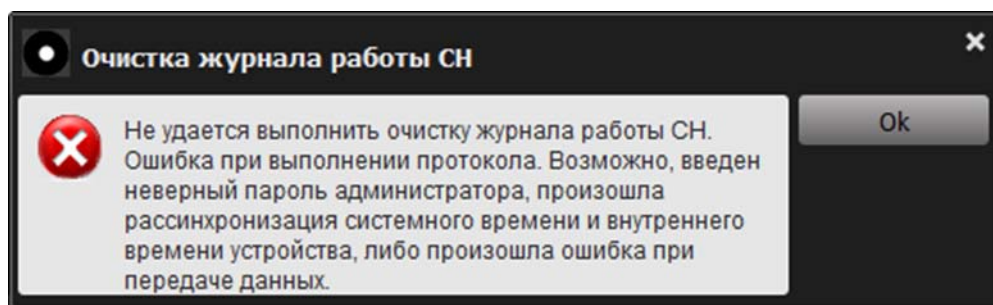


Рисунок 52 – Сообщение об ошибке при выполнении очистки журнала

В этом случае следует нажать <Ok> и повторить процедуру очистки журнала работы СН.

Если введен корректный пароль, содержимое журнала стирается, и отображается следующее сообщение (рисунок 53):

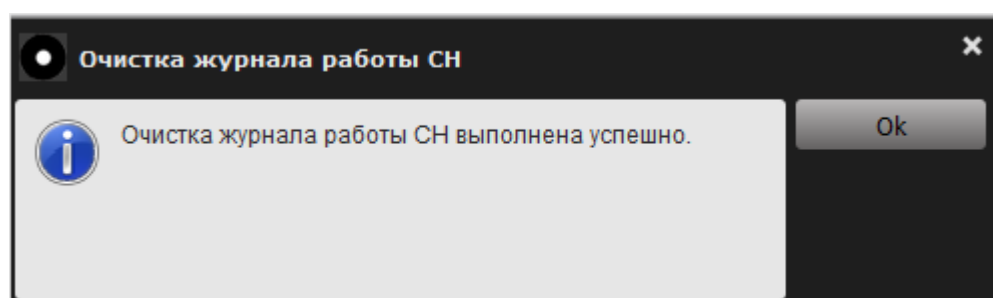


Рисунок 53 – Сообщение об успешном выполнении сброса протокола работы СН

При этом в журнале событий СН появляется сообщение о выполнении процедуры очистки журнала работы СН.

Если журнал СН переполнен (статус СН «Журнал переполнен» в главном окне консоли администрирования), то при нажатии кнопки «Просмотреть журнал работы СН...» (рисунок 11) появится сообщение:

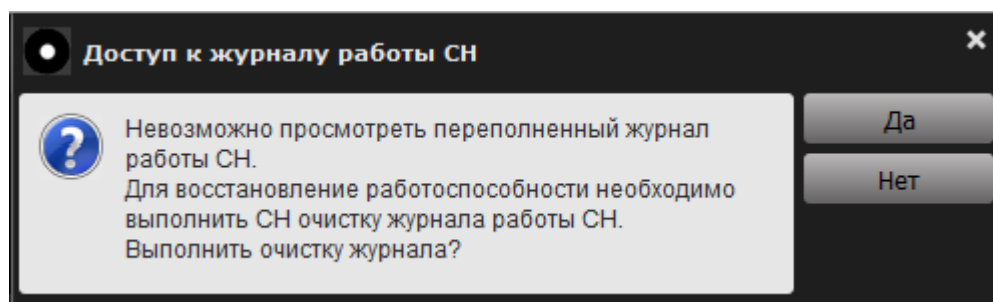


Рисунок 54 – Сообщение о переполнении журнала СН

Чтобы получить доступ к журналу регистрации событий, необходимо провести очистку журнала. Для этого нажать кнопку <Да> в сообщении (рисунок 54).

После выполнения всех необходимых действий с журналом регистрации событий СН нажать <Заккрыть>. Описание возможных сообщений, фиксируемых в журнале событий СН, см. в разделе 7.

3.5. Смена пароля администратора

В случае необходимости смены пароля администратора (например, в случае его компрометации) в консоли администратора (рисунок 11) следует нажать кнопку «Сменить пароль администратора...» - появится окно, показанное на рисунке 55.

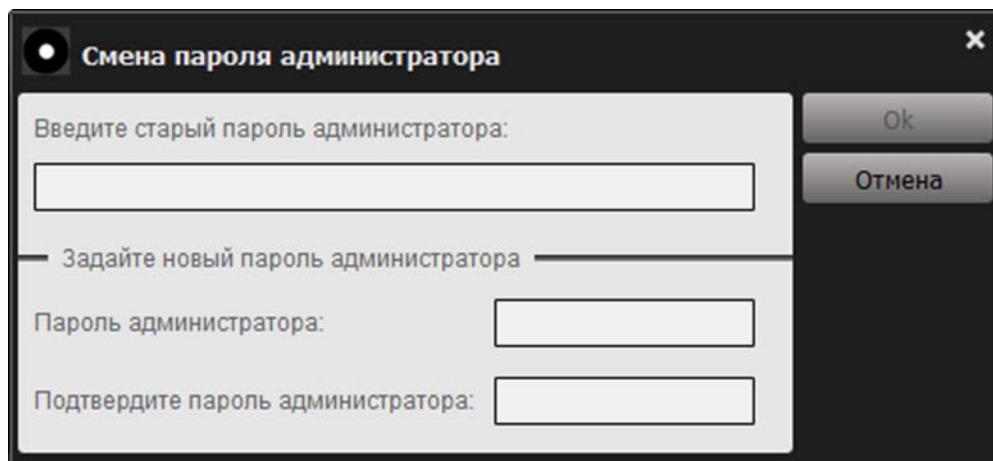


Рисунок 55 – Окно смены пароля администратора

В верхнем поле данного окна необходимо ввести пароль администратора, в нижних полях – ввести новый пароль с подтверждением. После этого нажать <Ok> для завершения текущей операции или <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>.

Если введенное количество символов выходит за рамки допустимого количества символов, появится следующее предупреждение (рисунок 56).

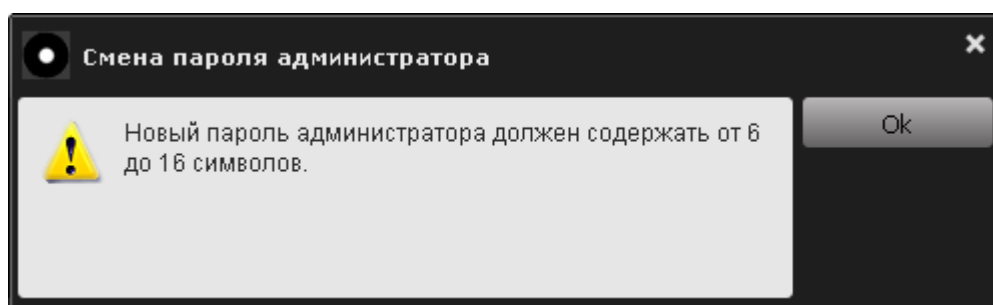


Рисунок 56 – Предупреждение о том, что новый пароль администратора должен содержать от 6 до 16 символов

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

Если подтверждение пароля введено некорректно, появляется предупреждение (рисунок 57):

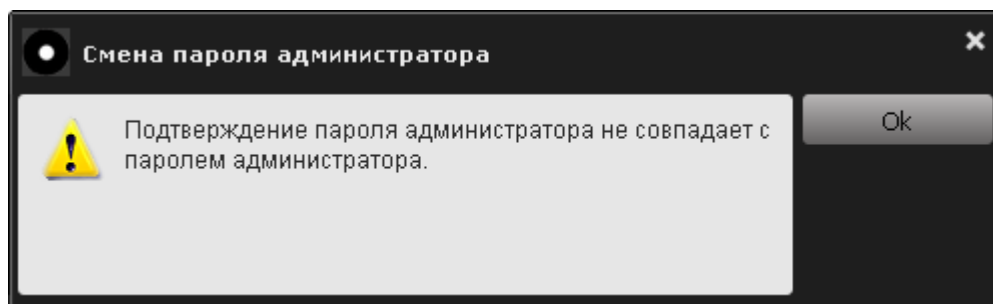


Рисунок 57 – Предупреждение о том, что подтверждение пароля администратора не совпадает с паролем администратора

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

Если старый пароль администратора введен некорректно, появляется сообщение об ошибке в процессе смены пароля (рисунок 58).

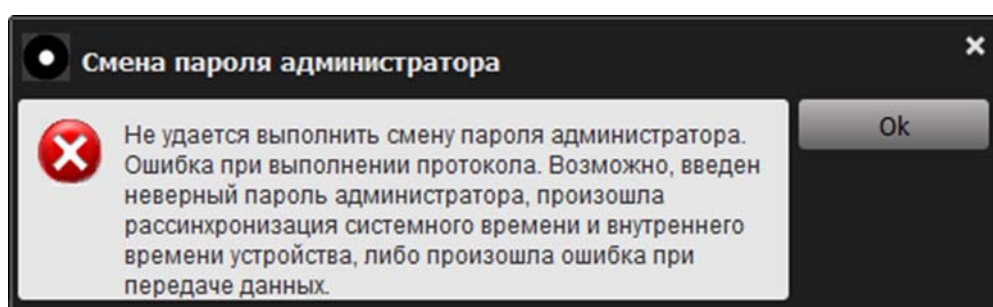


Рисунок 58 – Сообщение об ошибке при смене пароля администратора

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

Если операция смены пароля администратора выполнена успешно, отображается оповещение об успешной смене пароля (рисунок 59):

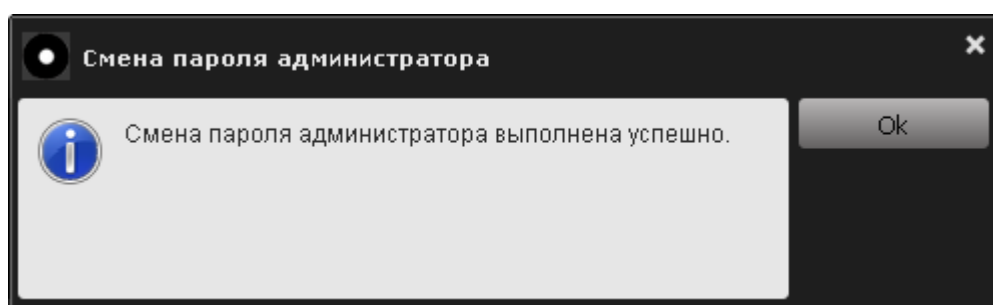


Рисунок 59 – Оповещение об успешной смене пароля

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

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

3.6. 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;
- Утрачены код авторизации пользователя 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 11).

После выбора соответствующей функции (рисунок 11) появляется окно запроса пароля администратора (рисунок 60):

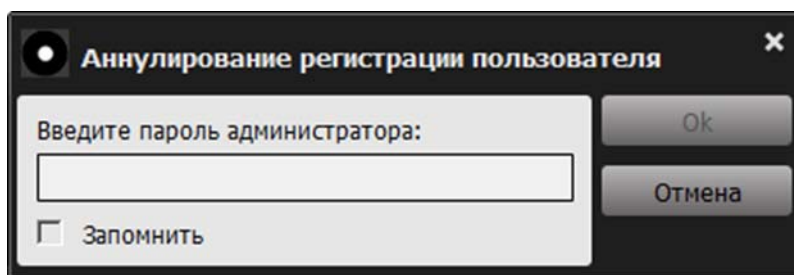


Рисунок 60 – Окно ввода пароля администратора

Следует ввести пароль администратора и для завершения текущей операции нажать <Ok>. Для отмены операции нажать <Отмена>.

Если пароль введен некорректно, появляется сообщение об ошибке в процессе аннулирования регистрации пользователя (рисунок 61):

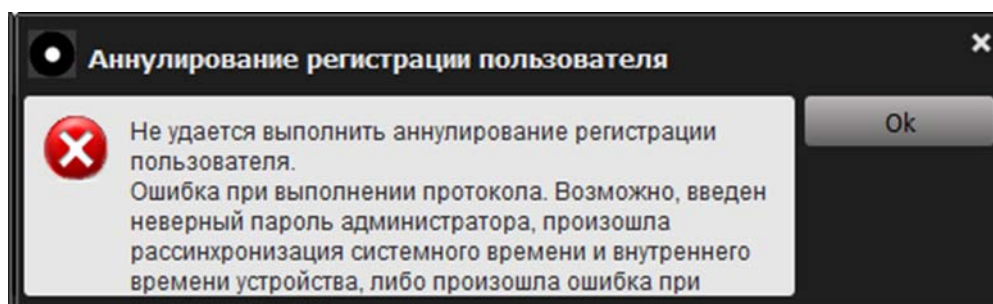


Рисунок 61 – Сообщение об ошибке при аннулировании регистрации пользователя

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

После корректного ввода пароля отображается сообщение об успешном аннулировании регистрации пользователя СН (рисунок 62):

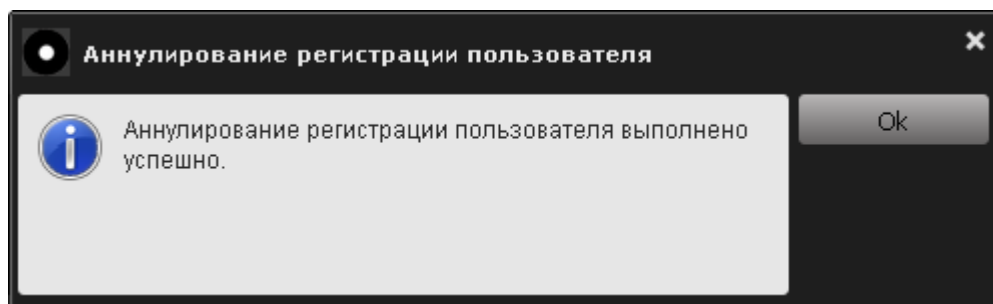


Рисунок 62 – Сообщение об успешном аннулировании регистрации пользователя

Для завершения операции нажать <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.

3.7. Установка размеров журнала и закрытого раздела диска СН

ВНИМАНИЕ! При выполнении процедуры установки размеров журнала и закрытого раздела диска СН произойдет очистка журнала событий СН и удаление пользовательской информации.

В ПО ПАК «Секрет Особого Назначения» имеется возможность установки размеров журнала событий СН (доступного только администратору ПАК «Секрет Особого Назначения» после успешного получения доступа к журналу СН, п. 3.4) и закрытого раздела диска СН, на котором хранится пользовательская информация (доступного только пользователю после успешного прохождения процедуры авторизации, см. «Руководство пользователя» 37222406.26.20.40.140.094 34).

Чтобы изменить размер дисков СН, следует нажать кнопку <Размер дисков СН...> в консоли администратора (рисунок 11).

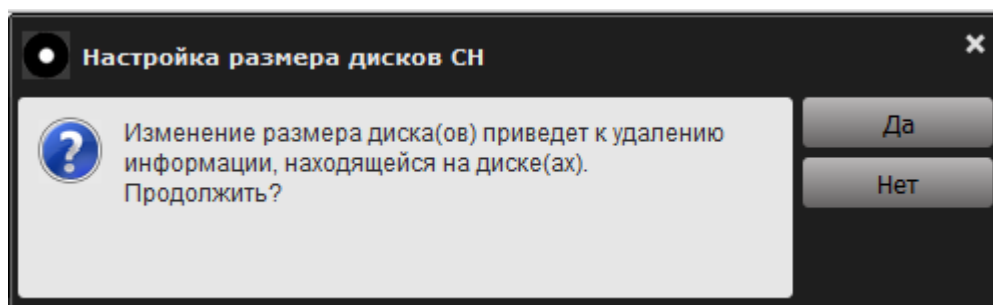


Рисунок 63 – Предупреждение о том, что изменение размера дисков СН приведет к удалению информации, хранящейся на дисках

37222406.26.20.40.140.094 90

В появившемся предупреждении (рисунок 60) следует нажать кнопку <Да>, если действительно необходимо изменить размер.

Появится окно, в котором следует установить нужные размеры (рисунок 64).

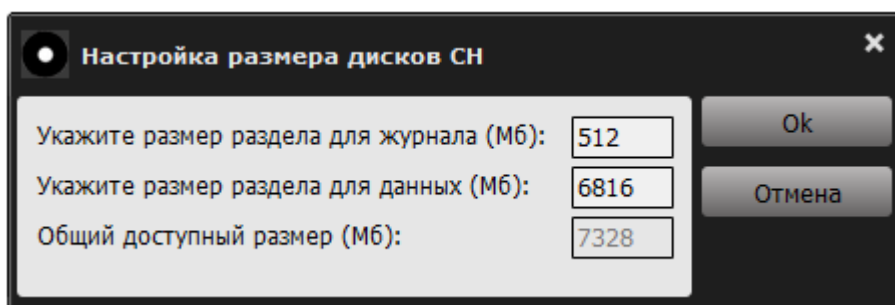


Рисунок 64 – Установка размеров дисков СН «Секрет Особого Назначения»

Для завершения операции нажать <Ok>, для ее отмены – <Отмена>.

Если описанная последовательность действий выполнена верно, на экран выводится сообщение об успешном выполнении процедуры установки размеров дисков СН (рисунок 65).

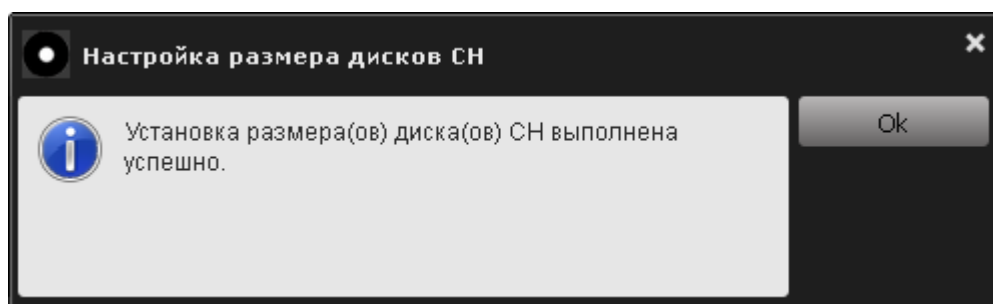


Рисунок 65 – Сообщение об успешной настройке размеров дисков СН «Секрет Особого Назначения»

При этом в журнале событий СН появится сообщение о выполнении процедуры установки размеров журнала событий и закрытого раздела диска СН.

ВНИМАНИЕ! Для получения доступа к журналу работы или к закрытому разделу диска СН после выполнения процедуры установки размеров журнала событий и закрытого раздела диска СН необходимо переподключить СН.

3.8. Общий сброс СН

В случае необходимости возврата устройства к заводским настройкам следует выполнить общий сброс СН.

ВНИМАНИЕ! Следует помнить, что при выборе данной функции кроме аннулирования регистрации администратора также произойдет сброс всех настроек СН, журнала событий, аннулирование регистрации пользователя СН (п. 3.6) и удаление его информации.

37222406.26.20.40.140.094 90

Для выполнения операции сброса СН следует нажать кнопку <Общий сброс СН...> в консоли администратора (рисунок 11) - появится следующее сообщение (рисунок 66):

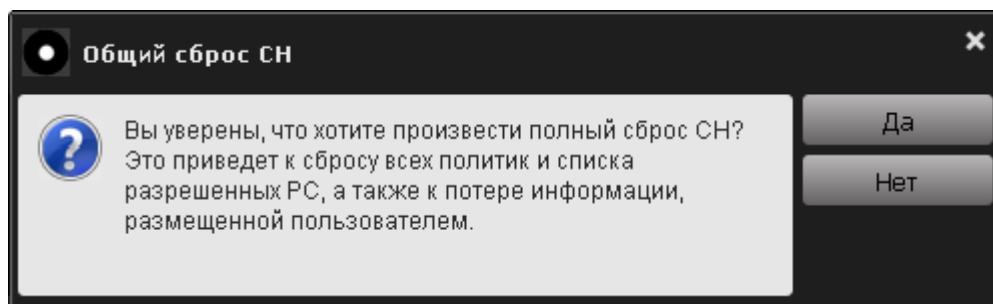


Рисунок 66 – Общий сброс СН

При нажатии кнопки <Да> появляется окно для ввода пароля администратора (рисунок 67).

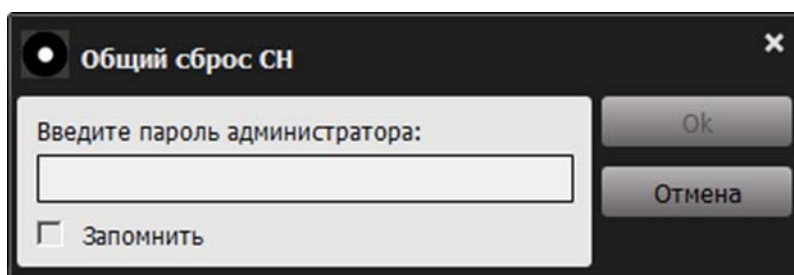


Рисунок 67 – Окно ввода пароля

Если пароль введен некорректно, то отображается сообщение об ошибке при выполнении операции общего сброса СН (рисунок 68).

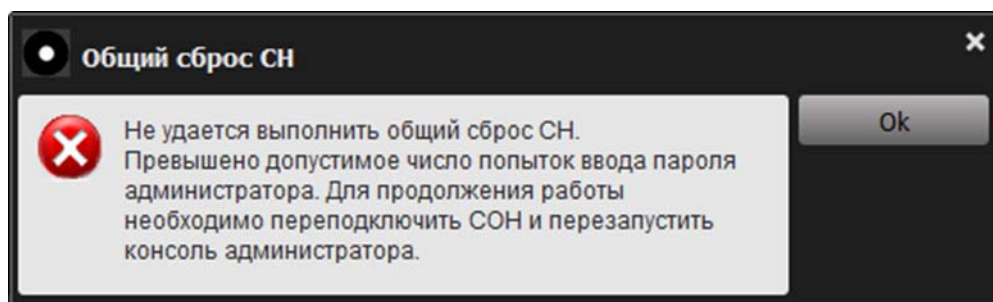


Рисунок 68 – Оповещение об ошибке при выполнении общего сброса СН

Если пароль введен корректно, появляется сообщение об успешном выполнении общего сброса СН (рисунок 69).

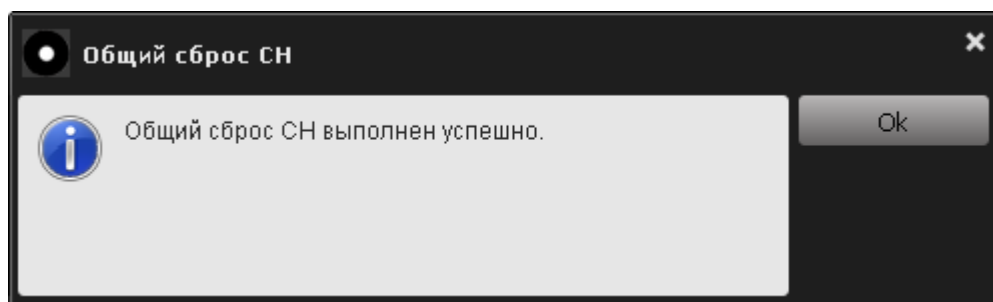


Рисунок 69 – Сообщение об успешном выполнении общего сброса СН

37222406.26.20.40.140.094 90

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

3.9. Установка внутреннего времени

ВНИМАНИЕ! Функция установки внутреннего времени доступна в ПАК «Секрет Особого Назначения», СН в составе которого снабжен внутренними часами.

Наличие встроенных часов в СН и внутреннее время можно определить, наведя курсор мыши на строку с подключенным устройством в консоли администратора. Если СН снабжен внутренними часами, в строке «Внутренние часы» стоит значение «Есть» (рисунок 70).

Версия: 1.2.5048
Серийный номер: 0000000112
Описание: 123
Производитель: ЗАО ОКБ САПР
Состояние: Администратор зарегистрирован
Тип доступа к СН: Без ограничений
Журнал (Всего/Свободно, МБ): 512/511
Внутренние часы: есть
Внутреннее время: 05.10.2016 12:21:38

Рисунок 70 – Окно с параметрами СН

Время на внутренних часах устанавливается при производстве.

Если СН снабжен внутренними часами, и внутренние часы были сброшены, например, вследствие извлечения элемента питания, функции консоли пользователя блокируются, а в строке «Состояние» консоли пользователя и консоли администратора для данного СН стоит значение «Некорректное внутреннее время» (рисунок 71).

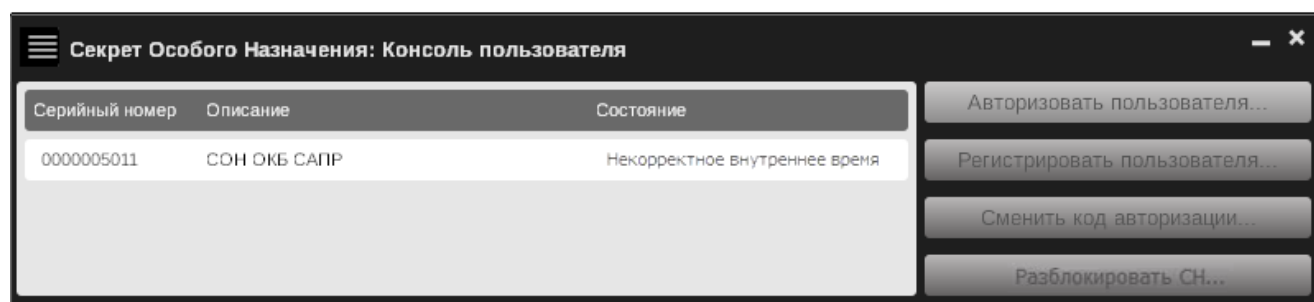


Рисунок 71 – Консоль пользователя с заблокированными функциями

При этом запись о событии заносится в журнал регистрации.

В таком случае администратору нужно самостоятельно установить внутреннее время. Для выполнения операции следует нажать кнопку «Установить внутреннее время...» в консоли администратора - появляется окно, представленное на рисунке 72.

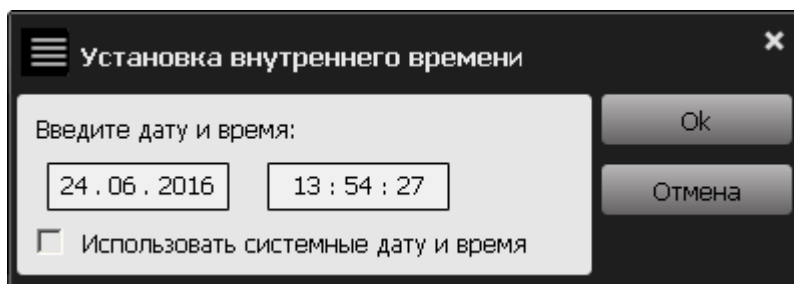


Рисунок 72 – Окно установки внутреннего времени

ВНИМАНИЕ! Кнопка <Установить внутреннее время...> в консоли администратора активна только при подключении СН с внутренними часами.

Если данные введены корректно, при нажатии кнопки <Ok> появляется сообщение об успешном выполнении операции (рисунок 73).

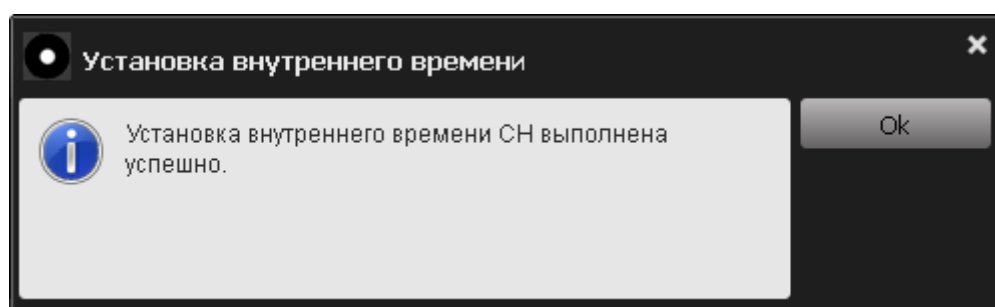


Рисунок 73 – Сообщение об успешной установке внутреннего времени

ВНИМАНИЕ! Если в СН отсутствуют внутренние часы, перед началом использования ПАК «Секрет Особого Назначения» следует сверить текущее время с отображаемым в ОС и при необходимости установить точное время средствами ОС.

3.10. 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 (п. 3.6). Подробное описание процедуры разблокирования СН приведено в «Руководстве пользователя» 37222406.26.20.40.140.094 34.

3.11. Изменение буквы открытого раздела ПАК «Секрет Особого Назначения»

В случае необходимости изменить в ОС Windows букву открытого раздела ПАК «Секрет Особого Назначения» следует:

1. Запустить командную строку с правами администратора ОС, запустить утилиту diskpart;
2. Выполнить команду *list volume*;

3. В выведенном списке разделов найти открытый раздел ПАК «Секрет Особого Назначения». Чтобы поменять букву для открытого раздела ПАК «Секрет Особого Назначения», необходимо:

- выполнить команду *select volume <номер_раздела>*;
- выполнить команду *remove letter=X*, где «X» — текущая буква открытого раздела ПАК «Секрет Особого Назначения»;
- выполнить команду *assign letter=H*, где «H» - буква, которую необходимо назначить.

3.12. 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) - появится следующее сообщение (рисунок 74):

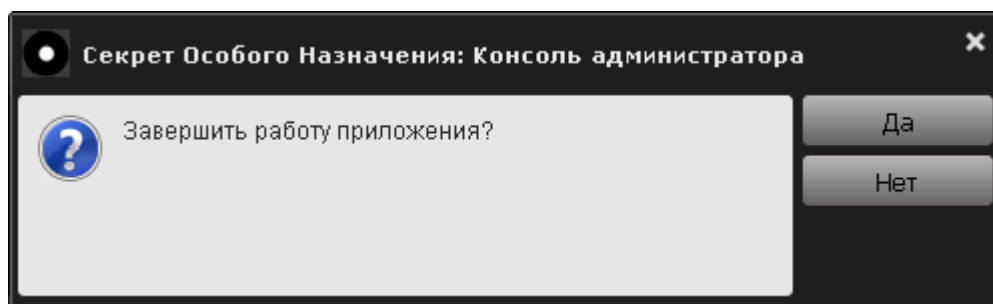


Рисунок 74 – Завершение работы СН

Для подтверждения текущей операции следует нажать кнопку <Да>, для ее отмены – 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 75). Данная операция может быть выполнена для рабочих станций, не включенных в домен.

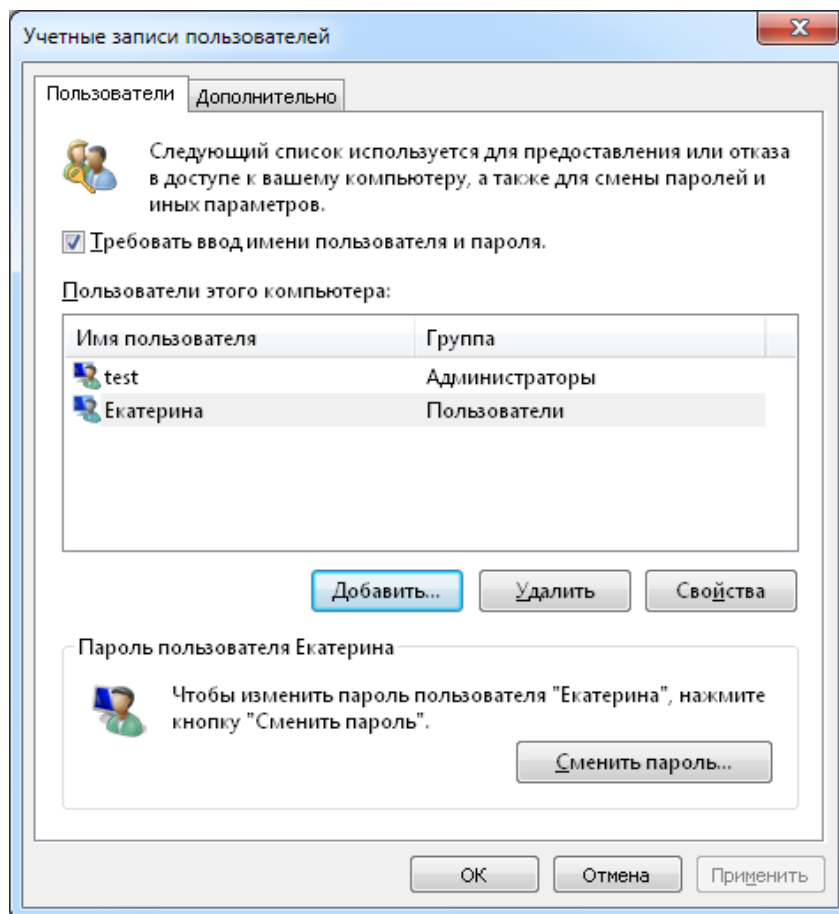


Рисунок 75 – Окно настроек учетных записей пользователей

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 76).

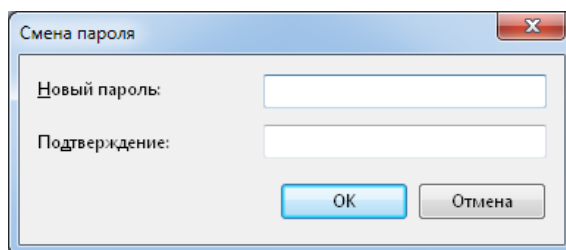


Рисунок 76 – Окно смены пароля пользователя для входа в ОС

4.3. Включение режима автоматической блокировки экрана

Для включения режима автоматической блокировки экрана по истечении заданного периода неактивности следует выполнить следующие действия: в меню Пуск-> Параметры-> Персонализация-> Экран блокировки-> Параметры заставки-> Параметры экранной заставки установить галочку «Начинать с экрана входа в систему» и выставить необходимый интервал времени неактивности (рисунок 77).

37222406.26.20.40.140.094 90

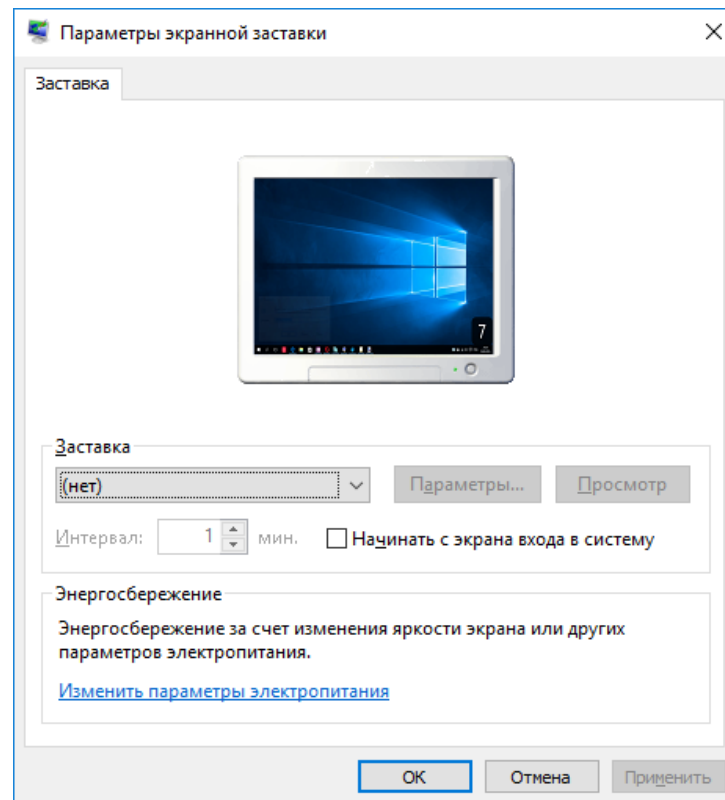


Рисунок 77 - Окно настройки заставки экрана в ОС Windows 10

5. Настройки для обеспечения работы ПАК «Секрет Особого Назначения» в режиме терминальной сессии

В случаях, когда запуск ПО РС на стороне терминального клиента невозможен (например, при использовании тонкого клиента в качестве РС пользователя, или при использовании СЗИ, не позволяющих запускать стороннее ПО на клиентском рабочем месте), необходимо копирование ПО комплекса на жесткий диск терминального сервера.

При этом терминальный сервер должен быть добавлен в список разрешенных компьютеров (п. 3.3.2), а каталог с ПО РС из состава ПАК «Секрет Особого Назначения» – доступен пользователю.

При совместном использовании ПАК «Секрет Особого Назначения» и Citrix Presentation Server 4.5/XenApp 5.0/6.0/XenDesktop 5.0 может возникнуть ситуация, при которой пользователь, подключившийся к серверу XenApp или XenDesktop, не может получить доступ к файлам, находящимся на внешнем диске. Тогда на экране может появиться одно из предупреждений об ошибке, показанных на рисунках 78 - 80.

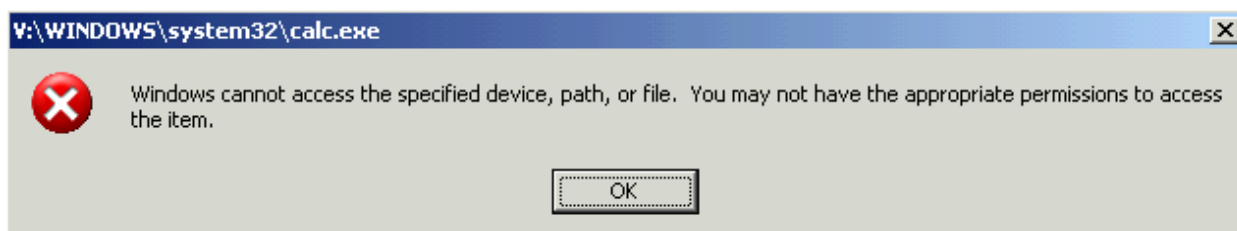


Рисунок 78 – Сообщение об ошибке при получении доступа к данным внешнего диска Citrix Presentation Server 4.5/XenApp 5.0

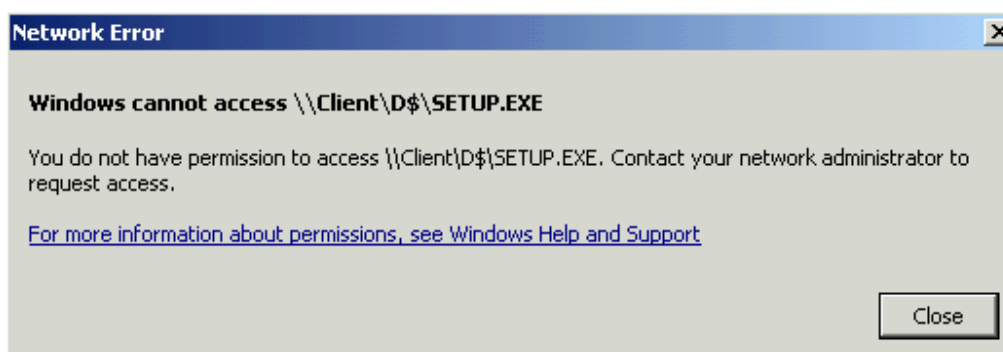


Рисунок 79 - Сообщение об ошибке при получении доступа к данным внешнего диска Citrix XenApp 6.0

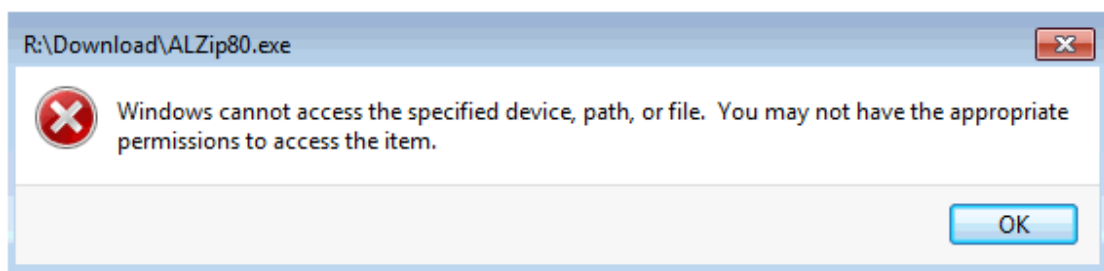


Рисунок 80 - Сообщение об ошибке при получении доступа к данным внешнего диска Citrix XenDesktop 5.0

Причина отсутствия доступа к диску – контроль со стороны Citrix запуска нежелательных (недоверенных) приложений в сеансе. В качестве меры предосторожности на XenApp или XenDesktop по умолчанию внешние подключенные диски пользователя (в том числе открытый диск CH) не отображаются. В случае необходимости запуска ПО ПАК «Секрет Особого Назначения» с открытого диска CH ПАК «Секрет Особого Назначения», нужно изменить значение параметра ExecuteFromMappedDrive в реестре на сервере XenApp или XenDesktop.

Чтобы изменить значение параметра реестра ExecuteFromMappedDrive на сервере XenApp, необходимо выполнить следующую последовательность действий:

- 1) после установки XenApp запустить редактор реестра Regedit;
- 2) найти ключ реестра

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Cdm/ Parameters и установить значение параметра ExecuteFromMappedDrive (рисунок 81) равным 1 (по умолчанию – 0);

(на Citrix XenApp 6.0 расположение ключей реестра отличается от XenApp 5.0: параметр ExecuteFromMappedDrive размещен в ключе HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/picadm/Parameters);

- 3) перезапустить сервер, чтобы изменения вступили в силу.

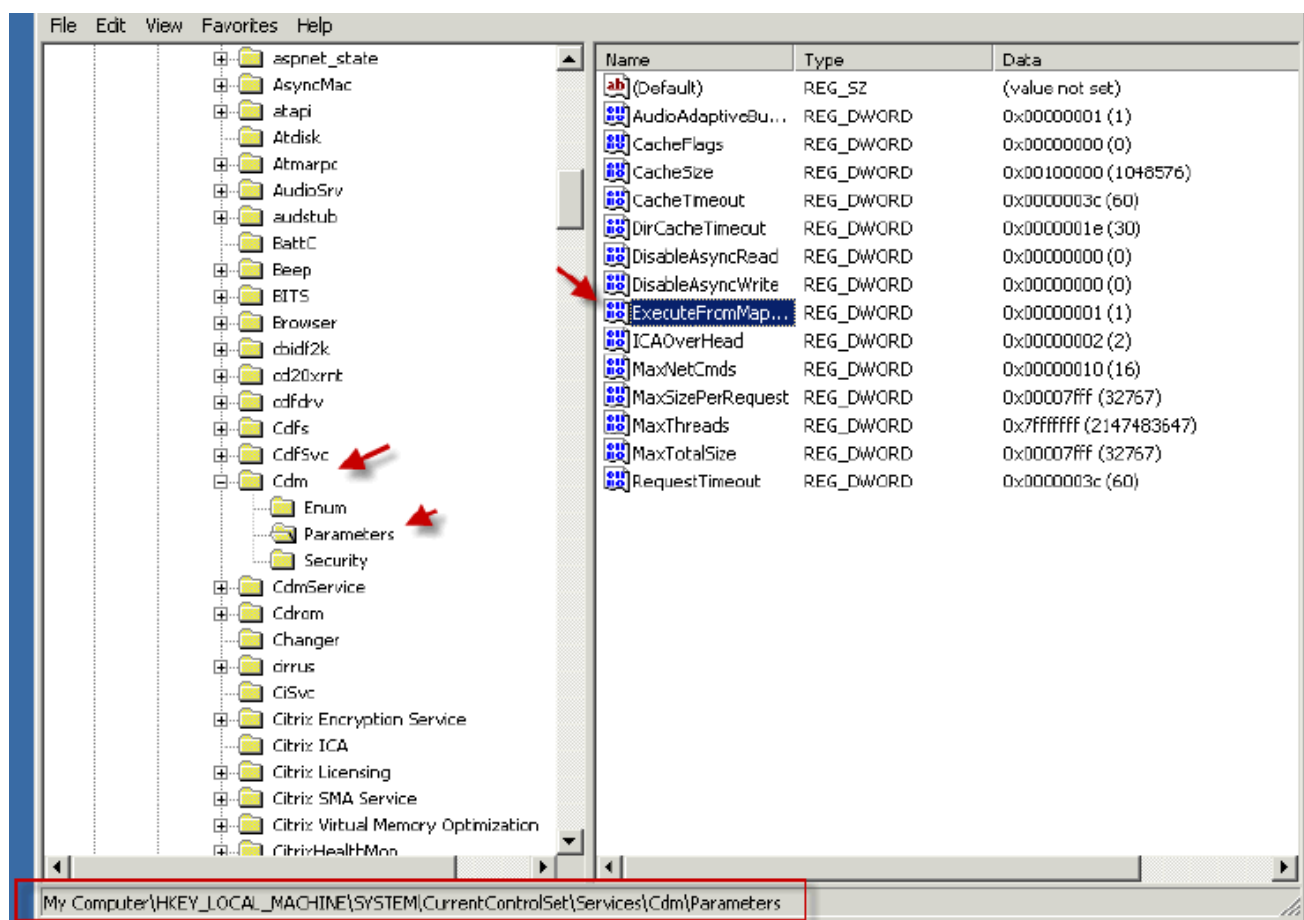


Рисунок 81 - Параметр ExecuteFromMappedDrive, определяющий возможность получения доступа к данным на внешнем диске

Чтобы изменить значение параметра реестра ExecuteFromMappedDrive на XenDesktop 5.0, необходимо выполнить следующую последовательность действий:

1) после установки Virtual Desktop Agent, запустить редактор реестра Regedit;

2) перейти в раздел реестра

HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\;

3) создать новый подраздел CDMSettings;

4) создать в разделе CDMSettings новый параметр типа REG_DWORD с именем ExecuteFromMappedDrive (рисунок 82) и изменить его значение на 1 (по умолчанию – 0).

5) перезапустить компьютер с настроенным виртуальным рабочим столом, чтобы изменения вступили в силу.

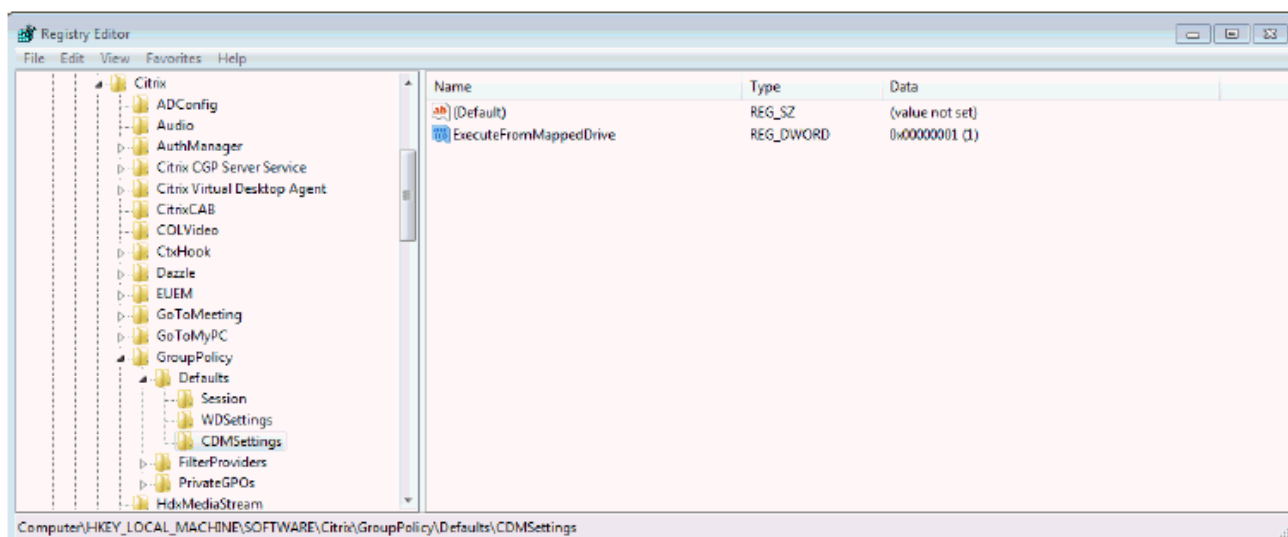


Рисунок 82 - Параметр реестра ExecuteFromMappedDrive на XenDesktop

При необходимости совместного использования ПАК «Секрет Особого Назначения» и Xen Desktop 7.0 и выше необходимо в Desktop Studio настроить разрешающие правила «USB Redirection Policy Rules».

Если в рамках терминальной сессии по протоколу RDP планируется использование CCID-устройств, то на терминальном RDP-клиенте необходимо выполнить настройку подключения к удаленному рабочему столу.

Для этого необходимо выполнить следующую последовательность действий:

1) выбрать команду меню Программы\Стандартные\Подключение к удаленному рабочему столу;

2) в появившемся окне нажать кнопку <Параметры>;

3) при нажатии кнопки <Подробнее> во вкладке «Локальные ресурсы» появится окно, в котором необходимо установить флаги «Смарт-карты» и «Дисководы, которые будут подключены позже» (рисунок 83).

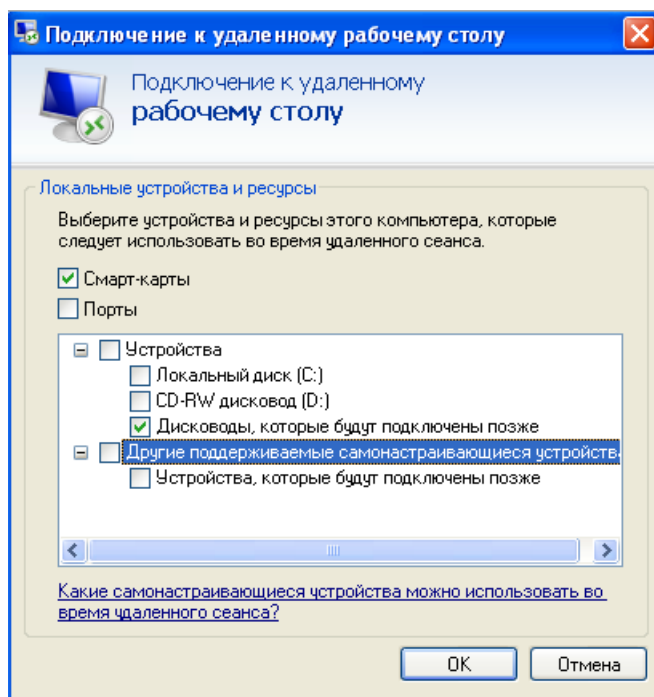


Рисунок 83 - Настройка подключения к удаленному рабочему столу

Также в случае необходимости использования ПАК «Секрет Особого Назначения» в рамках терминальной сессии по протоколу RDP следует учесть, что если на терминальном сервере установлена ОС Windows Server 2012 R2 и выше, то на таком сервере необходимо установить обновление Microsoft (KB2919355), которое можно получить с использованием механизмов, предусмотренных Microsoft для их распространения.

6. 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» 37222406.26.20.40.140.094 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.

7. 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 установки времени»	Неисправность устройства	Повторить операцию. В случае если сообщение появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении установки описания рабочей станции»	Неисправность устройства	Повторить операцию. В случае если сообщение появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении запроса информации»	Неисправность устройства	Повторить операцию. В случае если сообщение появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении расширенного запроса информации»	Неисправность устройства	Повторить операцию. В случае если сообщение появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении регистрации администратора»	Введен неверный пароль администратора	Повторить операцию. В случае если введен неверный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении регистрации пользователя»	Введен неверный код авторизации	Повторить операцию. В случае если введен верный код авторизации, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении смены ключа авторизации»	Введен неверный код авторизации	Повторить операцию. В случае если введен верный код авторизации, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	

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

Сообщение об ошибке	Возможные причины возникновения ошибки	Порядок действий по устранению ошибки
«Ошибка при выполнении форматирования устройства»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении авторизации пользователя»	Введен неверный код авторизации	Повторить операцию. В случае если введен верный код авторизации, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении установки политики заполнения журнала»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении просмотра журнала событий»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении очистки журнала событий»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении обновления программного обеспечения»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения	

Сообщение об ошибке	Возможные причины возникновения ошибки	Порядок действий по устранению ошибки
	операции	
«Ошибка при выполнении сброса пользователя СН»	Неисправность устройства	Повторить операцию. В случае если сообщение появляется снова, следует обратиться в службу технической поддержки
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении персонализации носителя»	Неисправность устройства	Повторить операцию. В случае если сообщение 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 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 появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении защищенного получения списка разрешенных рабочих станций»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении установки размера диска»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при выполнении установки внутренних часов»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка	

Сообщение об ошибке	Возможные причины возникновения ошибки	Порядок действий по устранению ошибки
«Время РС ДД/ММ/ГГГГ чч:мм:сс не совпадает со внутренним временем»	Неисправность устройства	Выполнить операцию установки внутреннего времени или изменить время на РС
	Программная ошибка	
	На РС установлено неверное время	
«Время РС ДД/ММ/ГГГГ чч:мм:сс меньше времени последнего сеанса»	Неисправность устройства	Выполнить операцию установки внутреннего времени или изменить время на РС
	Программная ошибка	
	На РС установлено неверное время	
«Ошибка при выполнении временного отключения контроля доступа»	Введен неверный пароль администратора	Повторить операцию. В случае если введен верный пароль администратора, но сообщение появляется снова, следует обратиться в службу технической поддержки
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Достигнут предел неудачных попыток ввода пароля пользователя. Пользователь заблокирован»	Достигнут предел неудачных попыток ввода пароля пользователя	Выполнить операцию разблокировки пользователя
	Неисправность устройства	
	Программная ошибка в процессе выполнения операции	
«Ошибка при конфигурировании ПЛИС»	Неисправность устройства	Обратиться в службу технической поддержки

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

Информационное сообщение	Описание
«Успешное выполнение установки времени»	Установка времени выполнена успешно
«Успешное выполнение установки описания рабочей станции»	Установка описания рабочей станции выполнена успешно
«Успешное выполнение регистрации администратора»	Регистрация администратора завершена успешно
«Успешное выполнение регистрации пользователя»	Регистрация пользователя завершена успешно
«Успешное выполнение смены ключа авторизации»	Смена ключа авторизации завершена успешно
«Успешное выполнение разблокирования»	Разблокирование СН завершено успешно
«Успешное выполнение установки политики использования кода авторизации»	Установка политики использования кода авторизации завершена успешно
«Успешное выполнение установки политики доступа к рабочим станциям»	Установка политики доступа к рабочим станциям завершена успешно
«Успешное выполнение смены пароля администратора»	Смена пароля администратора выполнена успешно
«Успешное выполнение установки списка разрешенных рабочих станций»	Установка списка разрешенных рабочих станций завершена успешно
«Успешное выполнение форматирования»	Форматирование устройства завершено

Информационное сообщение	Описание
устройства»	успешно
«Успешное выполнение авторизации пользователя»	Авторизация пользователя завершена успешно
«Успешное выполнение установки политики заполнения журнала»	Установка политики заполнения журнала событий СН выполнена успешно
«Успешное выполнение разрешения просмотра журнала событий»	Доступ к журналу событий СН выполнен успешно
«Успешное выполнение очистки журнала событий»	Очистка журнала событий СН выполнена успешно
«Успешное выполнение обновления программного обеспечения»	Обновление программного обеспечения завершено успешно
«Успешное выполнение сброса пользователя СН»	Сброс пользователя СН выполнен успешно
«Успешное выполнение защищенного получения списка разрешенных рабочих станций»	Получение списка разрешенных станций выполнено успешно
«Успешное выполнение установки размера диска»	Установка размеров диска выполнено успешно
«Успешное выполнение установки внутренних часов»	Установка внутренних часов выполнена успешно
«Успешное выполнение временного отключения контроля доступа»	Процедура временного снятия ограничений на доступ к СН на РС успешно завершена
«Имя РС Серийный номер МП, Серийный номер ОС, Имя РС, Домен (рабочая группа), Серийный номер АМДЗ»	Идентификационная информация рабочей станции, на которой использовался СН ¹
Устройство подключено к РС, отсутствующей в списке разрешенных: «Имя РС Серийный номер МП, Серийный номер ОС, Имя РС, Домен (рабочая группа), Серийный номер АМДЗ»	Идентификационная информация рабочей станции, отсутствующей в списке разрешенных ²
Устройство подключено к РС: «Имя РС Серийный номер МП, Серийный номер ОС, Имя РС, Домен (рабочая группа), Серийный номер АМДЗ»	Идентификационная информация рабочей станции, добавленной в список разрешенных ³
«Успешное выполнение персонализации носителя»	Персонализация СН завершена успешно
«Устройство подключено к USB порту»	Устройство подключено в USB-разъем компьютера
«Выполнен общий сброс СН»	Выполнена процедура общего сброса устройства

¹ Сообщение появляется, если в настройках политик доступа к СН на РС установлена опция «Доступ без ограничения».

² Сообщение появляется, если в настройках политик доступа к СН на РС установлена опция «Доступ с ограничением по доменам и рабочим станциям».

³ Сообщение появляется, если в настройках политик доступа к СН на РС установлена опция «Доступ с ограничением по доменам и рабочим станциям».

Информационное сообщение	Описание
«Выполнена очистка журнала работы СН»	Выполнена процедура очистки содержимого журнала работы СН
«Выполнено изменение размеров дисков»	Выполнена процедура изменения размеров дисков
«Контроль доступа временно отключен с ДД/ММ/ГГГГ по ДД/ММ/ГГГГ»	Ограничения на доступ к СН на РС временно отключены
«Постоянный контроль доступа возобновлен»	Флаг временного отключения контроля доступа снят администратором. Ограничения на доступ к СН на РС снова вступают в силу
«Установка внутреннего времени на ДД/ММ/ГГГГ чч:мм:сс»	Выполнена процедура установки/изменения внутреннего времени
«Устанавливаемое время РС ДД/ММ/ГГГГ чч:мм:сс»	Выполнена процедура изменения времени РС

8. Перечень принятых сокращений и обозначений

АМДЗ	–	аппаратный модуль доверенной загрузки;
СН	–	специальный носитель;
КА	–	код авторизации;
НСД	–	несанкционированный доступ;
ОС	–	операционная система;
ПАК	–	программно-аппаратный комплекс;
ПО	–	программное обеспечение;
РС	–	рабочая станция;
PUK	–	Personal Unblocking Key;
USB	–	Universal Serial Bus.