ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс защищенного хранения файлов журналов
«Программно-аппаратный неперезаписываемый журнал»

Руководство по эксплуатации

11443195.4012.067 РЭ

Листов 61

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством по эксплуатации программно-аппаратного комплекса «Программно-аппаратный неперезаписываемый журнал» (далее по тексту – ПАК «ПАЖ», либо «ПАЖ») – средства ведения неперезаписываемого журнала событий.

В документе приведены общие сведения о комплексе, основные функции, особенности установки, настройки и эксплуатации ПАК «ПАЖ».

Перед установкой и эксплуатацией ПАК «ПАЖ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных средств комплекса должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

1 Общие сведения

1.1 Назначение ПАК «ПАЖ»

ПАК «ПАЖ» предназначен для ведения аппаратного неперезаписываемого журнала событий.

Основные особенности ПАК «ПАЖ»:

- возможность экспортирования файлов журналов событий различных приложений из заданного каталога на жестком диске компьютера на диск аппаратного неперезаписываемого журнала;
- возможность экспортирования журнала комплекса «Аккорд-АМДЗ» на диск аппаратного неперезаписываемого журнала;
- возможность интеграции со сторонним программным обеспечением в части ведения аппаратного неперезаписываемого журнала с использованием специальной библиотеки, входящей в состав ПАК «ПАЖ» и реализующей интерфейс программирования приложений (API) для записи журналов приложений;
- возможность задания правил доступа к содержимому аппаратного журнала посредством настройки соответствующих политик: работа с диском аппаратного журнала на чтение или запись возможна только на заранее зарегистрированных в качестве разрешенных средствах вычислительной техники (СВТ). На любых других СВТ диск устройства не будет смонтирован, и оно не будет определяться в системе как «съемный диск». Все случаи подключений (как успешные, так и неуспешные) записываются в собственный журнал устройства, доступный для просмотра только его администратору.

Функционирование компонентов ПАК «ПАЖ» обеспечивает обслуживающий персонал, реализующий роли:

- Пользователь ПАК «ПАЖ» выполняет следующие процедуры:
  - создание новых файлов журналов;
  - добавление записей в имеющиеся файлы журналов;
  - экспорт файлов журналов приложений на закрытый раздел диска специального носителя (СН) «ПАЖ»;
  - смена параметров авторизации (кода авторизации, КА) пользователя;
  - разблокирование пользователя в случае превышения максимально допустимого количества неудачных попыток ввода КА.
- Администратор ПАК «ПАЖ» выполняет следующие процедуры:
  - регистрация администратора и пользователя ПАК «ПАЖ»;
  - аннулирование регистрации аудитора (в случае утраты им КА и PUK-кода для разблокирования «ПАЖ») или необходимости передачи «ПАЖ» другому аудитору;

- аннулирование регистрации пользователя (в случае утраты им КА и PUK-кода для разблокирования «ПАЖ») или необходимости передачи «ПАЖ» другому пользователю;
- настройка политик использования СН;
- добавление (удаление) рабочей станции (РС) в список разрешенных;
- смена пароля администратора;
- просмотр собственного журнала ПАК «ПАЖ».

- Аудитор ПАК «ПАЖ» выполняет следующие процедуры:
  - регистрация аудитора;
  - авторизация для доступа к журналам приложений;
  - просмотр, копирование файлов журналов приложений;
  - смена КА аудитора;
  - разблокирование аудитора в случае превышения максимально допустимого количества неудачных попыток ввода КА.

ПАК «ПАЖ» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением операционных систем (ОС) семейства Windows.

1.2 Состав комплекса

ПАК «ПАЖ» включает:

1) СН «ПАЖ»;

2) ПО РС, которое содержится на открытом разделе флеш-диска СН и не требует установки:

- библиотека, реализующая процедуру записи файлов журналов приложений на закрытый раздел диска СН «ПАЖ»;
- приложения для управления доступом к закрытому диску СН «ПАЖ».

СН «ПАЖ» представляет собой аппаратный модуль, выполненный по технологии флеш-диска с интерфейсом USB, предназначенный сбора и хранения файлов журналов приложений. Основными элементами данного аппаратного модуля являются:

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

2) энергонезависимая флеш-память, используемая для хранения файлов журналов приложений.

1.3 Технические условия применения комплекса

Для работы с ПАК «ПАЖ» необходим следующий минимальный набор технических и программных средств:

- установленная на РС ОС семейства Windows;
- 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.

2 Порядок работы ПАК «ПАЖ»

Типовой порядок работы ПАК «ПАЖ» состоит из следующих основных этапов:

- подключение СН «ПАЖ» (см. 2.1);
- запуск ПО РС (см. 2.2);
- регистрация администратора ПАК «ПАЖ» (см. 3.1);
- настройка администратором ПАК «ПАЖ» политик использования СН «ПАЖ» (см. 3.2);
- формирование списка разрешенных РС (см. 3.3 и 3.4);
- регистрация аудитора ПАК «ПАЖ» (см. 3.7);
- использование ПАК «ПАЖ» по назначению (см. 4).

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. 1.3).

После этого ОС обнаруживает новое устройство. Далее установка системного драйвера, как правило, происходит автоматически.

2.2 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;
- консоль аудитора.

При подключении СН к USB-разъему РС автоматически монтируется открытый диск СН, доступный только для чтения (рисунок 1). 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.

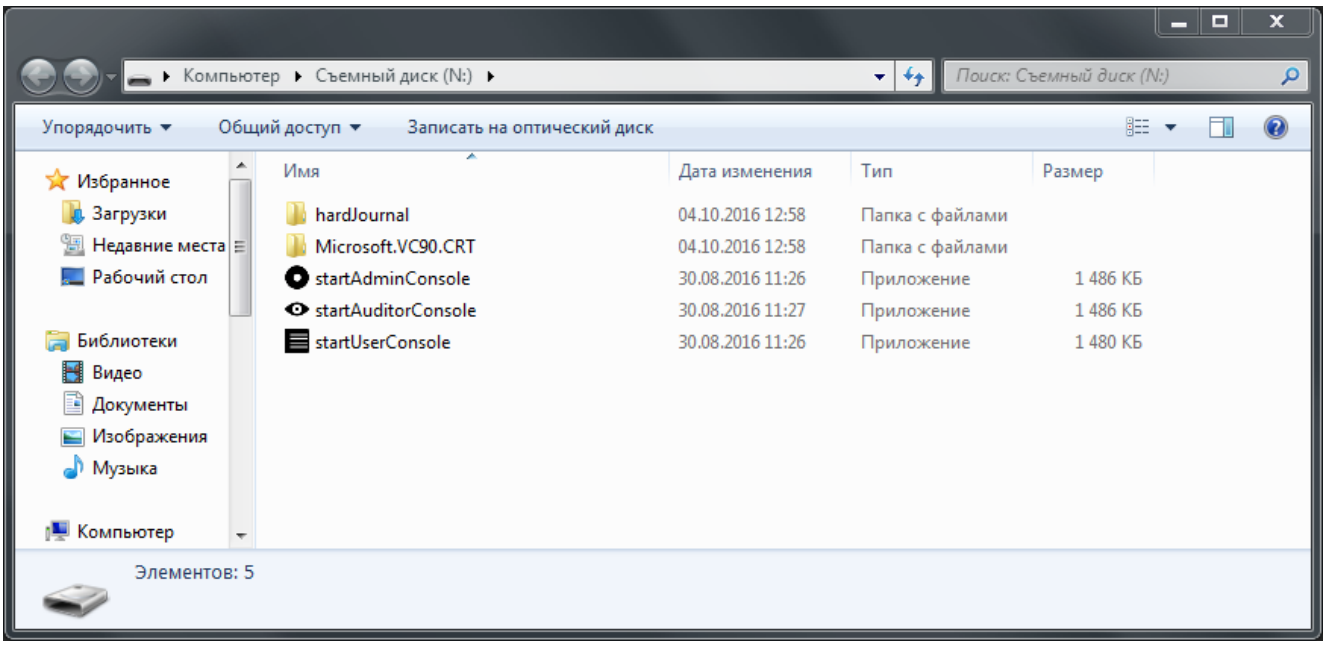


Рисунок 1 – Содержимое открытого раздела флеш-диска СН

2.3 Начало работы

Необходимо выполнить подключение СН «ПАЖ» к РС (допускается использование USB–хаба с внешним источником питания, см. подраздел 2.1).

Следующий шаг – запуск ПО РС (консоли администратора) (см. 2.2).

Далее выполняется процедуры регистрации администратора (см. 3.1), пользователя СН «ПАЖ» и аудитора СН «ПАЖ» (см. 3.7), в результате выполнения которых формируются пароль администратора, КА аудитора и КА пользователя. Эти процедуры выполняются один раз, в рабочем режиме повторять их не требуется.

Пароль администратора необходим для выполнения настроек политик использования и функций администрирования ПАК «ПАЖ» (подробнее см. п. 3.2-3.5).

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. 3.5).

КА аудитора необходим для выполнения следующих функций:

- авторизация аудитора при доступе к закрытому разделу диска СН «ПАЖ» (п. 3.8);
- смена КА (п. 3.9);
- разблокирование аудитора ПАК «ПАЖ» (п. 3.10).

Регистрация пользователя СН «ПАЖ» не относится к числу обязательных процедур. Процедура регистрации пользователя может использоваться в том случае, если необходимо ограничить возможность создания новых файлов журналов, добавления записей в имеющиеся файлы журналов, экспортирования файлов журналов приложений на закрытый раздел диска СН «ПАЖ» посредством механизма авторизации.

Следует отметить, что процедуры смены КА пользователя, разблокирования и аннулирования регистрации пользователя доступны, если в СН «ПАЖ» зарегистрирован пользователь.

Консоли из состава ПО ПАК «ПАЖ» не могут быть запущены на исполнение одновременно. При попытке запуска нескольких консолей на экране появляется соответствующее оповещение. Например, при попытке запустить консоль аудитора при работающей консоли администратора на экране появляется сообщение (рисунок 2):

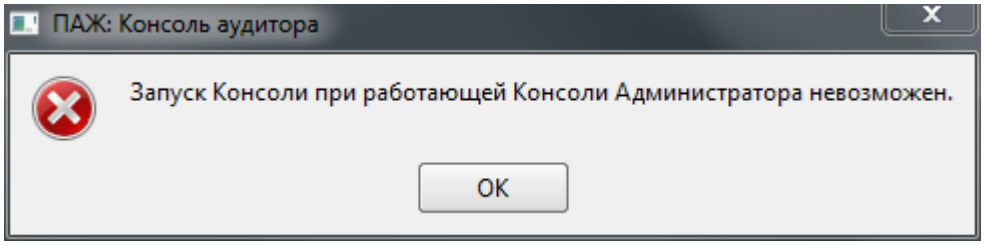


Рисунок 2 – Сообщение о невозможности запуска консоли аудитора при работающей консоли администратора

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

В случае блокирования СН аудитор может разблокировать СН с помощью PUK–кода. Если значение PUK–кода утеряно, разблокировать СН может только администратор с помощью функции «Аннулировать регистрацию аудитора…» (п. 3.11). При этом аннулируются параметры авторизации (PUK–код и КА).

После выполнения регистрации администратора и аудитора ПАК «ПАЖ» можно использовать по назначению (подробнее о способах использования ПАК см. п. 4).

3 Управление ПАК «ПАЖ»

3.1 Регистрация администратора

Для регистрации администратора необходимо запустить консоль администратора (исполняемый файл startAdminConsole.exe или исполняемый файл adminConsole.exe в папке hardJournal), хранящуюся на открытом разделе флеш-диска СН (см. подраздел 2.2). После этого в трее появляется значок ПАК «ПАЖ» (рисунок 3).

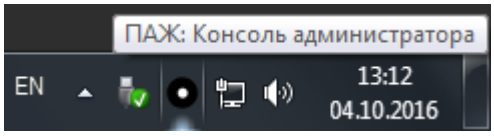


Рисунок 3 – Значок ПАК «ПАЖ» в трее

По нажатию правой кнопкой мыши на значок СН в трее на экране появляется меню (рисунок 4), которое содержит следующие пункты:

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

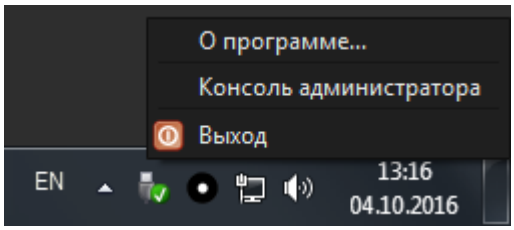


Рисунок 4 – Контекстное меню значка ПАК «ПАЖ» в трее

Если процедура регистрации администратора ранее не выполнялась, при запуске консоли администратора активна только функция регистрации администратора (рисунок 5). В графе «Состояние» отображается: «Персонализирован».

Рисунок 5 – Консоль администратора

Если зарегистрирован аудитор (но не зарегистрирован администратор), то в графе «Состояние» отображается: «Аудитор зарегистрирован» (рисунок 6).

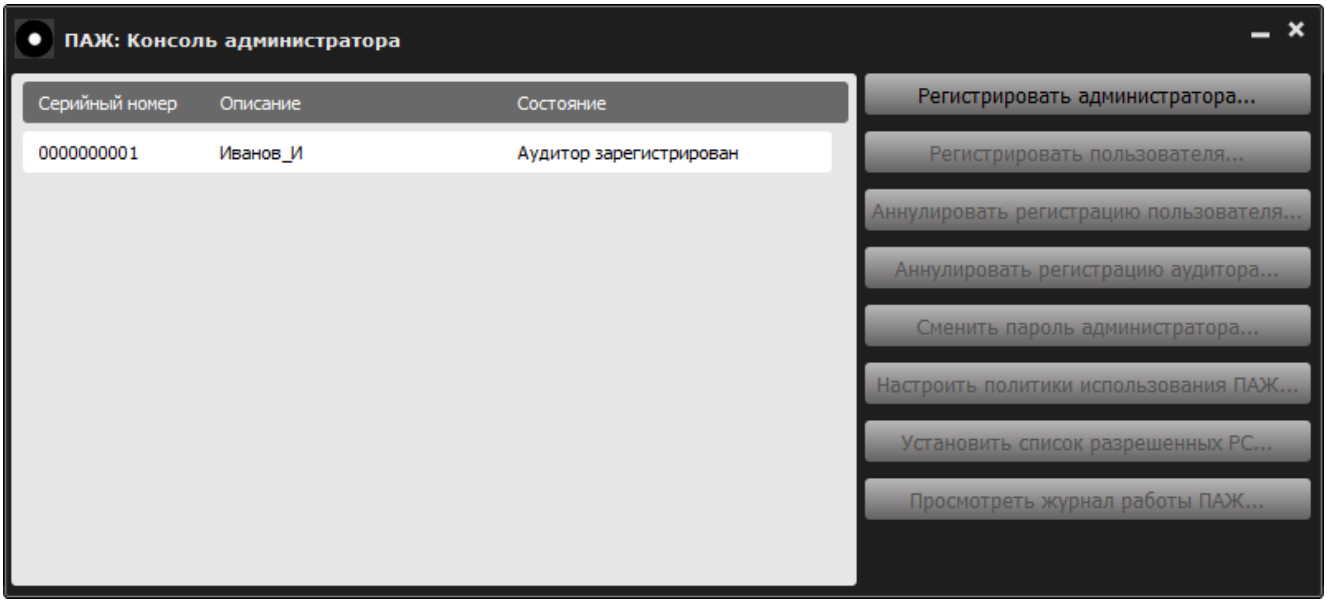


Рисунок 6 – Консоль администратора (зарегистрирован аудитор)

Чтобы зарегистрировать администратора, необходимо нажать кнопку <Регистрировать администратора…>. Далее на экране появляется окно регистрации администратора (рисунок 7).

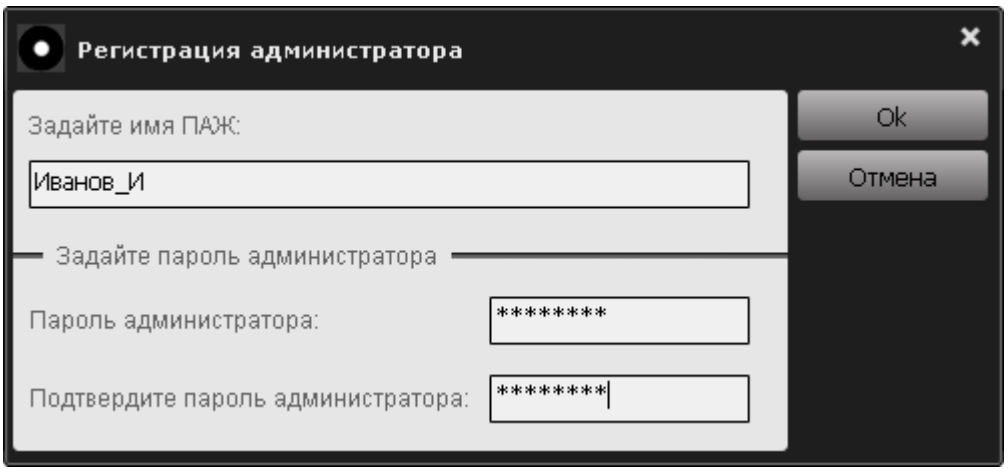


Рисунок 7 – Регистрация администратора

В появившемся диалоговом окне необходимо задать имя СН (имя СН уже могло быть задано ранее при регистрации аудитора, 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 СН «ПАЖ». Представляет собой строку, длина которой ограничена 32 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 СН «ПАЖ» не связано с защитными функциями и задается только для удобства владельца, 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 «ПАЖ». Важно помнить о необходимости сохранения пароля администратора недоступным для третьих лиц!

Кнопка <Ok> окна регистрации недоступна, если:

- имя «ПАЖ» 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 8).

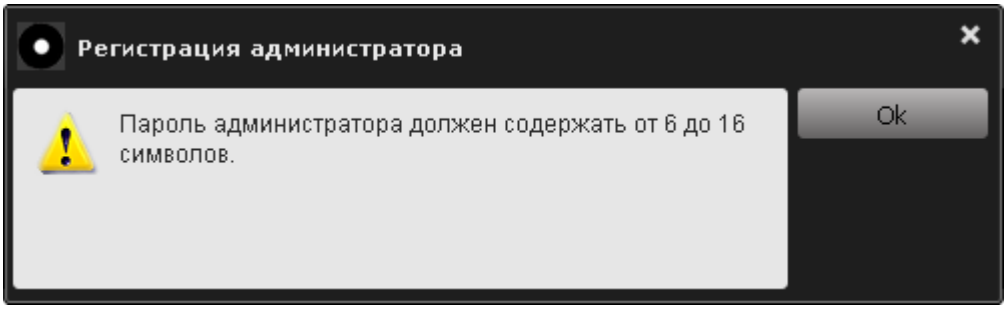


Рисунок 8 – Предупреждение о том, что пароль администратора должен содержать от 6 до 16 символов

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

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

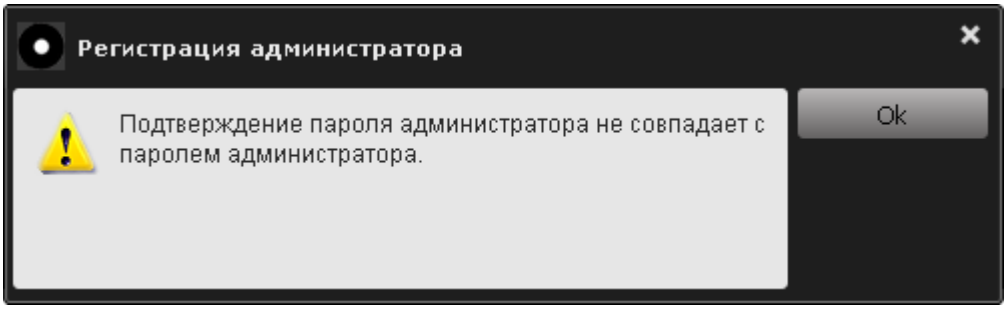


Рисунок 9 – Предупреждение об ошибке при подтверждении пароля администратора

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

ВНИМАНИЕ! Во время выполнения операции регистрации не отключайте СН «ПАЖ» 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).

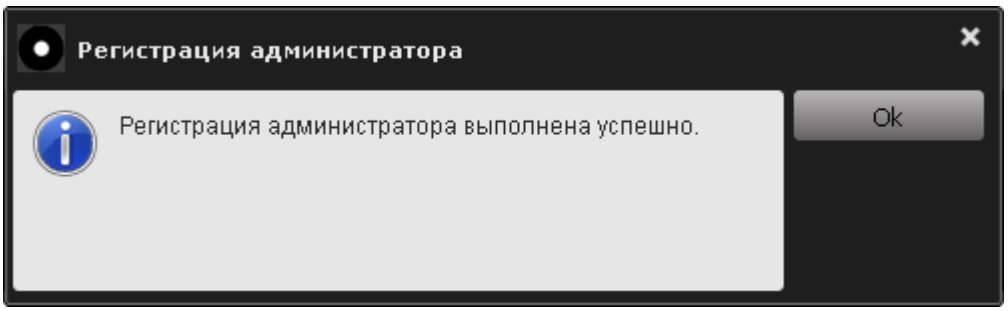


Рисунок 10 – Сообщение об успешной регистрации администратора

Далее функция регистрации администратора блокируется, и становятся доступными остальные функции администрирования (рисунок 11).

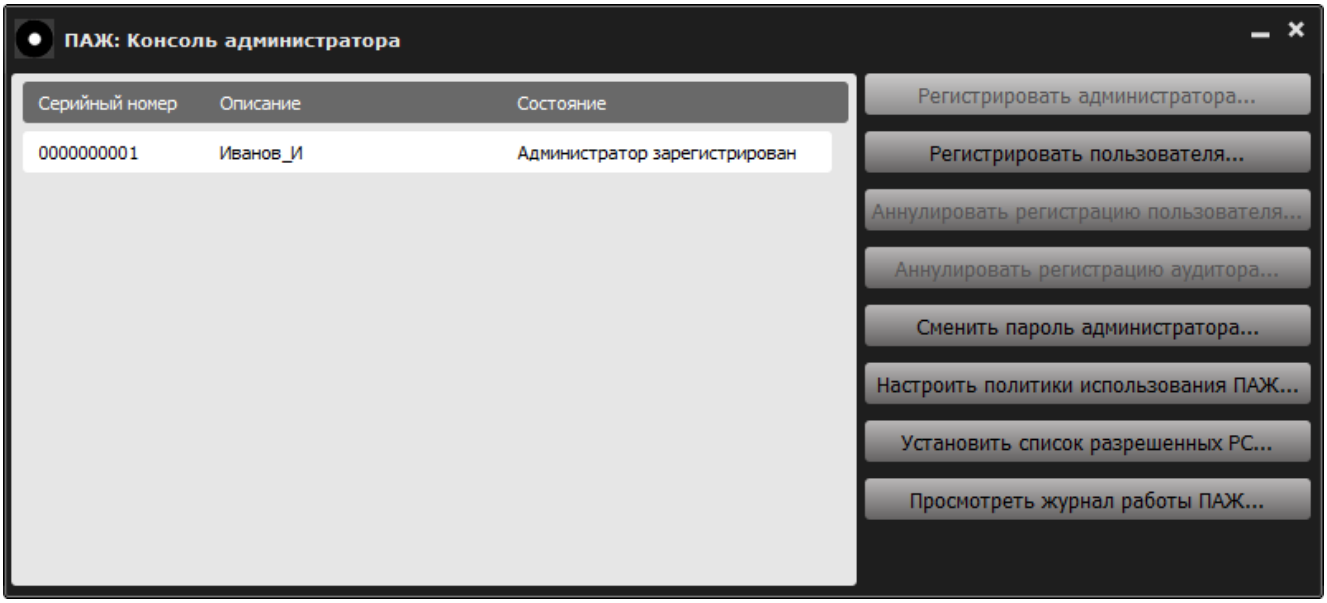


Рисунок 11 – Консоль администратора с доступными опциями

После регистрации аудитора (п. 3.7) и пользователя становятся доступными функции «Аннулировать регистрацию аудитора…» и «Аннулировать регистрацию пользователя…» (рисунок 12).

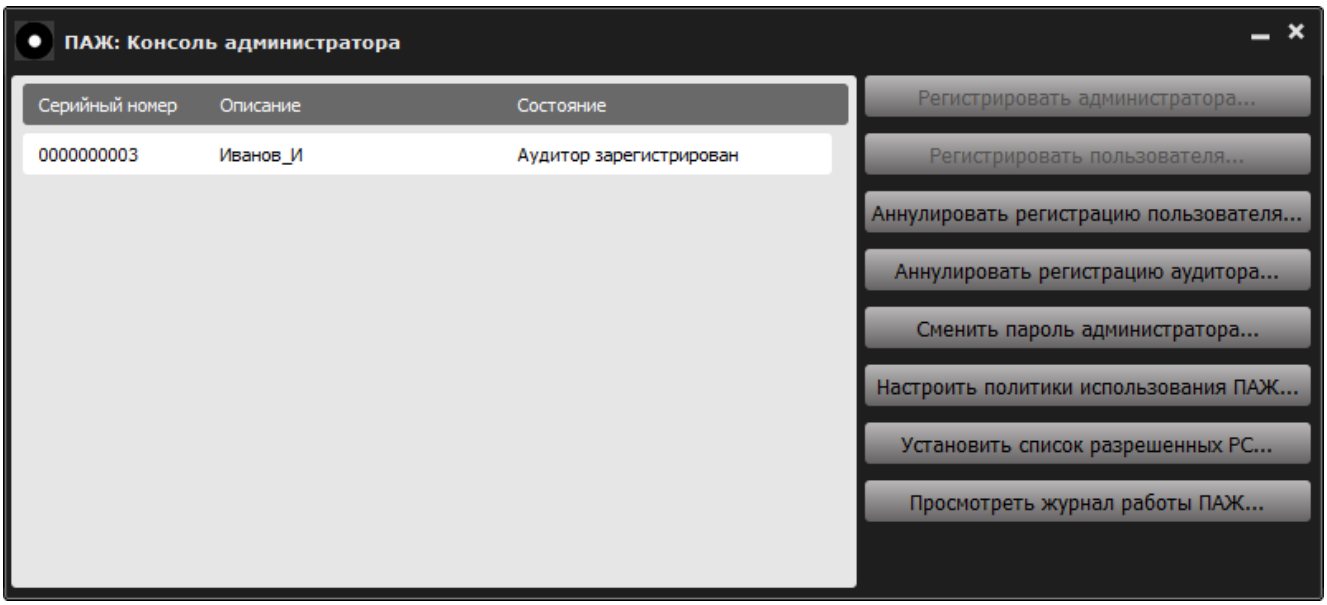


Рисунок 12 – Консоль администратора после регистрации аудитора

3.2 Настройка политик использования СН

До изменения настроек действуют политики по умолчанию:

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

В консоли администратора (рисунок 11) следует выбрать функцию «Настроить политики использования ПАЖ…». На экране появляется окно настройки политик (рисунок 13).

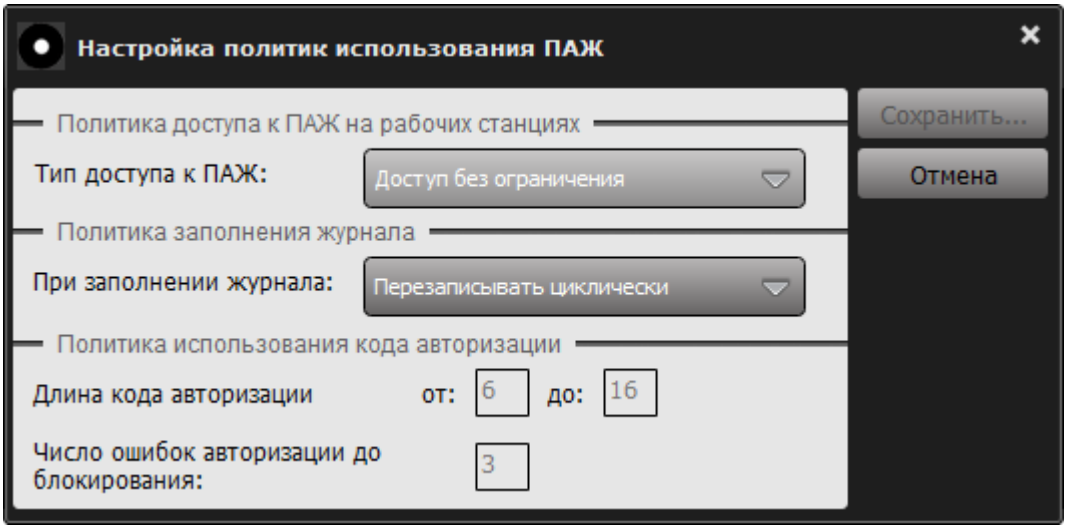


Рисунок 13 – Настройка политик использования СН «ПАЖ»

Экран настройки политик позволяет задать следующие параметры:

- тип доступа к СН «ПАЖ» на рабочих станциях;
- реакция при заполнении объема, выделенного для хранения журнала;

– длина КА и условия блокировки СН «ПАЖ».

3.2.1 Настройка политики доступа к СН на РС

Экран настройки политик доступа к СН «ПАЖ» на РС позволяет выбрать одно из следующих значений: «Доступ без ограничения», «Доступ с ограничением по доменам и рабочим станциям» (рисунок 14).

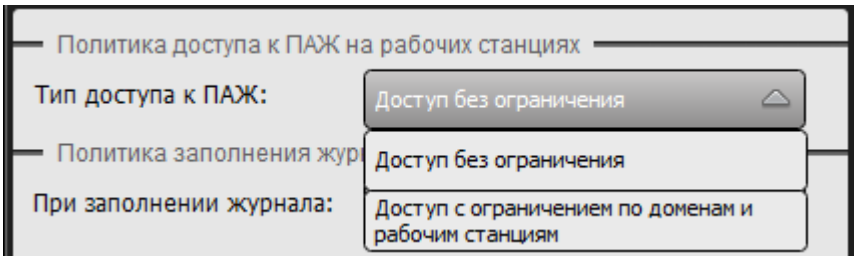


Рисунок 14 – Политика доступа к СН «ПАЖ» на РС

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 аудитора СН получает от ПО РС идентификатор домена и идентификатор РС в домене, и на основании полученных данных устройство разрешает доступ или отказывает в авторизации аудитору при нарушении политики доступа.

3.2.2 Настройка реакции при заполнении объема, выделенного для хранения журнала

Экран настройки действий при возможном переполнении собственного журнала событий СН (рисунок 15) позволяет выбрать одно из следующих значений:

– перезаписывать циклически;
– блокировать при переполнении.

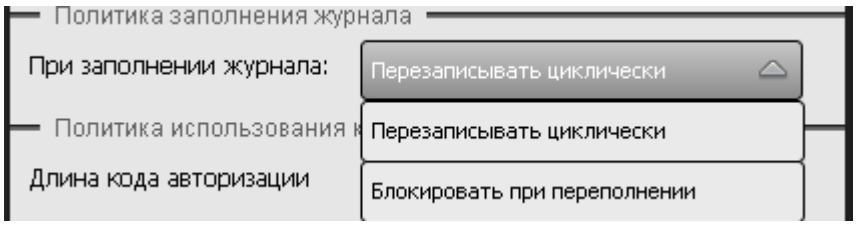


Рисунок 15 – Политика заполнения журнала

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 функций аудитора СН до тех пор, пока администратор не выполнит очистку журнала событий.

3.2.3 Настройка политики использования КА

Экран настройки политик использования КА 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 16));
- 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 16).

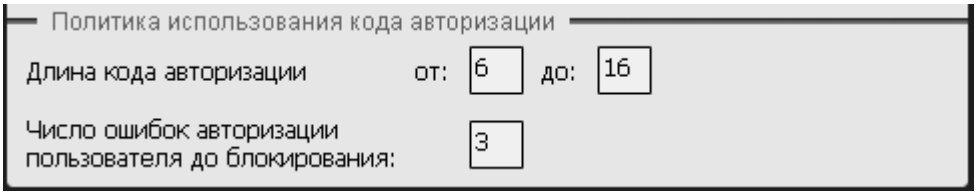


Рисунок 16 – Окно настройки политики использования КА

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 17):

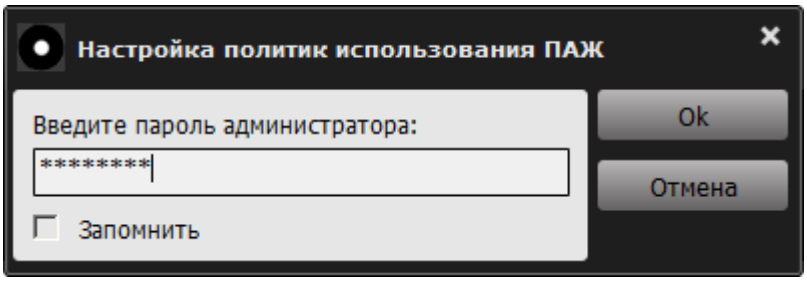


Рисунок 17 – Окно запроса пароля администратора

Для того чтобы завершить операцию настройки политик, 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 18).

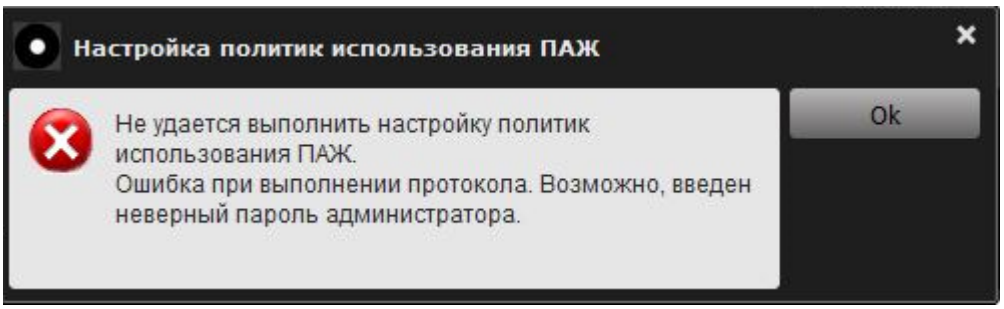


Рисунок 18 – Сообщение об ошибке в процессе ввода пароля

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 «ПАЖ» (рисунок 19).

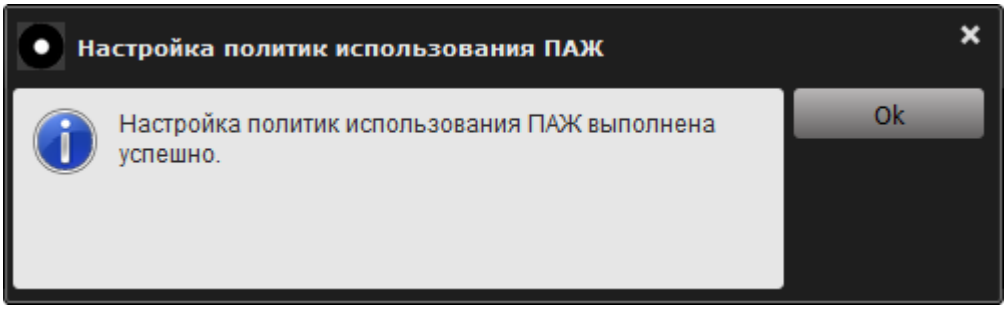


Рисунок 19 – Сообщение об успешном выполнении настройки СН «ПАЖ»

Для продолжения работы с консолью администратора (рисунок 11) следует нажать кнопку <Ok>.

3.3 Добавление РС в список разрешенных

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…». После этого на экране появляется окно установки списка разрешенных РС (рисунок 20).

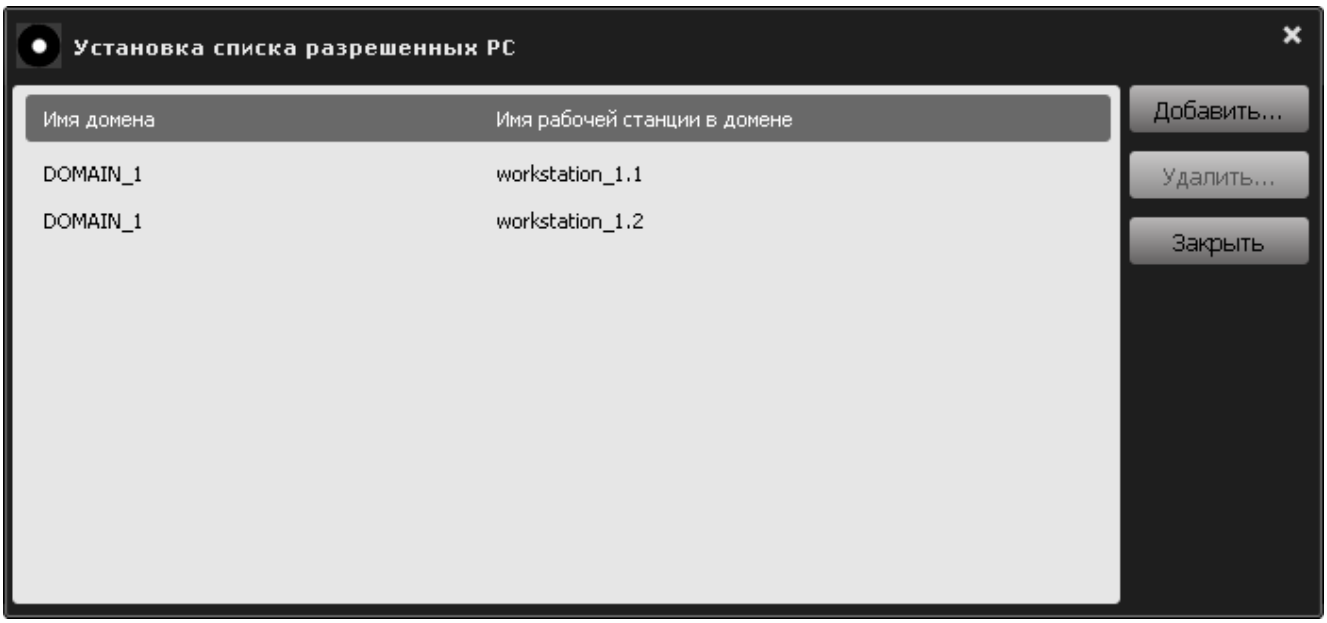


Рисунок 20 – Установка списка разрешенных станций

По нажатии кнопки <Добавить…> на экране появляется окно выбора рабочей станции (рисунок 21):

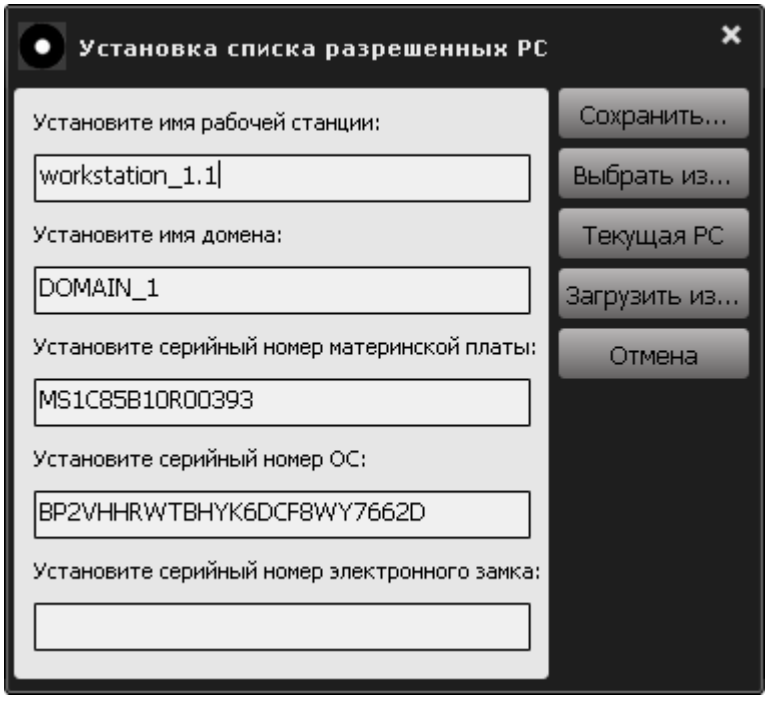


Рисунок 21 – Окно установки имени и домена рабочей станции

Следует ввести следующие параметры (три последних параметра являются необязательными для заполнения):

- имя PC;
- имя домена (рабочей группы), в котором находится данная PC;
- серийный номер материнской платы;
- серийный номер ОС;
- серийный номер электронного замка.

По выполнении описанной последовательности действий необходимо 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 22):

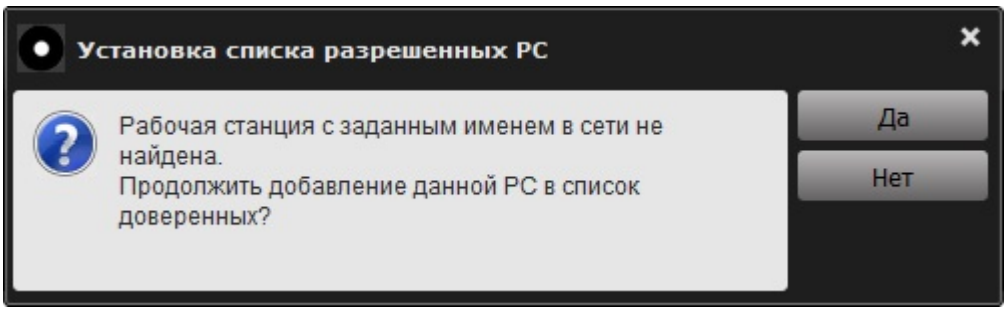


Рисунок 22 – Оповещение о том, что рабочая станция с заданным именем не найдена в сети

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 23).

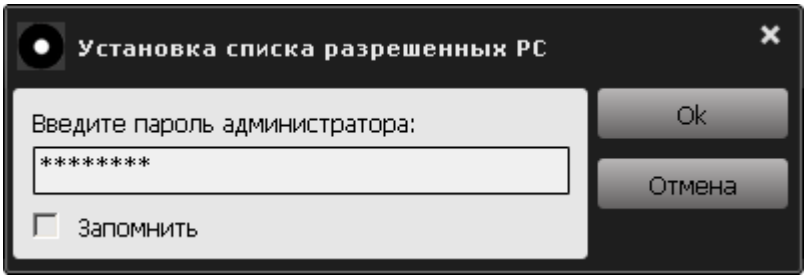


Рисунок 23 – Окно ввода пароля

Если домена с заданным именем в сети не найден, то на экране появляется сообщение (рисунок 24):

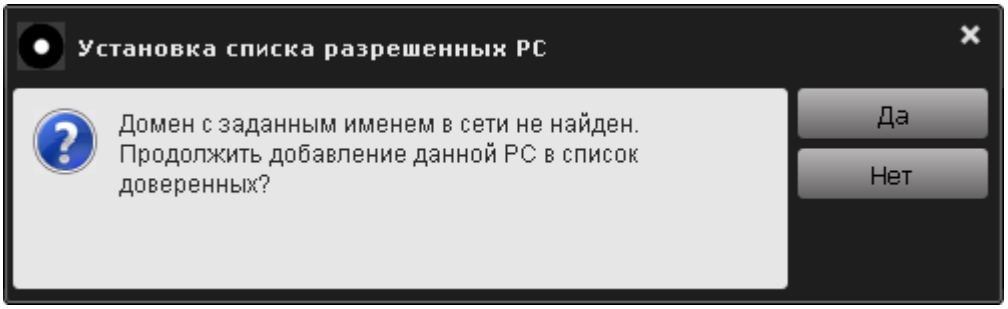


Рисунок 24 – Оповещение о том, что домен с заданным именем не найден в сети

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 23). Необходимо ввести пароль администратора и нажать кнопку <Ok>. Либо кнопку <Отмена> для прерывания текущей операции.

По нажатии кнопки <Текущая РС> (рисунок 21) на экране появляются имя и домен РС, на которой в данный момент времени работает аудитор или пользователь СН.

По нажатии кнопки <Выбрать из…> (рисунок 21) на экране отображается окно с доступными доменными именами РС (рисунок 25).

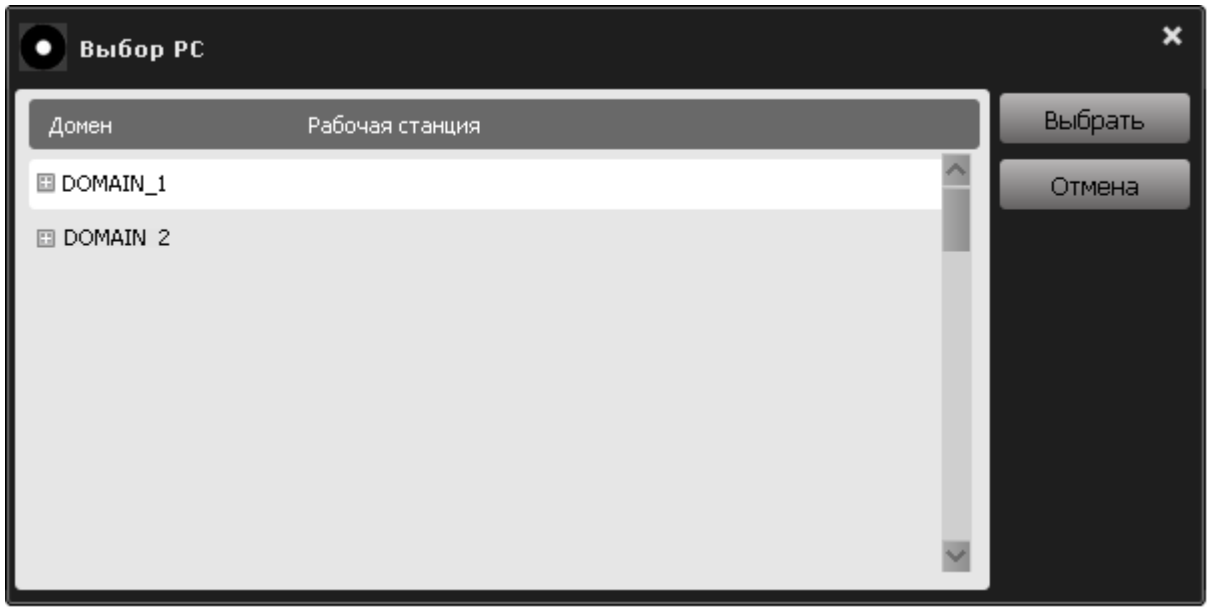


Рисунок 25 – Список доменных имен РС

Следует нажать на кнопку ⊞, чтобы увидеть список имен различных рабочих станций находящихся в доменах (рисунок 26).

Рисунок 26 – Выбор имени разрешенной рабочей станции

Необходимо отметить нужное имя и нажать кнопку <Выбрать…> (рисунок 26). Для отмены текущей операции следует нажать кнопку <Отмена>.

После выбора нужной РС на экран вновь выводится окно установки имени и домена разрешенных РС (рисунок 21), но в полях этого окна будут записаны имя и домен выбранной РС (рисунок 27).

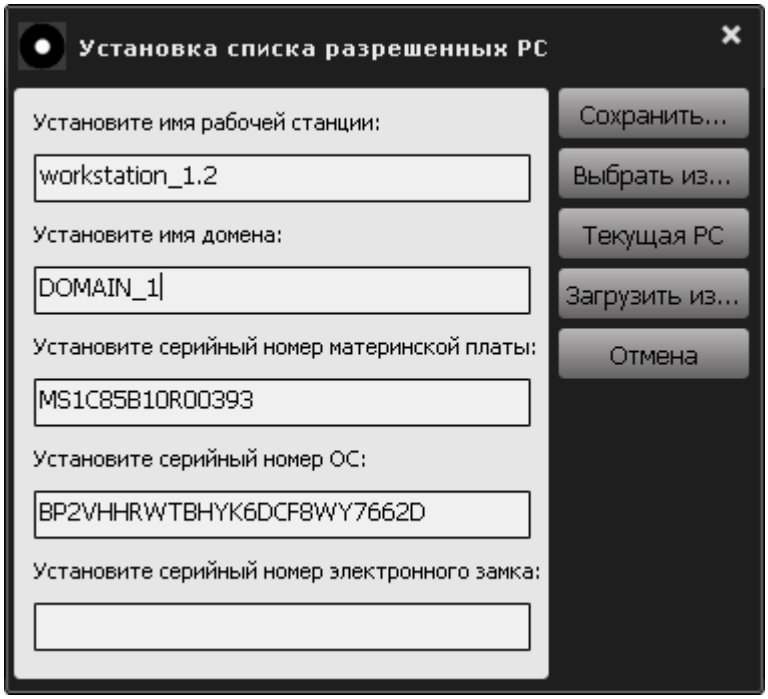


Рисунок 27 – Окно установки списка разрешенных РС с введенными именем и именем домена РС

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

По нажатии кнопки <Сохранить…> на экране появляется окно для ввода пароля (рисунок 28).

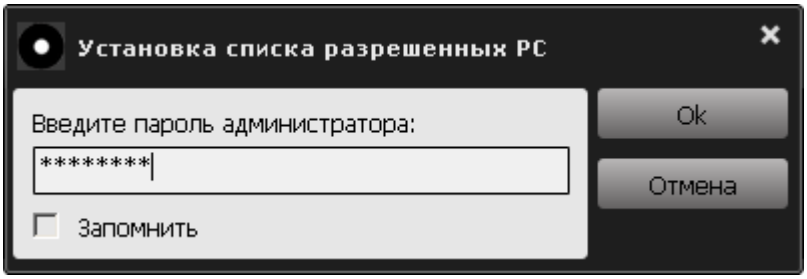


Рисунок 28 – Окно ввода пароля

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 РС (рисунок 29).

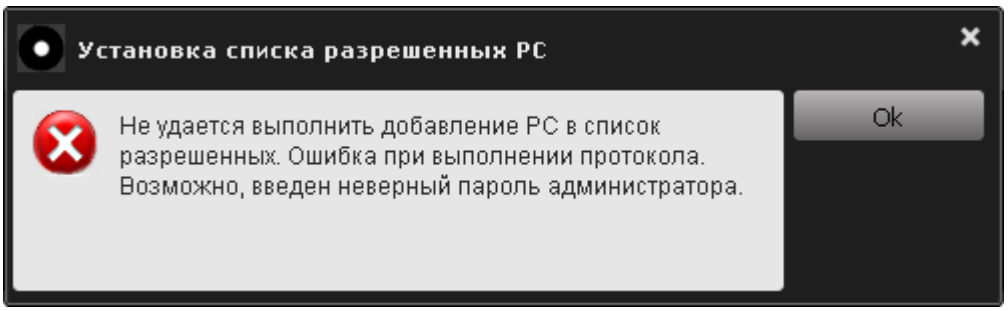


Рисунок 29 – Сообщение об ошибке в процессе ввода пароля администратора

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 30).

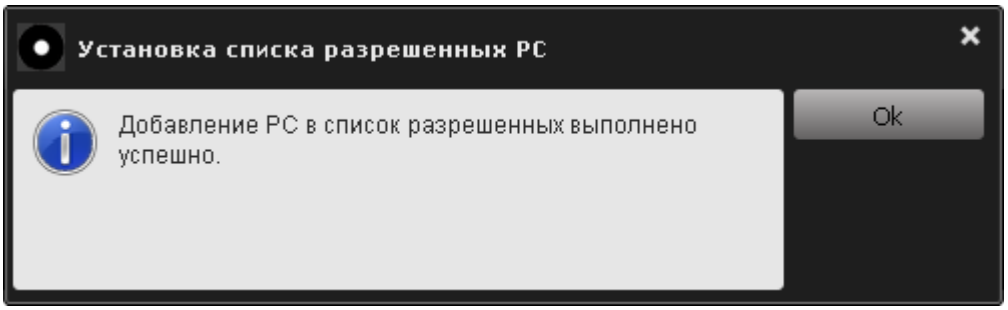


Рисунок 30 – Сообщение об успешном выполнении установки разрешенных PC

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 закрытому разделу диска СН «ПАЖ» на PC.

ВНИМАНИЕ! При корпоративном применении ПАК «ПАЖ» в целях безопасности рекомендуется, чтобы первое подключение СН к PC выполнял администратор.

Если в настройках политики доступа к PC был выбран тип доступа к PC: «Доступ без ограничений», то после выполнения процедуры добавления PC в список разрешенных на экране появляется оповещение (рисунок 31) о том, что внесенные изменения вступят в силу после установки типа доступа к PC «Доступ с ограничением по доменам и рабочим станциям».

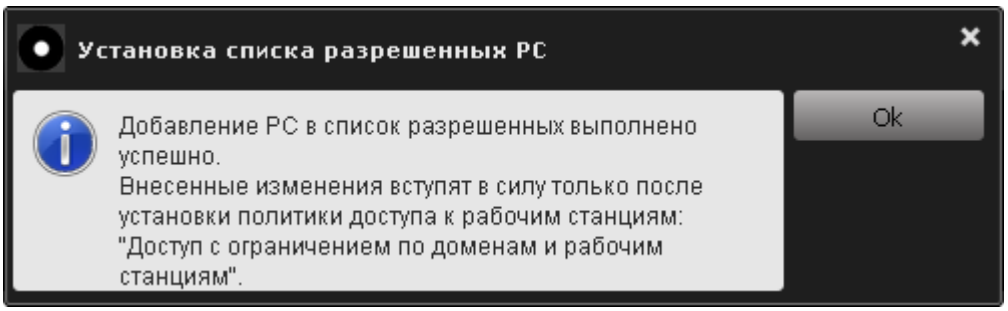


Рисунок 31 – Сообщение о внесенных изменениях

3.4 Удаление PC из списка разрешенных

Если необходимо удалить PC из числа разрешенных, в списке разрешенных PC следует выбрать нужную запись и нажать кнопку <Удалить…> (рисунок 32).

Рисунок 32 – Список разрешенных PC

После этого на экране появляется окно запроса пароля администратора, как показано на рисунке 33:

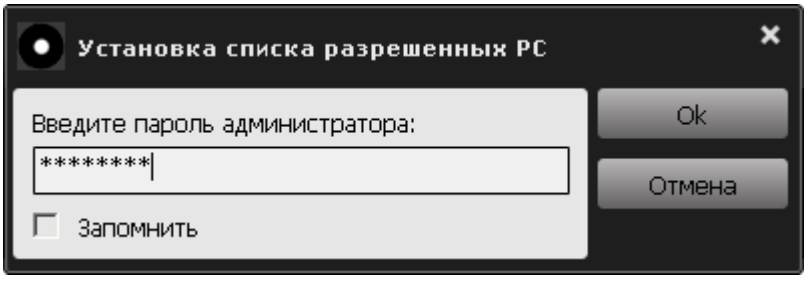


Рисунок 33 – Окно ввода пароля администратора

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 РС из списка разрешенных (рисунок 34):

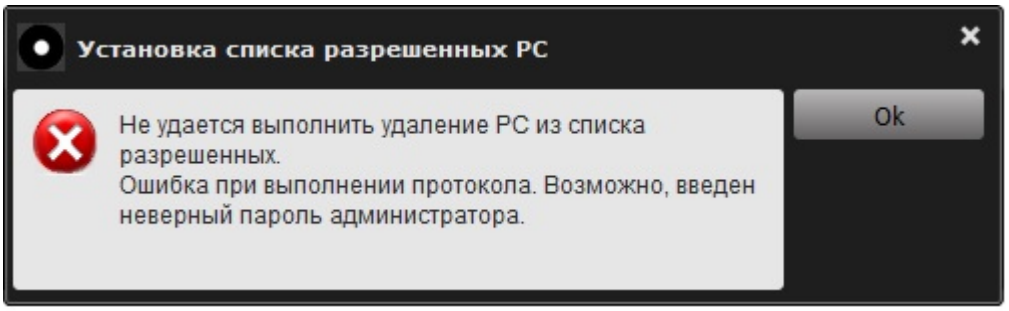


Рисунок 34 – Сообщение об ошибке при выполнении операции удаления разрешенной РС

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

Если операция удаления разрешенной РС выполнена корректно, на экране отображается сообщение об успешном удалении РС из списка разрешенных (рисунок 35):

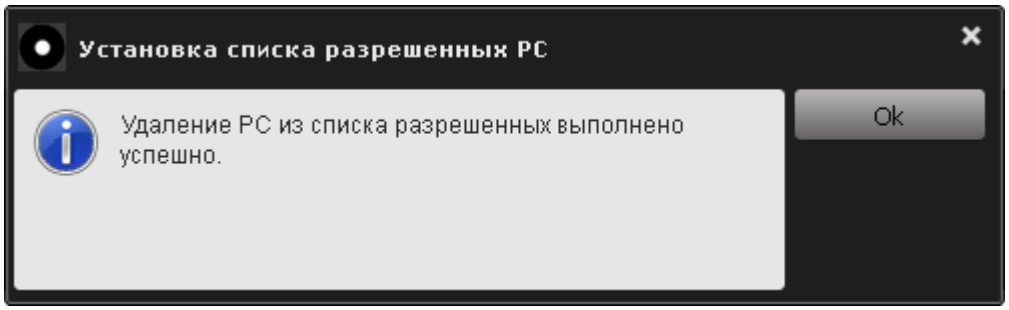


Рисунок 35 – Сообщение об успешном удалении РС из списка разрешенных РС

После завершения всех необходимых операций со списком разрешенных РС в окне задания списка разрешенных РС (рисунок 20) нужно нажать кнопку <Закрыть>.

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 на экране появляется сообщение (рисунок 36), оповещающее о том, что внесенные изменения вступят в силу после установки типа доступа к РС «Доступ с ограничением по доменам и рабочим станциям».

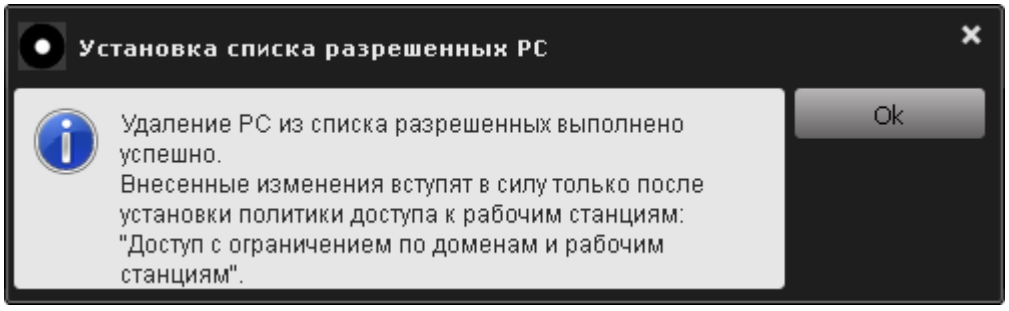


Рисунок 36 – Сообщение о внесенных изменениях

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…». После выбора этой функции на экране появляется окно, показанное на рисунке 37.

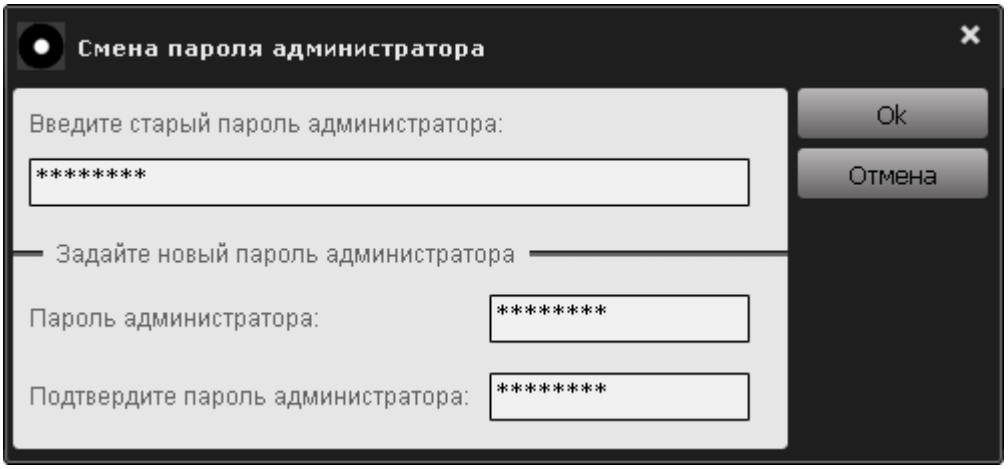


Рисунок 37 – Окно смены пароля администратора

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 38).

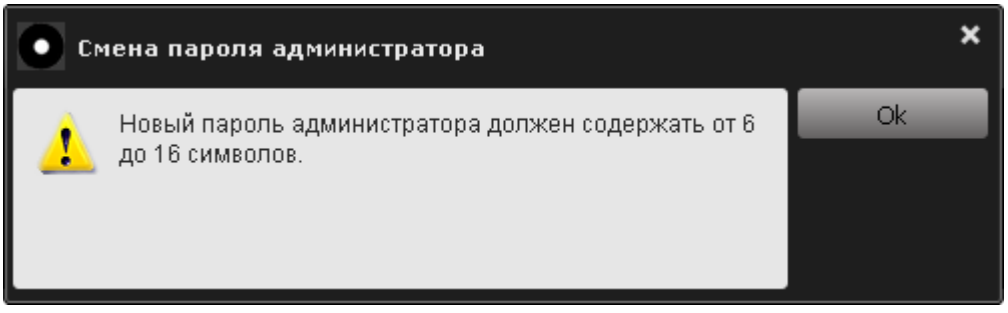


Рисунок 38 – Предупреждение о том, что новый пароль администратора должен содержать от 6 до 16 символов

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

Если подтверждение пароля введено некорректно, на экране появляется предупреждение (рисунок 39):

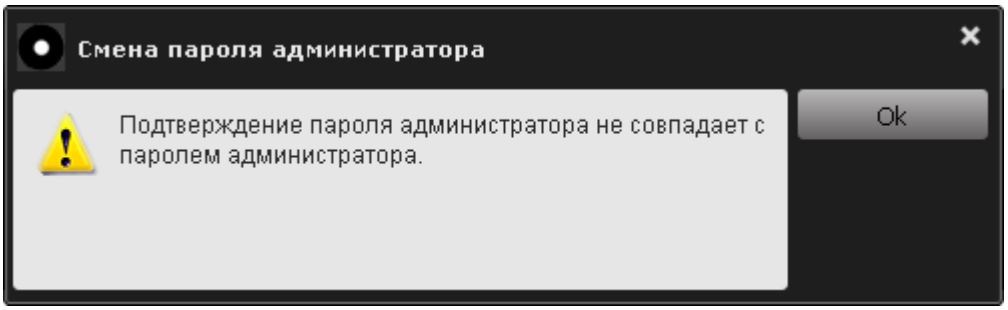


Рисунок 39 – Предупреждение о том, что подтверждение пароля администратора не совпадает с паролем администратора

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 40).

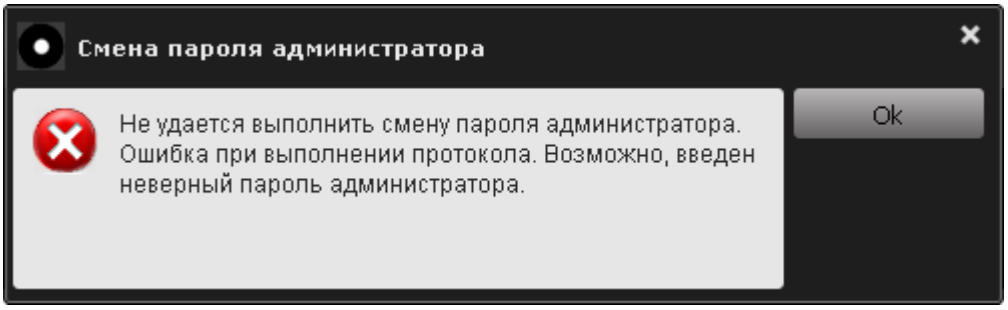


Рисунок 40 – Сообщение о вводе некорректного старого пароля

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 41):

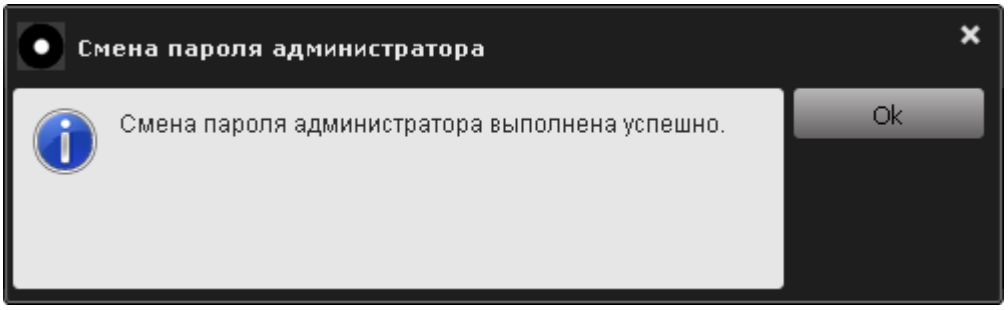


Рисунок 41 – Оповещение об успешной смене пароля

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

3.6 Просмотр журнала событий

ВНИМАНИЕ! Доступ к журналу событий ПАК «ПАЖ» имеет только администратор устройства.

Для того чтобы посмотреть журнал событий СН «ПАЖ», необходимо нажать кнопку «Просмотреть журнал работы ПАЖ…» на панели консоли администратора (рисунок 11).

После выбора данной функции на экране появляется окно с запросом пароля администратора СН для доступа к журналу работы (рисунок 42). 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.

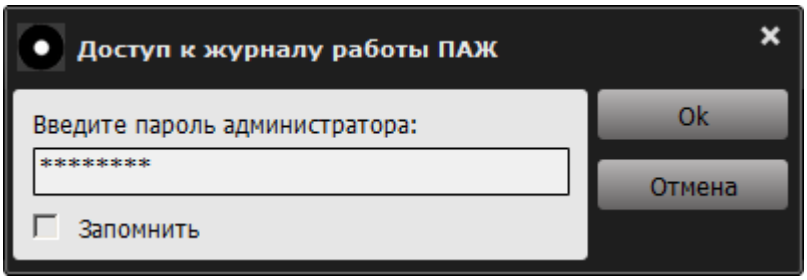


Рисунок 42 – Запрос пароля администратора для доступа к журналу работы СН «ПАЖ»

Если пароль введен некорректно, то на экране отображается сообщение об ошибке при вводе пароля администратора (рисунок 43):

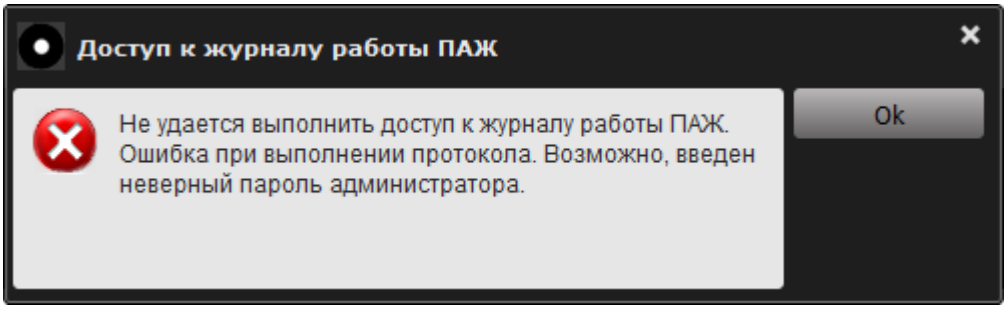


Рисунок 43 – Ошибка при выполнении доступа к протоколу работы СН «ПАЖ»

Если пароль введен корректно, на экране появляется сообщение об успешном доступе к протоколу работы (рисунок 44).

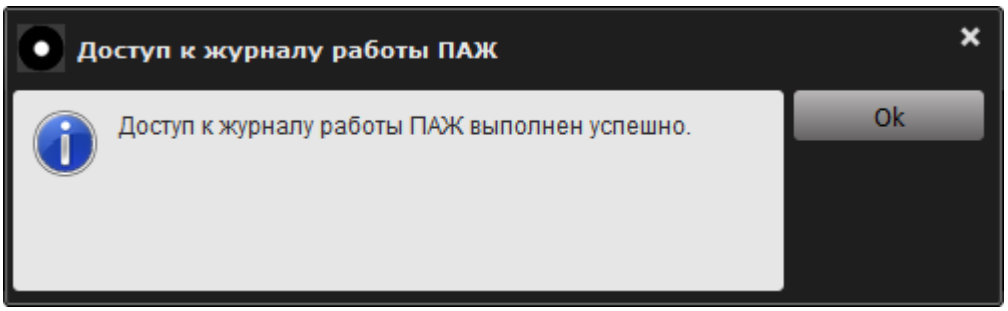
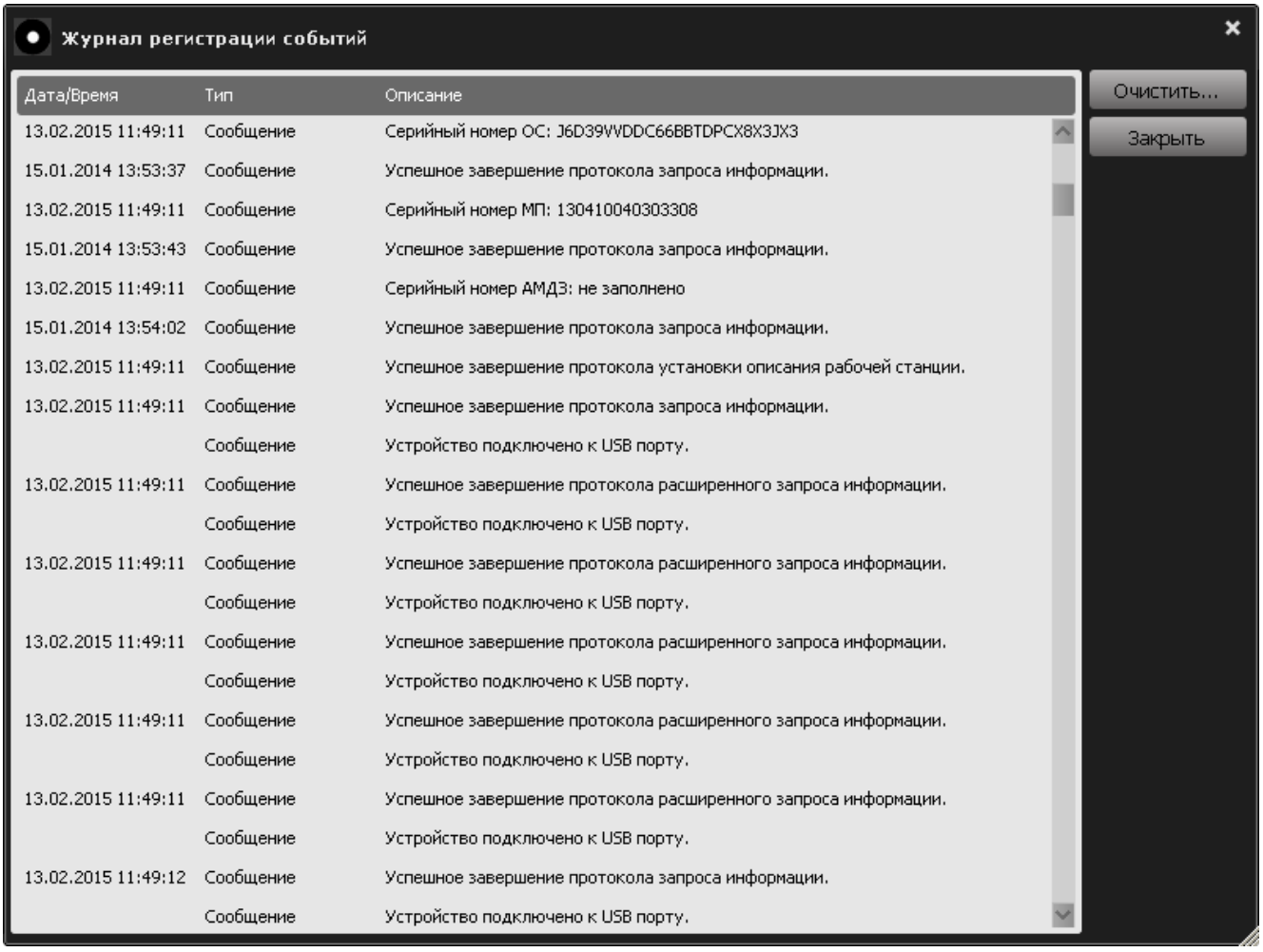


Рисунок 44 – Сообщение об успешном доступе к протоколу работы СН «ПАЖ»

По нажатии кнопки <Ok> на экране появляется журнал регистрации событий (рисунок 45), который содержит информацию о событиях, зафиксированных в процессе работы с ПАК «ПАЖ» 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).



Дата/Время	Тип	Описание
13.02.2015 11:49:11	Сообщение	Серийный номер ОС: J6D39WDDC66BBTDPCX8X3JX3
15.01.2014 13:53:37	Сообщение	Успешное завершение протокола запроса информации.
13.02.2015 11:49:11	Сообщение	Серийный номер МП: 130410040303308
15.01.2014 13:53:43	Сообщение	Успешное завершение протокола запроса информации.
13.02.2015 11:49:11	Сообщение	Серийный номер АМДЗ: не заполнено
15.01.2014 13:54:02	Сообщение	Успешное завершение протокола запроса информации.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола установки описания рабочей станции.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола расширенного запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола расширенного запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола расширенного запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола расширенного запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:11	Сообщение	Успешное завершение протокола расширенного запроса информации.
	Сообщение	Устройство подключено к USB порту.
13.02.2015 11:49:12	Сообщение	Успешное завершение протокола запроса информации.
	Сообщение	Устройство подключено к USB порту.

Рисунок 45 – Журнал регистрации событий

В журнале событий фиксируется время возникновения события в соответствии с системным временем ОС. При сортировке по дате/времени события на самом деле отображаются не по времени, а в порядке их действительного возникновения.

Если журнал 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 45).

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.

Далее запрашивается пароль администратора для доступа к журналу работы СН (рисунок 46).

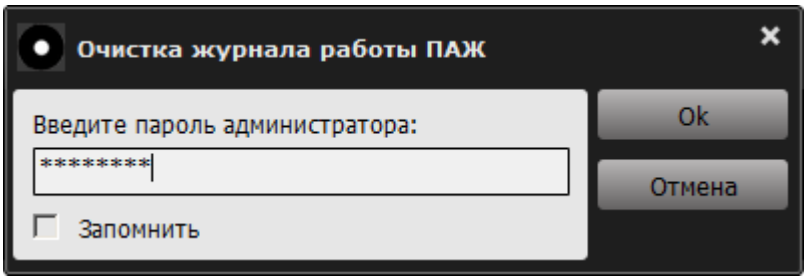


Рисунок 46 – Запрос пароля администратора для очистки журнала работы СН «ПАЖ»

В случае если пароль введен некорректно, на экране появляется оповещение об ошибке (рисунок 47):

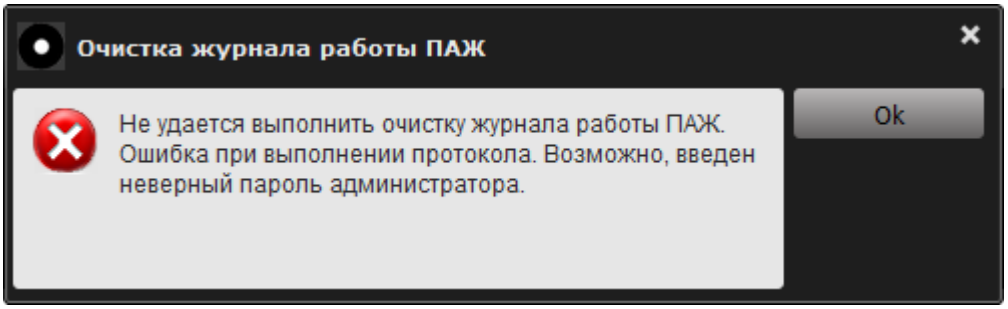


Рисунок 47 – Оповещение о невозможности доступа к протоколу работы СН «ПАЖ»

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 48).

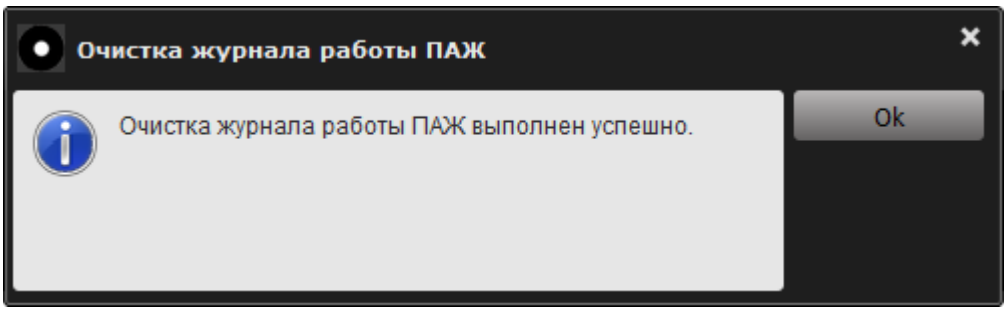


Рисунок 48 – Сообщение об успешном выполнении сброса протокола работы СН «ПАЖ»

После выполнения всех необходимых действий с журналом регистрации событий, можно нажать кнопку <Закрыть>.

3.7 Регистрация аудитора СН

Для регистрации аудитора необходимо запустить консоль аудитора (исполняемый файл startAuditorConsole.exe или исполняемый файл auditorConsole.exe в папке hardJournal), хранящуюся на открытом разделе флеш-диска СН (см. подраздел 2.2). После этого в трее появляется значок консоли аудитора ПАК «ПАЖ» (рисунок 49).

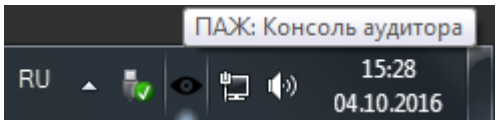


Рисунок 49 – Значок ПАК «ПАЖ» в трее

По нажатию правой кнопкой мыши на значок СН в трее на экране появляется меню (рисунок 50), которое содержит следующие поля:

- «О программе» - выводит сведения о ПО ПАК «ПАЖ»;
- «Консоль аудитора» – позволяет открыть консоль аудитора;
- «Выход» - осуществляет выход из программы.

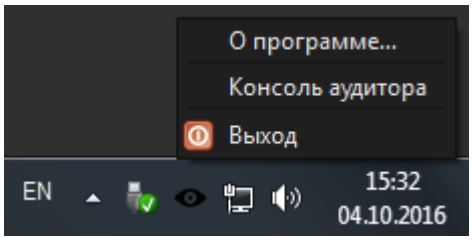


Рисунок 50 – Контекстное меню значка ПАК «ПАЖ»в трее

Если процедура регистрации аудитора ранее не выполнялась, при запуске консоли аудитора активна только функция регистрации аудитора СН (рисунок 51). Если до регистрации аудитора на СН была выполнена регистрация администратора, то в консоли аудитора в графе «Состояние» будет отображаться статус «Администратор зарегистрирован», а в графе «Описание» - имя СН.

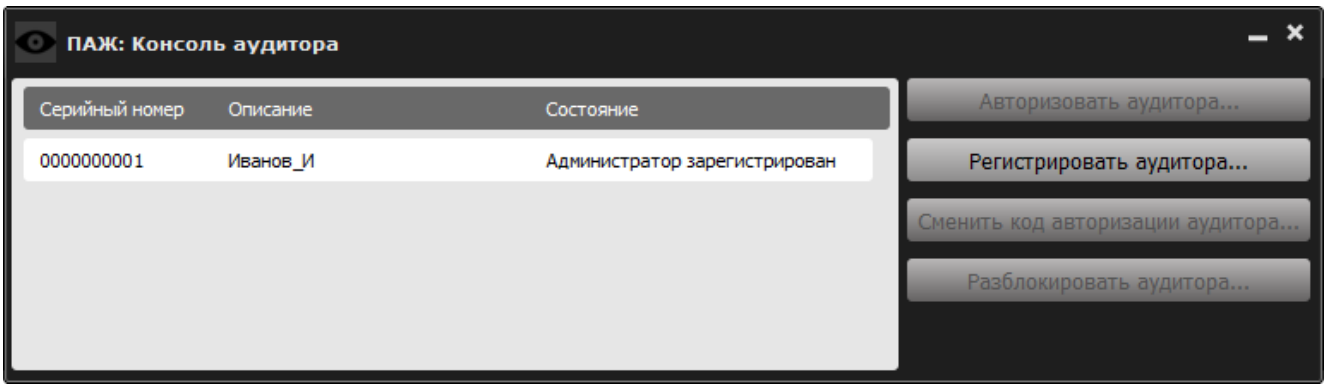


Рисунок 51 – Консоль аудитора

После выбора этой функции посредством нажатия кнопки <Регистрировать аудитора…> на экране отображается окно регистрации аудитора (рисунок 52).

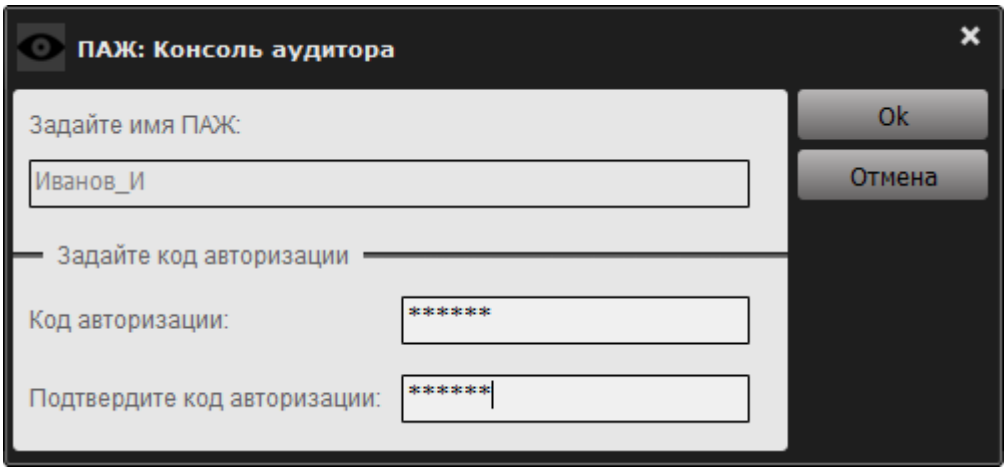


Рисунок 52 – Регистрация аудитора

В появившемся диалоговом окне необходимо установить КА аудитора с подтверждением. Для завершения операции необходимо нажать <Ok>, для отмены операции – кнопку <Отмена>.

Регистрационный параметр аудитора СН – КА аудитора. Представляет собой строку, длина которой варьируется в пределах от 6 до 16 произвольных символов.

В процессе авторизации аудитора формируется PUK-код (16 цифр), необходимый для восстановления возможности получения доступа к закрытому разделу диска СН «ПАЖ» при блокировании аудитора (в случае превышения порога неудачных попыток авторизации).

Кнопка <Ok> окна регистрации недоступна, если не заданы значения в полях «Код авторизации» или «Подтвердите код авторизации».

Если вводимое количество символов КА меньше минимального значения, установленного администратором, на экране появится следующее предупреждение (рисунок 53).

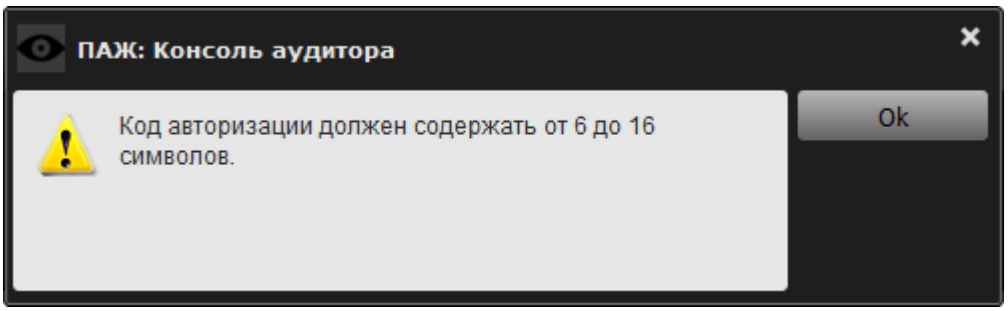


Рисунок 53 – Предупреждение о том, что КА должен содержать от 6 до 16 символов

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

Если подтверждение КА не совпадает с исходным КА, на экране появляется предупреждение (рисунок 54):

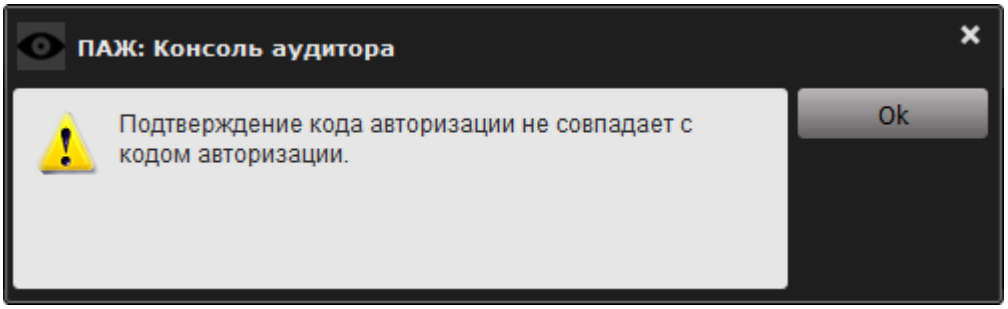


Рисунок 54 – Предупреждение о том, что подтверждение КА не совпадает с КА

В таком случае нужно в поле данного сообщения нажать кнопку <Ok> и ввести корректный КА.

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

После процесса регистрации аудитора СН на экране появляется сообщение об успешной регистрации (рисунок 55):

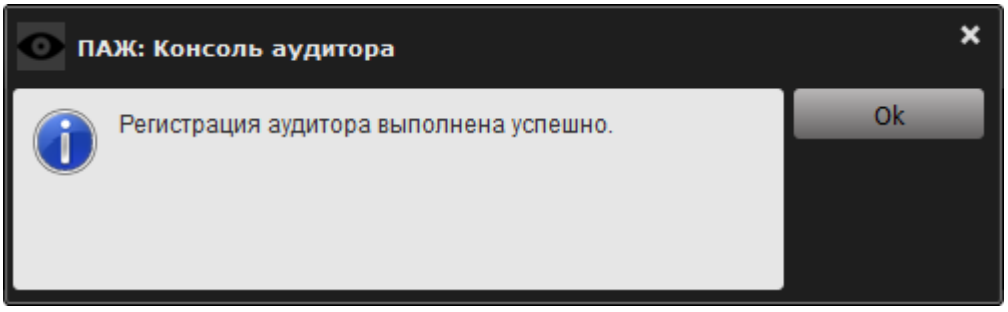


Рисунок 55 – Сообщение об успешном завершении процесса регистрации аудитора

После нажатия кнопки <Ok> на экране отобразится сообщение с серийным номером, именем СН, КА и PUK-кодом аудитора (рисунок 56). Имеется возможность вывода этой информации на печать посредством нажатия кнопки <Печать…>.

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить КА и PUK-код, знание которых позволяет получать доступ к файлам журналов приложений, записанным на закрытый раздел флеш-диска СН «ПАЖ». Важно помнить о необходимости сохранения этих данных недоступными третьим лицам!

В случае утраты КА и PUK-кода СН необходимо выполнить процедуру аннулирования регистрации аудитора СН, которая приведет к стиранию параметров аутентификации аудитора (КА и PUK-код СН).

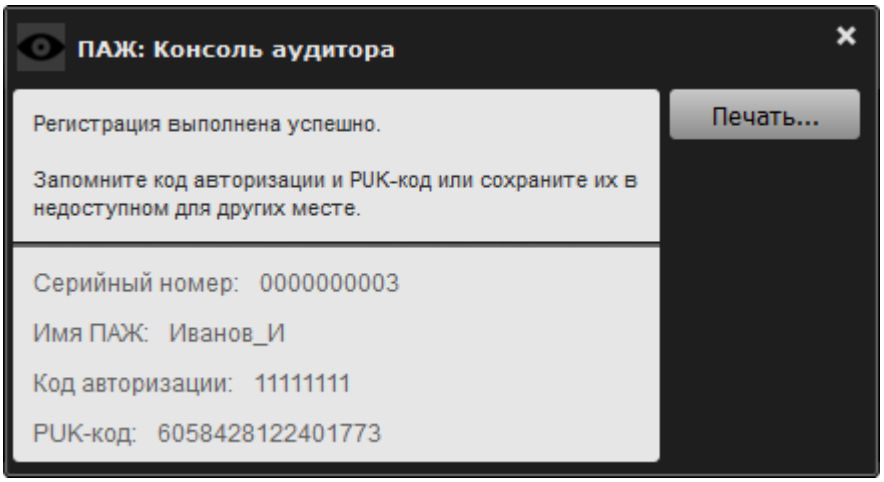


Рисунок 56 – Информация об аудиторе

По нажатию кнопки <Печать…> на экране появляется окно печати документа (рисунок 57):

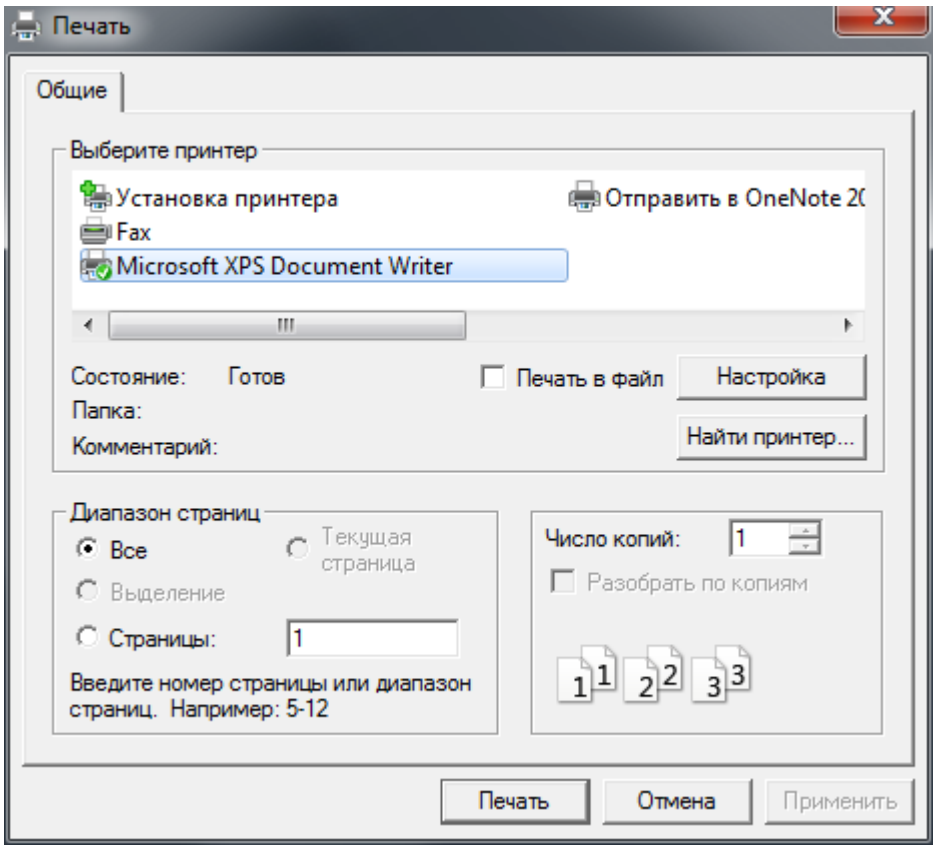


Рисунок 57 – Окно печати документа

В верхнем поле следует выбрать нужный принтер и вывести документ с информацией об аудиторе на печать, нажав кнопку <Ok>, или отменить текущую операцию, нажав кнопку <Отмена>.

После регистрации аудитора становятся доступными другие операции консоли аудитора, в то время как функция регистрации становится недоступной (рисунок 58).

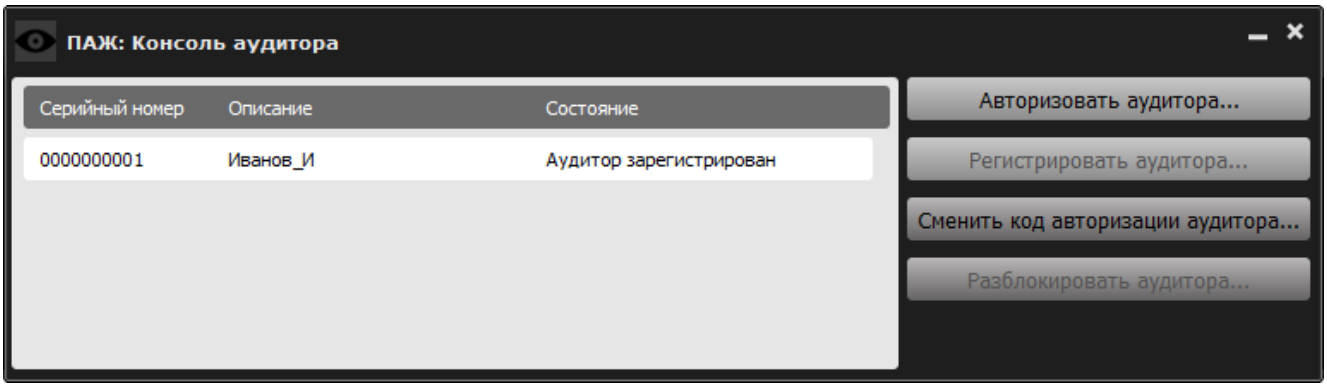


Рисунок 58 – Консоль аудитора с доступными опциями

3.8 Авторизация аудитора

ВНИМАНИЕ! Доступ к чтению файлов журналов приложений, хранящихся на закрытом разделе диска СН «ПАЖ», может получить только аудитор после прохождения процедуры авторизации.

Для авторизации аудитора СН необходимо в консоли аудитора выбрать функцию «Авторизовать аудитора …». После этого на экране появляется окно запроса КА. В поле данного окна необходимо ввести КА и для завершения операции нажать кнопку <Ok>. Для отмены текущей операции следует нажать кнопку <Отмена> (рисунок 59).

В рамках сеанса работы с СН введение КА для авторизации аудитора устройства требуется только один раз. Однако если во время сеанса администратор СН получит доступ к журналу событий, то процедуру авторизации аудитора необходимо провести снова.

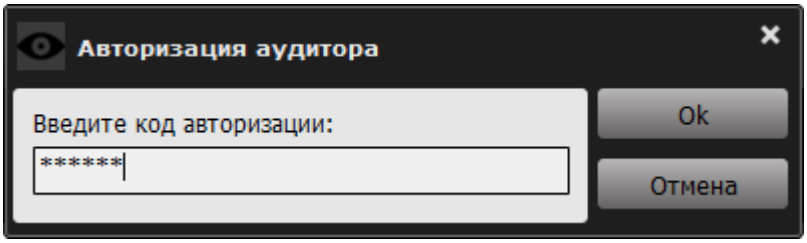


Рисунок 59 – Окно запроса КА аудитора

Если КА введен некорректно, то на экране отображается сообщение об ошибке при выполнении авторизации аудитора (рисунок 60).

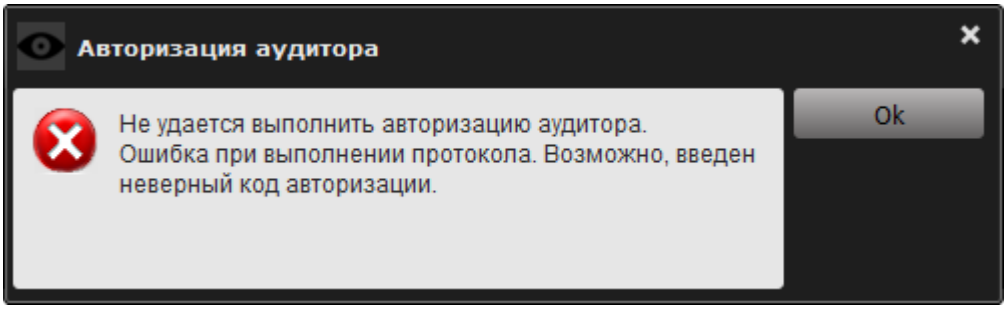


Рисунок 60 – Сообщение об ошибке при авторизации аудитора

В таком случае необходимо нажать кнопку <Ok> и повторить операцию авторизации аудитора еще раз.

Если КА введен корректно, на экране появляется сообщение об успешной авторизации аудитора (рисунок 61).

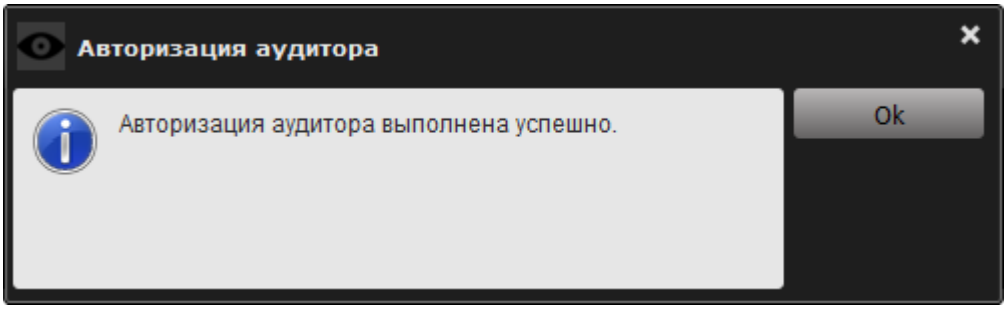


Рисунок 61 – Сообщение об успешной авторизации аудитора

После успешного завершения процедуры авторизации ПО РС монтирует закрытый раздел флеш-диска СН, который становится доступен операционной системе РС в режиме «только чтение». Если аудитор не прошел процедуру авторизации, доступ к закрытому разделу флеш-диска СН не предоставляется.

Экспортированные файлы журналов приложений сохраняются на закрытый раздел диска СН «ПАЖ» в каталог «\DomainName\PCName\C\CatalogName[2)]\JournalFileName.XXX», где DomainName – имя домена, в котором находится РС, PCName – имя РС, С – буква логического диска РС, на котором хранился каталог с файлами журнала приложения, CatalogName - имя каталога, в котором хранились файлы журнала, JournalFileName - имя файла журнала, XXX – символы расширения файла. Маска файла журнала следующая: «FileName ***.XXX», где FileName – имя файла журнала на РС, знак «***» обозначает дату в формате ГГГГ-ММ-ДД ЧЧ-ММ-СС.

Файлы журналов приложений, экспортированные из каталога C:\Windows\System32 на РС с 64-битной ОС Windows, сохраняются на закрытый раздел диска СН «ПАЖ» в каталог «\DomainName\PCName\C\Windows\sysnative\JournalFileName.XXX».

После успешного выполнения процедуры авторизации аудитора все функции консоли аудитора блокируются, а в колонке «Состояние» отображается: «Аудитор авторизован» (рисунок 62).

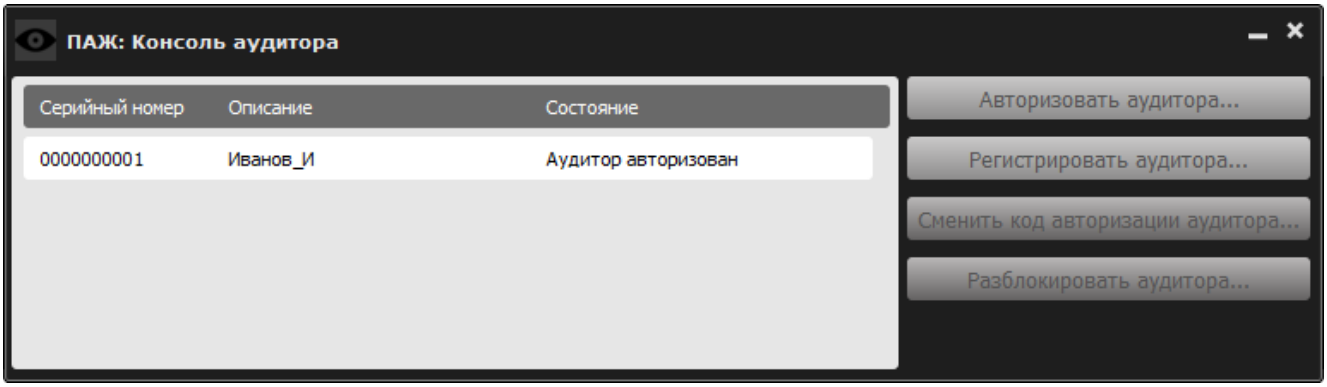


Рисунок 62 – Вид консоли аудитора после выполнения аудитором процедуры авторизации

3.9 Смена КА аудитора

ВНИМАНИЕ! Необходимо регулярно (в соответствии с внутренней политикой безопасности) или экстренно (в случае подозрения о компрометации КА) производить смену КА.

Чтобы сменить КА, в консоли аудитора нужно выбрать функцию «Сменить код авторизации аудитора…». После выбора этой функции на экране появляется окно смены КА аудитора (рисунок 63).

[2)] Каталог CatalogName в свою очередь может включать несколько каталогов.

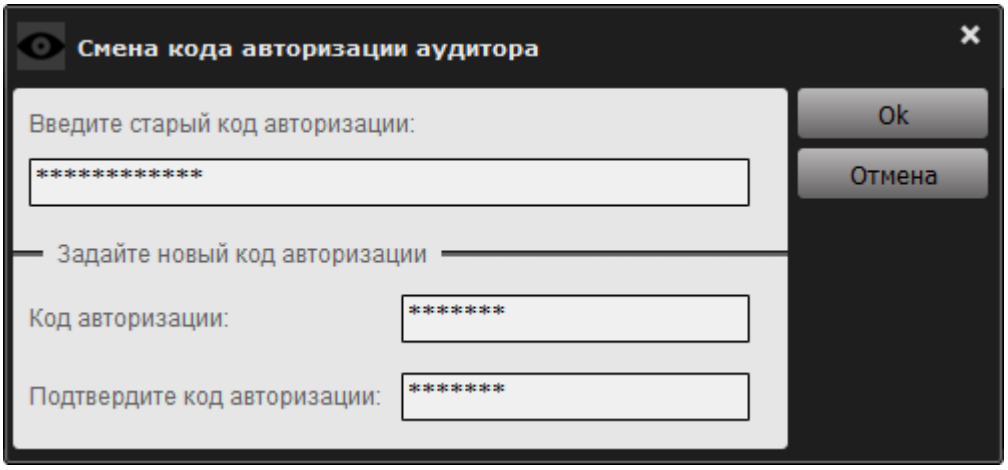


Рисунок 63 – Окно смены КА аудитора

В верхнем поле данного окна нужно ввести старый КА, в нижних полях – новый КА с подтверждением. Нужно нажать кнопку <Ok> для завершения текущей операции и кнопку <Отмена> для ее отмены.

Кнопка <Ok> является недоступной, если:

– не введен старый КА;

– не введен новый КА или его подтверждение.

Если вводимое количество символов нового КА меньше минимального значения, установленного администратором, на экране появится следующее предупреждение (рисунок 64).

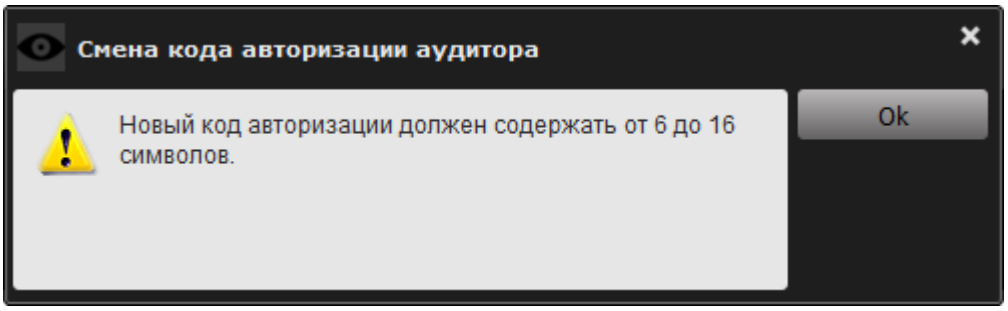


Рисунок 64 – Предупреждение о том, что новый КА должен содержать количество символов, определяемое политикой использования КА

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

Если подтверждение нового КА введено некорректно, на экране отображается предупреждение (рисунок 71).

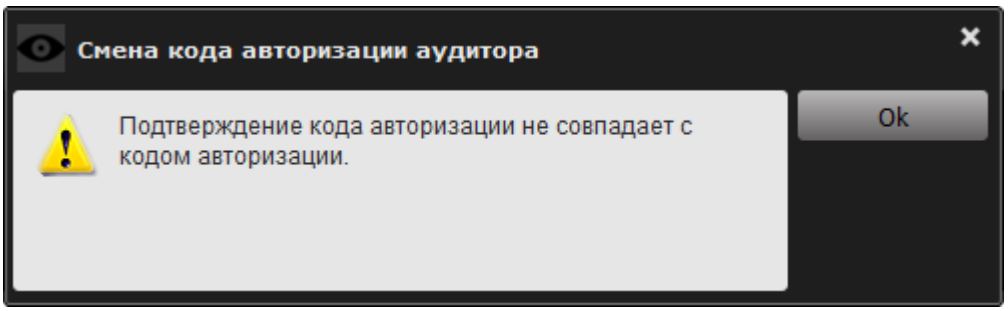


Рисунок 65 – Предупреждение о том, что подтверждение КА не совпадает с КА

В таком случае нужно в данном сообщении нажать кнопку <Ok> и ввести корректный КА.

Если в процессе смены КА введен некорректный старый КА, на экран выводится сообщение об ошибке (рисунок 66).

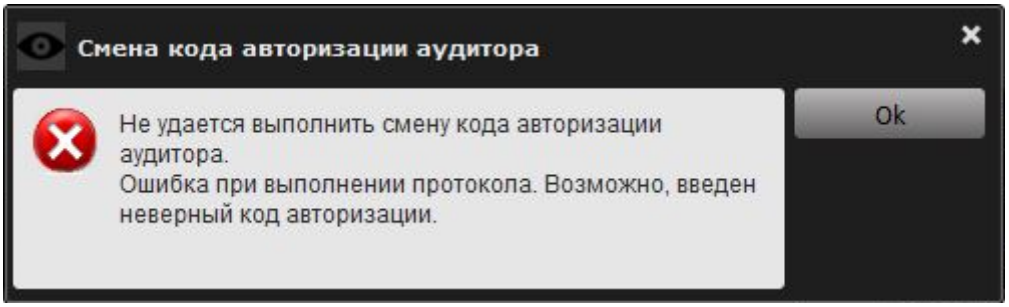


Рисунок 66 – Сообщение об ошибке в ходе смены КА

В этом случае необходимо нажать кнопку <Ok> и ввести корректный КА.

Если процесс смены КА выполнен корректно, на экране появляется сообщение об успешной смене КА (рисунок 67).

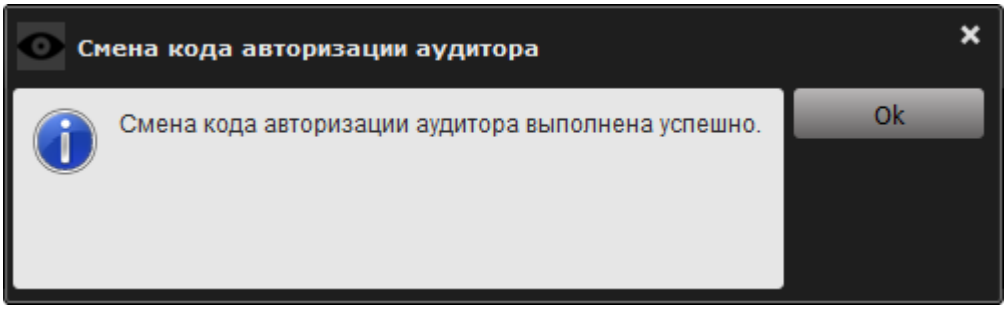


Рисунок 67 – Сообщение об успешной смене КА

3.10 Разблокирование аудитора

В случае нескольких последовательных неудачных попыток ввода КА аудитора (максимально допустимое количество неудачных попыток определяется администратором см. 3.2.3) СН блокируется и на экран выводится соответствующее сообщение (рисунок 68).

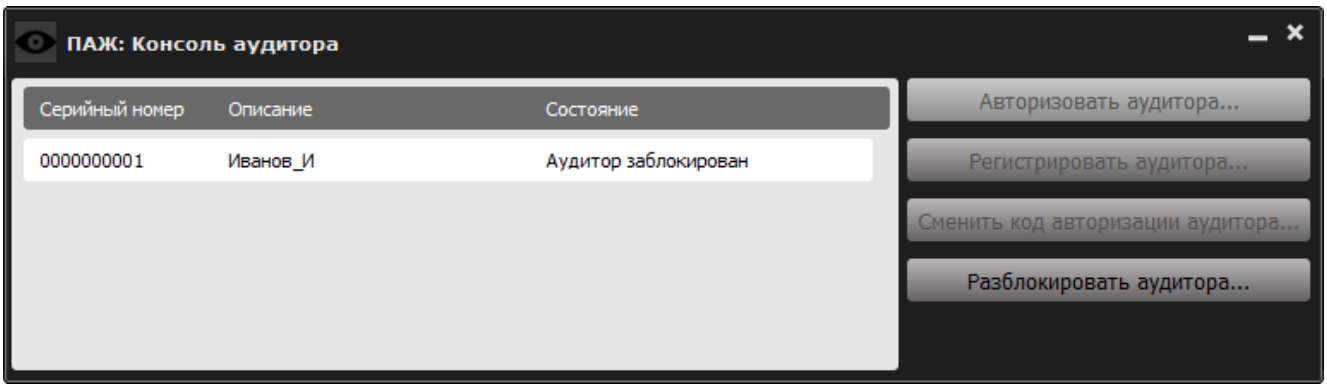


Рисунок 68 – Сообщение о блокировании аудитора

При этом статус СН в главном окне консоли аудитора изменяется на <Аудитор заблокирован> и единственной доступной функцией становится функция разблокирования аудитора (рисунок 69).

Чтобы разблокировать аудитора, в консоли аудитора необходимо нажать кнопку <Разблокировать аудитора…>. После этого на экране появляется окно разблокирования аудитора (рисунок 69).

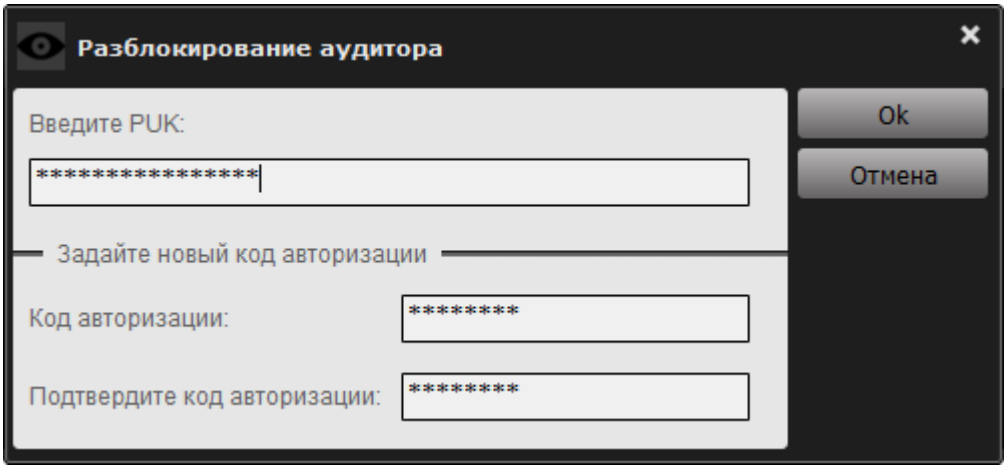


Рисунок 69 – Окно разблокирования аудитора

В верхнем поле данного окна нужно ввести PUK–код, в нижних полях - новый КА аудитора с подтверждением. Для завершения операции следует нажать кнопку <Ok>, для ее отмены – кнопку <Отмена>.

Кнопка <Ok> окна разблокирования аудитора недоступна, если:

– не введен КА; не введено подтверждение КА;

– не введен PUK-код.

Если вводимое количество символов КА меньше минимального значения, установленного администратором, на экране появится следующее предупреждение (рисунок 70).

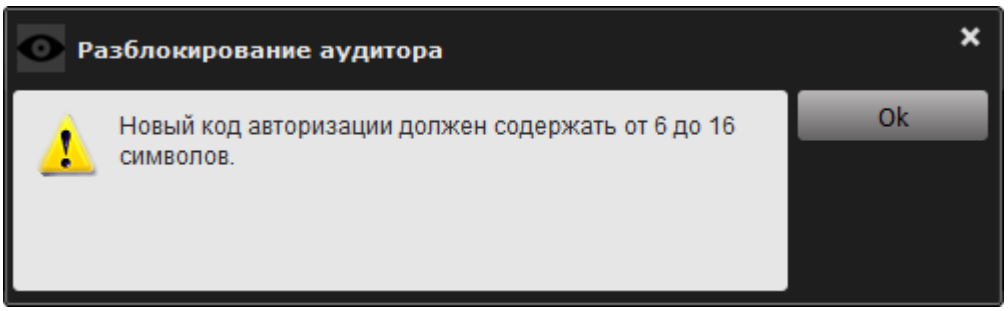


Рисунок 70 – Предупреждение о том, что КА должен содержать от 6 до 16 символов

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

Если подтверждение нового КА введено некорректно, то на экране отображается предупреждение (рисунок 71).

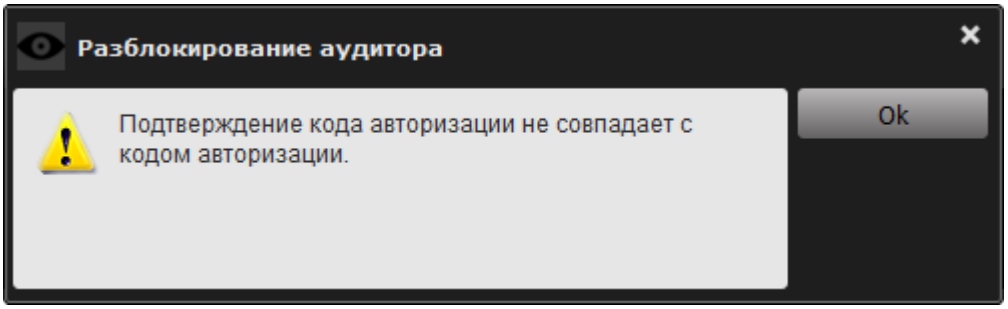


Рисунок 71 – Предупреждение о том, что подтверждение КА не совпадает с КА

В этом случае нужно нажать кнопку <Ok> и ввести корректный КА.

Если введен некорректный PUK-код, на экране появляется оповещение об ошибке в процессе ввода PUK-кода (рисунок 72):

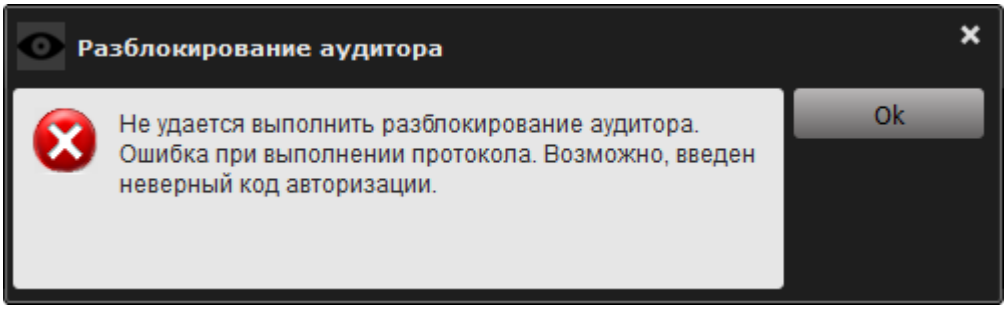


Рисунок 72 – Оповещение об ошибке в процессе ввода PUK–кода

В этом случае необходимо нажать кнопку <Ok> в поле данного окна и ввести корректный PUK-код.

ВНИМАНИЕ! Если значение PUK-кода утеряно, операцию разблокирования аудитора может провести только администратор, выполнив функцию аннулирования регистрации аудитора (см. 3.11).

Если операция разблокирования аудитора выполнена корректно, на экране появляется сообщение об успешно выполненном разблокировании аудитора (рисунок 73).

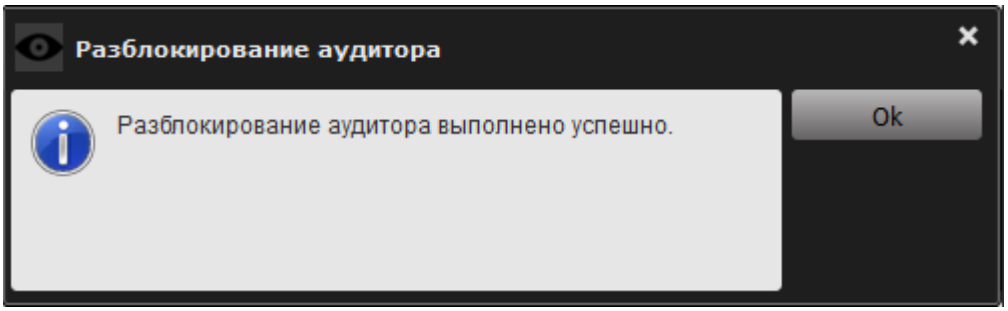


Рисунок 73 – Сообщение об успешном завершении процесса разблокирования аудитора

После нажатия кнопки <Ok> в консоли аудитора вновь будут доступными функции авторизации и смены КА.

3.11 Аннулирование регистрации аудитора СН

Как правило, данная операция выполняется в следующих случаях:

- СН необходимо передать другому аудитору;
- утрачен КА и PUK-код.

Данная операция доступна, если в СН ранее был зарегистрирован аудитор.

Для выполнения операции аннулирования регистрации аудитора следует нажать кнопку <Аннулировать регистрацию аудитора…> в консоли администратора (рисунок 11).

После выбора соответствующей функции (рисунок 11) на экране появляется окно запроса пароля администратора (рисунок 74):

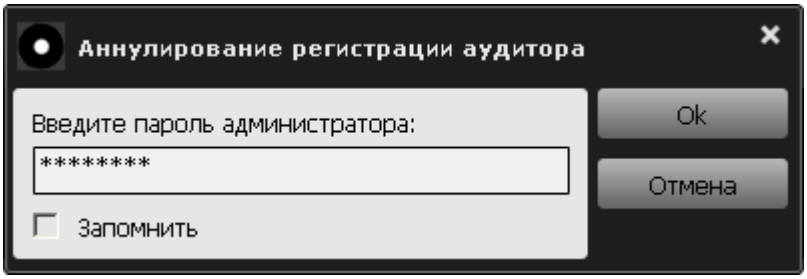


Рисунок 74 – Окно ввода пароля администратора

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 75):

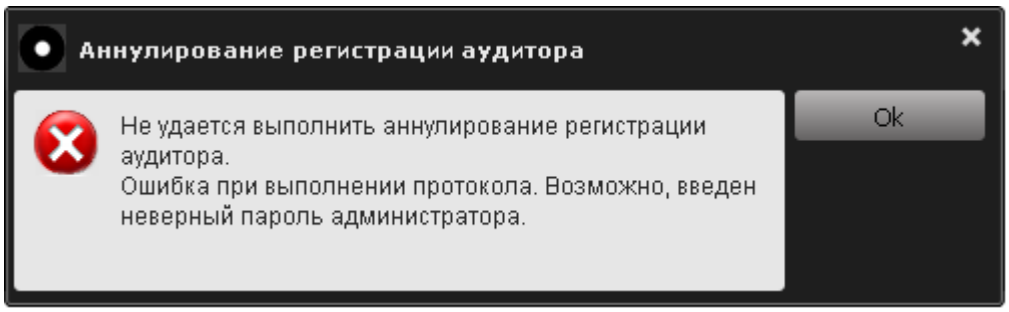


Рисунок 75 – Сообщение о невозможности выполнения аннулирования регистрации аудитора СН

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

После корректного ввода пароля на экране отображается сообщение об успешном аннулировании регистрации аудитора СН (рисунок 76):

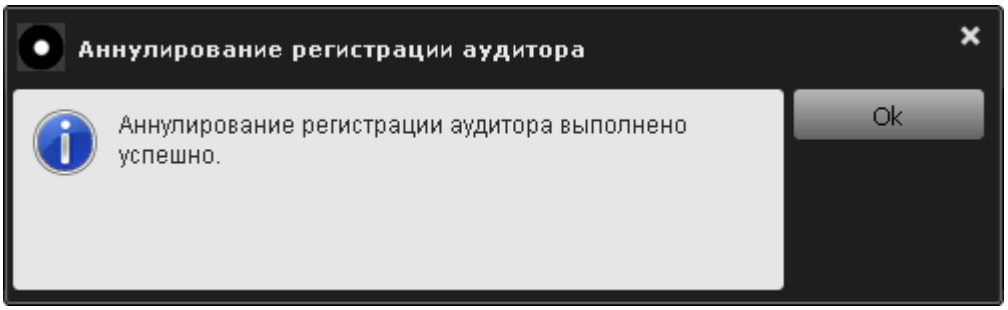


Рисунок 76 – Сообщение об успешном аннулировании регистрации аудитора СН

Для завершения операции необходимо нажать кнопку <Ok>.

ВНИМАНИЕ! Во избежание неполадок с устройством необходимо обеспечить бесперебойную подачу питания на протяжении выполнения данной операции.

3.12 Регистрация пользователя СН

Чтобы зарегистрировать пользователя, необходимо нажать кнопку <Регистрировать пользователя…> (рисунок 5). Далее на экране появляется окно регистрации пользователя (рисунок 77).

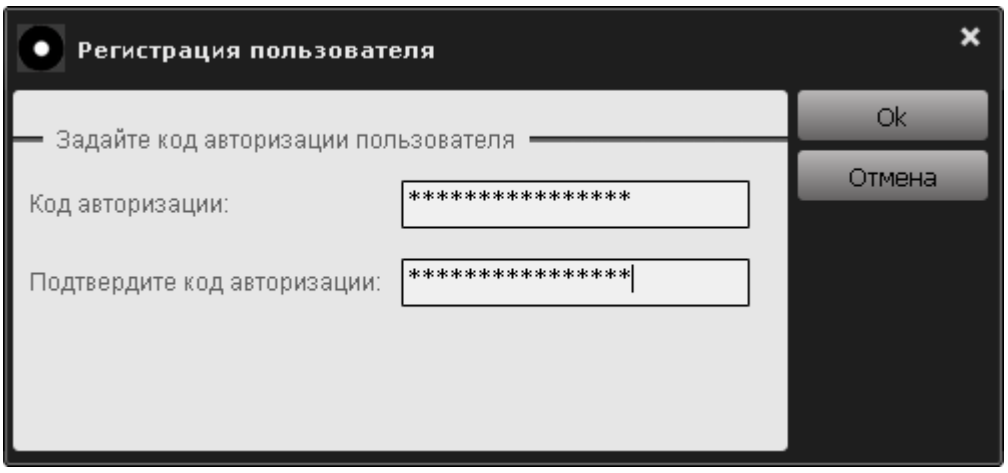


Рисунок 77 – Регистрация пользователя

В появившемся диалоговом окне необходимо установить КА пользователя с подтверждением. Для завершения операции нужно нажать кнопку <Ok>, для отмены операции – кнопку <Отмена>.

КА пользователя представляет собой строку, минимальная длина которой составляет 6 произвольных символов, а максимальная длина – 16 произвольных символов.

В процессе авторизации пользователя формируется PUK-код (16 цифр), необходимый для восстановления возможности экспортирования файлов журналов приложений на закрытый раздел диска СН «ПАЖ» при блокировании пользователя (в случае превышения порога неудачных попыток авторизации).

Кнопка <Ok> окна регистрации недоступна, если не заданы значения в полях <Код авторизации> или <Подтвердите код авторизации>.

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить КА и PUK-код, знание которых позволяет экспортировать файлы журналов приложений на закрытый раздел диска СН «ПАЖ». Важно помнить о необходимости сохранения этих данных недоступными третьим лицам!

В случае утраты КА и PUK-кода СН необходимо выполнить процедуру аннулирования регистрации пользователя СН, которая приведет к стиранию параметров аутентификации пользователя (КА и PUK-код СН).

Если вводимое количество символов КА пользователя меньше установленного минимального значения (6 символов), на экране появится следующее предупреждение (рисунок 78).

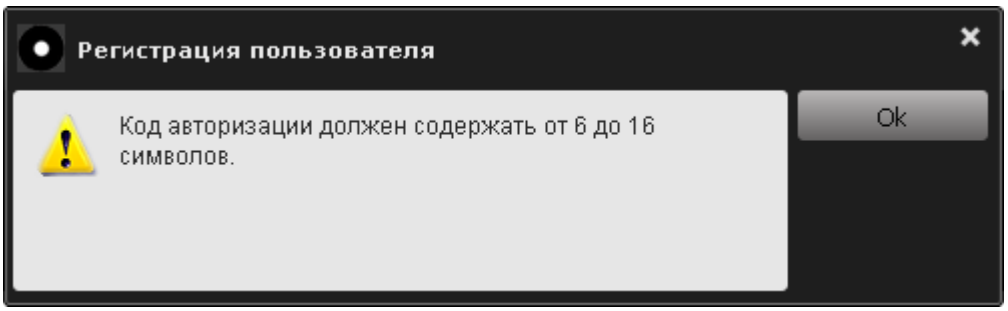


Рисунок 78 – Предупреждение о том, что КА пользователя должен содержать от 6 до 16 символов

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

Если пароль подтвержден неверно, после нажатия кнопки <Ok> на экран выводится соответствующее предупреждение (рисунок 79).

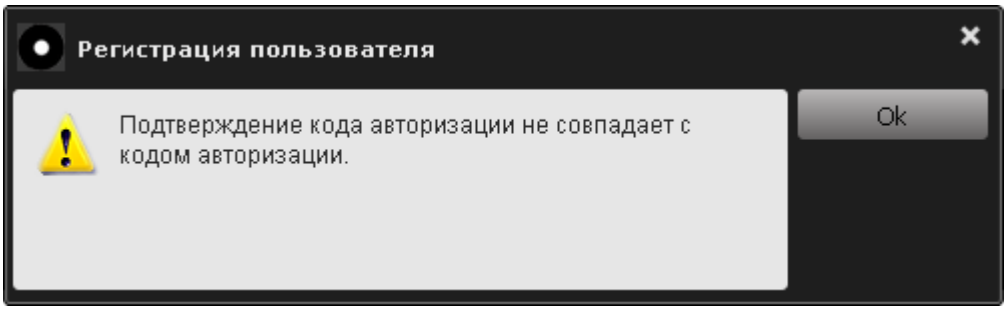


Рисунок 79 – Предупреждение об ошибке при подтверждении КА пользователя

В этом случае следует ввести корректное подтверждение пароля в поле <Подтвердите код авторизации> (рисунок 79) и нажать кнопку <Ok>.

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

Далее на экране появляется окно для ввода пароля администратора. Необходимо ввести пароль администратора и нажать кнопку <Ok> (рисунок 80).

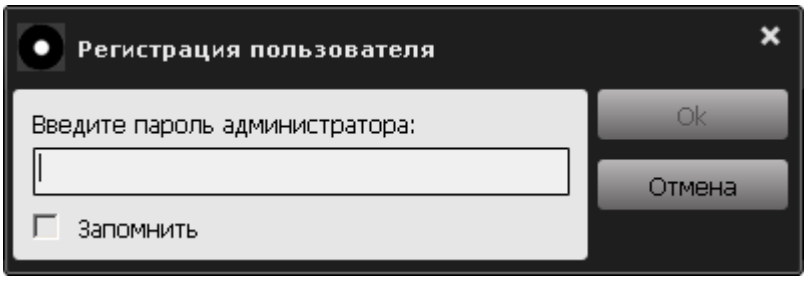


Рисунок 80 – Ввод пароля администратора

По нажатии кнопки <Ok> (рисунок 80) на экран выводится сообщение об успешной регистрации пользователя (рисунок 81).

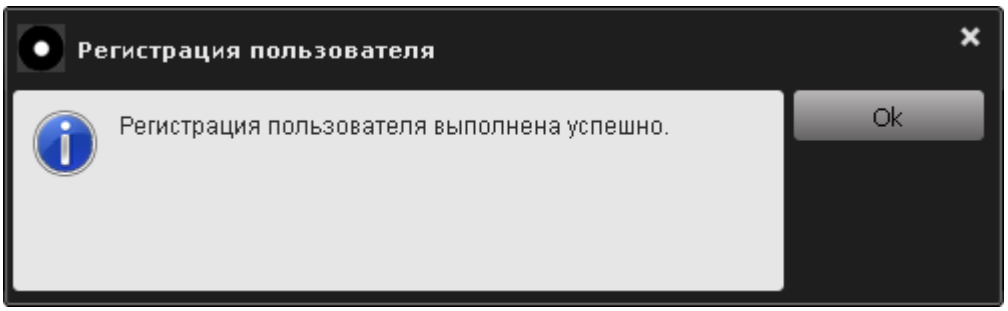


Рисунок 81 – Сообщение об успешной регистрации пользователя

По нажатию кнопки <Ok> (рисунок 81) на экране отображается сообщение с серийным номером, именем СН, КА и PUK-кодом пользователя (рисунок 82). Имеется возможность вывода этой информации на печать посредством нажатия кнопки <Печать…>.

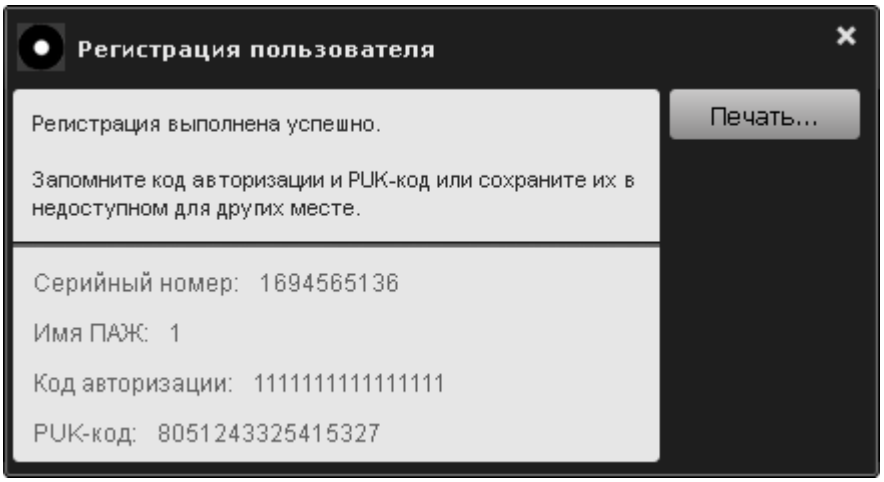


Рисунок 82 – Информация о пользователе

По нажатию кнопки <Печать…> на экране появляется окно печати документа (рисунок 56).

В верхнем поле следует выбрать нужный принтер и вывести документ с информацией о пользователе на печать, нажав кнопку <Ok>, или отменить текущую операцию, нажав кнопку <Отмена>.

После регистрации пользователя в графе «Состояние» консоли пользователя отображается: «Пользователь зарегистрирован»:

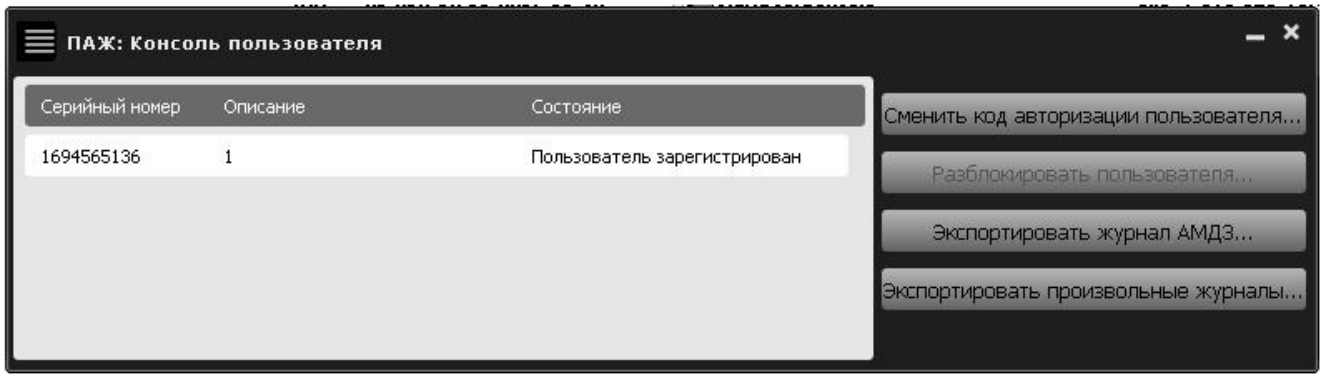


Рисунок 83 – Консоль пользователя (в СН зарегистрирован пользователь)

3.13 Смена КА пользователя

ВНИМАНИЕ! Необходимо регулярно (в соответствии с внутренней политикой безопасности) или экстренно (в случае подозрения о компрометации КА) производить смену КА.

Чтобы сменить КА, в консоли пользователя (рисунок 83) нужно выбрать функцию «Сменить код авторизации пользователя…». После выбора этой функции на экране появляется окно смены КА пользователя (рисунок 84).

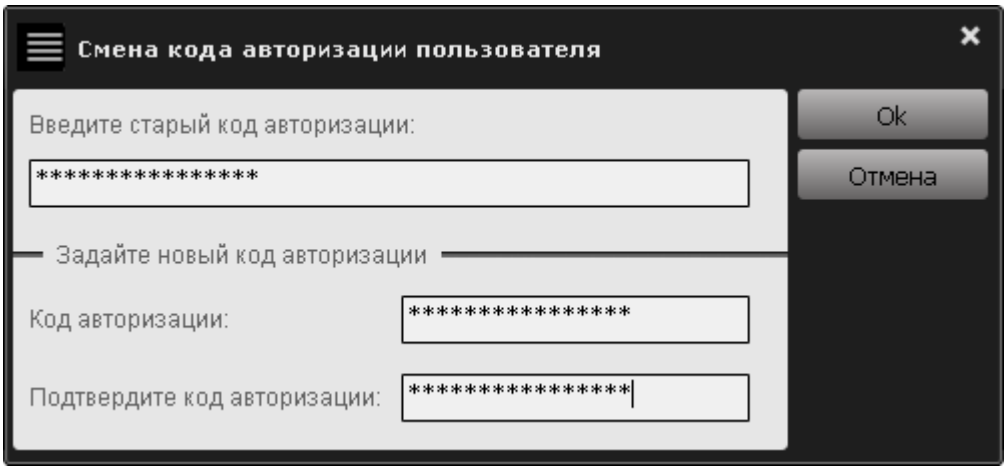


Рисунок 84 – Смена КА пользователя

В верхнем поле данного окна нужно ввести старый КА, в нижних полях – новый КА с подтверждением. Нужно нажать кнопку <Ok> для завершения текущей операции и кнопку <Отмена> для ее отмены.

Кнопка <Ok> является недоступной, если:

– не введен старый КА;

– не введен новый КА или его подтверждение.

Если вводимое количество символов нового КА меньше минимального значения, установленного администратором, на экране появится следующее предупреждение (рисунок 85).

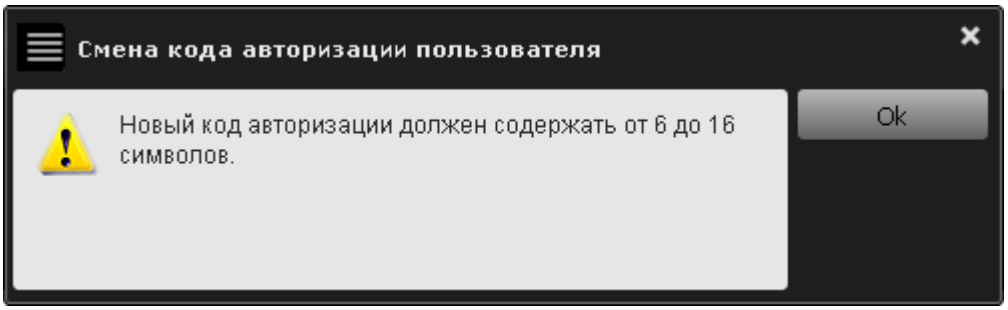


Рисунок 85 – Предупреждение о том, что новый КА должен содержать количество символов, определяемое политикой использования КА

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

Если подтверждение нового КА введено некорректно, на экране отображается предупреждение (рисунок 86).

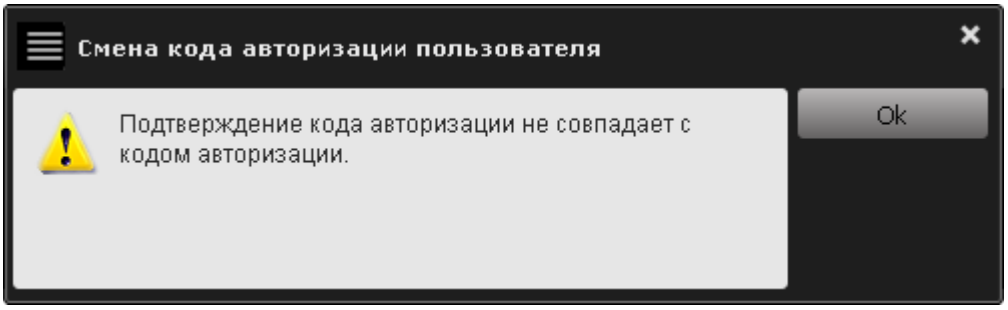


Рисунок 86 – Предупреждение о том, что подтверждение КА не совпадает с КА

В таком случае нужно в данном сообщении нажать кнопку <Ok> и ввести корректный КА.

Если в процессе смены КА введен некорректный старый КА, на экран выводится сообщение об ошибке при вводе КА (рисунок 87).

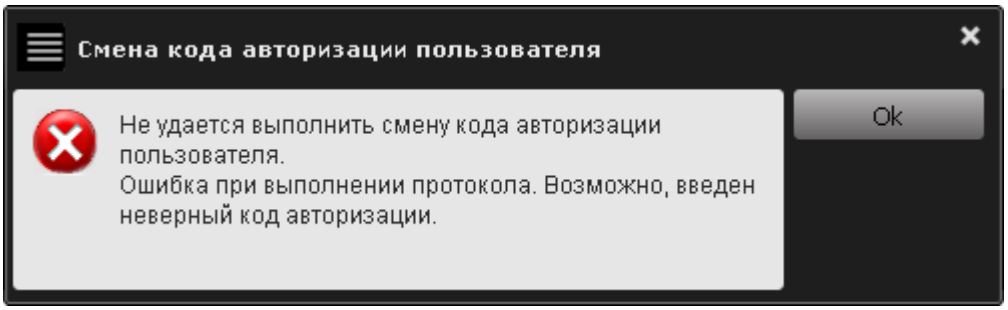


Рисунок 87 – Сообщение об ошибке в ходе смены КА

В этом случае необходимо нажать кнопку <Ok> и ввести корректный КА.

Если процесс смены КА выполнен корректно, на экране появляется сообщение об успешной смене КА (рисунок 88).

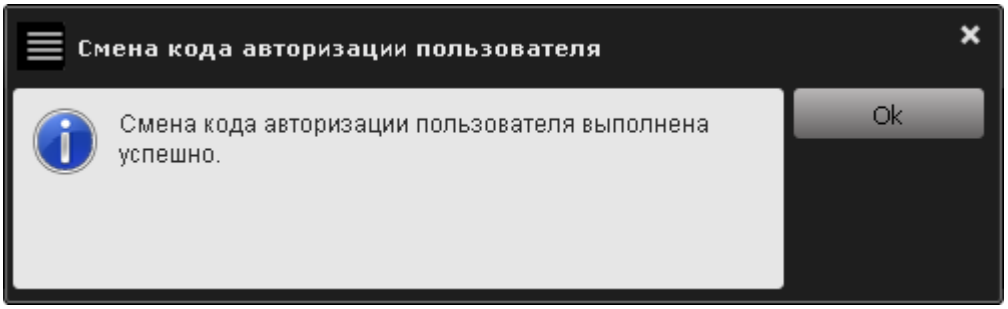


Рисунок 88 – Сообщение об успешной смене КА

3.14 Разблокирование пользователя

В случае нескольких последовательных неудачных попыток ввода КА пользователя (максимально допустимое количество неудачных попыток определяется администратором см. 3.2.3) СН блокируется и на экран выводится соответствующее сообщение (рисунок 89).

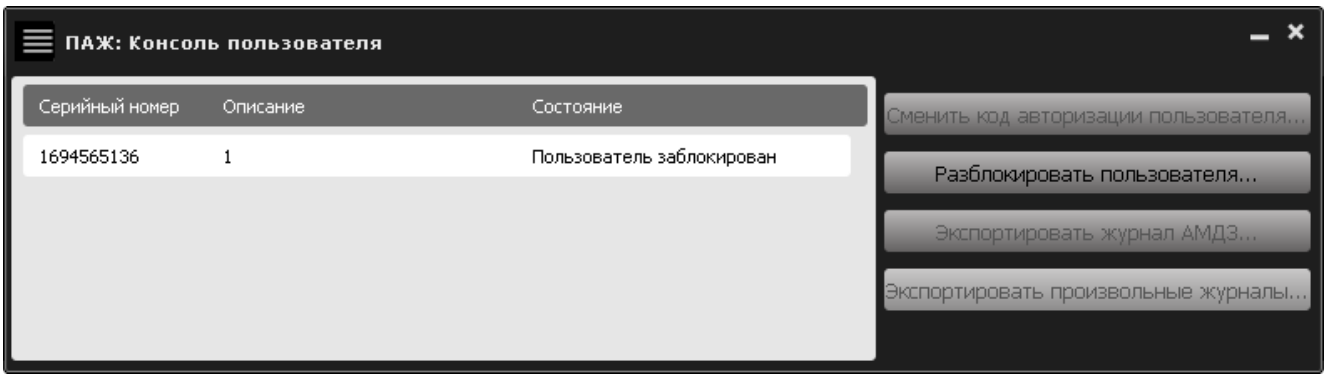


Рисунок 89 – Сообщение о блокировании пользователя

При этом статус СН в главном окне консоли пользователя изменяется на <Пользователь заблокирован> и единственной доступной функцией становится функция разблокирования пользователя (рисунок 89).

Чтобы разблокировать пользователя, в консоли пользователя необходимо нажать кнопку <Разблокировать пользователя…>. После этого на экране появляется окно разблокирования пользователя (рисунок 90).

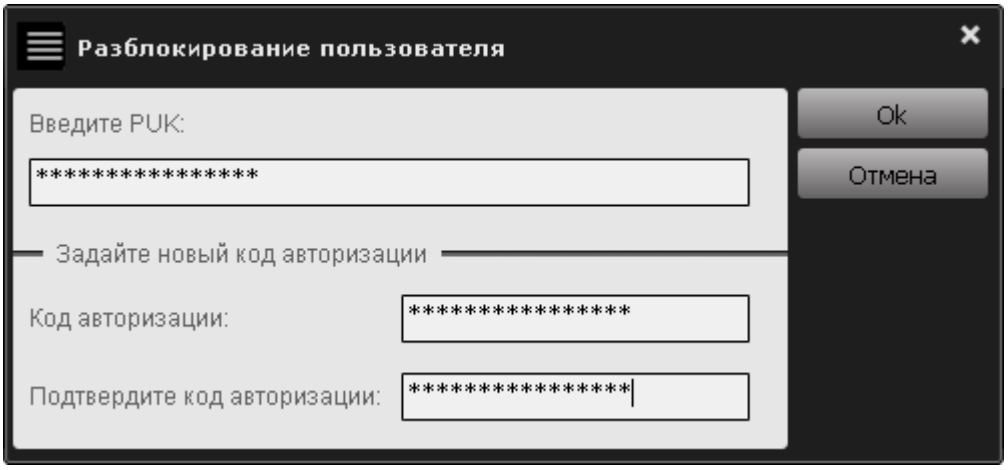


Рисунок 90 – Окно разблокирования пользователя

В верхнем поле данного окна нужно ввести PUK–код, в нижних полях - новый КА пользователя с подтверждением. Для завершения операции следует нажать кнопку <Ok>, для ее отмены – кнопку <Отмена>.

Кнопка <Ok> окна разблокирования пользователя недоступна, если:

– не введен КА;

– не введено подтверждение КА;

– не введен PUK-код.

Если вводимое количество символов КА меньше минимального значения, установленного администратором, на экране появится следующее предупреждение (рисунок 91).

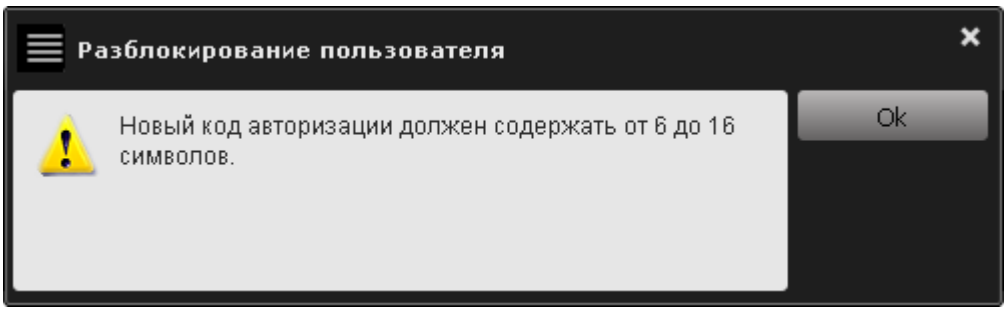


Рисунок 91 – Предупреждение о том, что КА должен содержать от 6 до 16 символов

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

Если подтверждение нового КА введено некорректно, то на экране отображается предупреждение (рисунок 92).

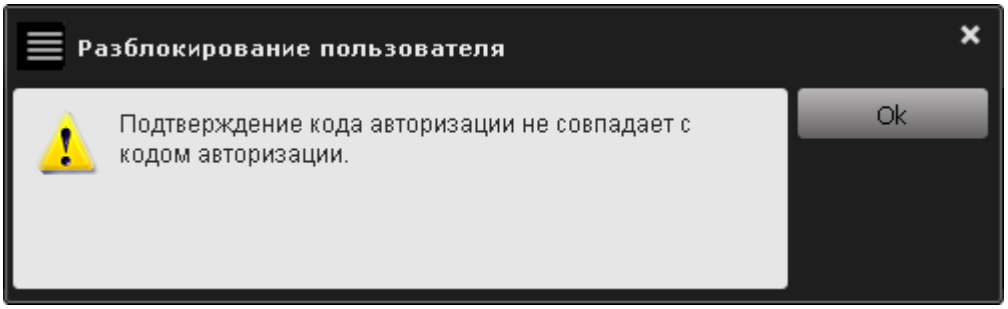


Рисунок 92 – Предупреждение о том, что подтверждение КА не совпадает с КА

В этом случае нужно нажать кнопку <Ok> и ввести корректный КА.

Если введен некорректный PUK-код, на экране появляется оповещение об ошибке в процессе ввода PUK-кода (рисунок 93):

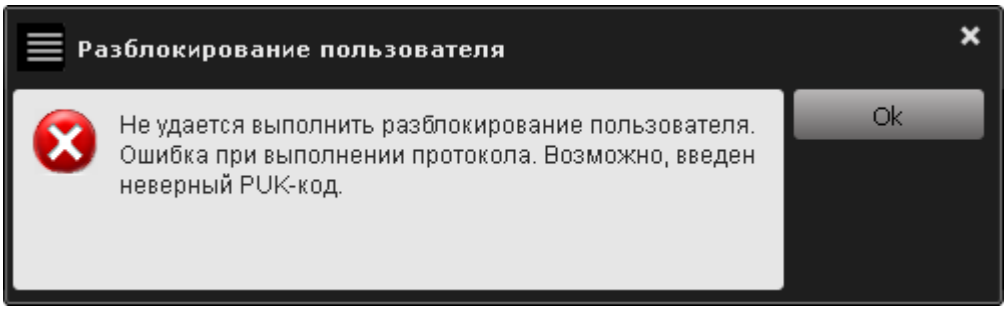


Рисунок 93 – Оповещение об ошибке в процессе ввода PUK–кода

В этом случае необходимо нажать кнопку <Ok> в поле данного окна и ввести корректный PUK-код.

ВНИМАНИЕ! Если значение PUK-кода утеряно, операцию разблокирования пользователя может провести только администратор, выполнив функцию аннулирования регистрации пользователя (см. 3.15).

Если операция разблокирования пользователя выполнена корректно, на экране появляется сообщение об успешно выполненном разблокировании пользователя (рисунок 94).

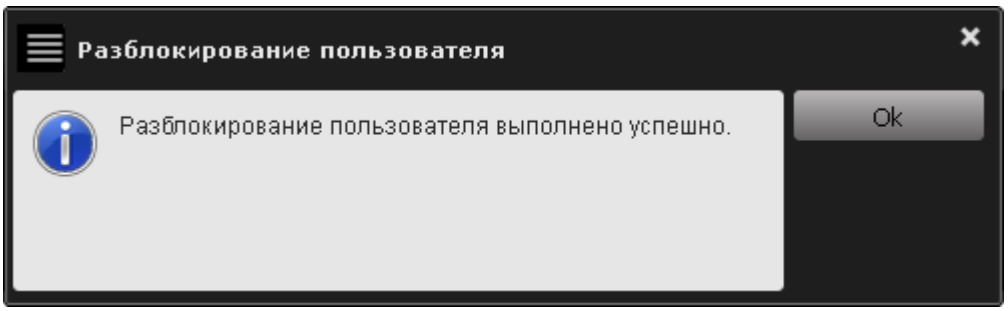


Рисунок 94 – Сообщение об успешном завершении процесса разблокирования пользователя

После нажатия кнопки <Ok> в консоли пользователя вновь будут доступными функции экспорта файлов журналов приложений и смены КА.

3.15 Аннулирование регистрации пользователя

Как правило, данная операция выполняется в следующих случаях:

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

Данная операция доступна, если в СН ранее был зарегистрирован пользователь.

Для выполнения операции аннулирования регистрации пользователя следует нажать кнопку <Аннулировать регистрацию пользователя…> в консоли администратора (рисунок 11).

После выбора соответствующей функции (рисунок 11) на экране появляется окно запроса пароля администратора (рисунок 95):

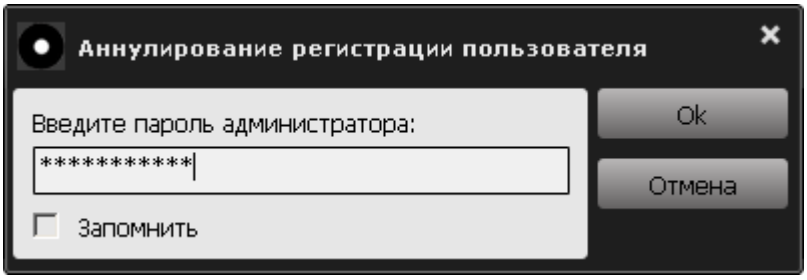


Рисунок 95 – Окно ввода пароля администратора

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 96):

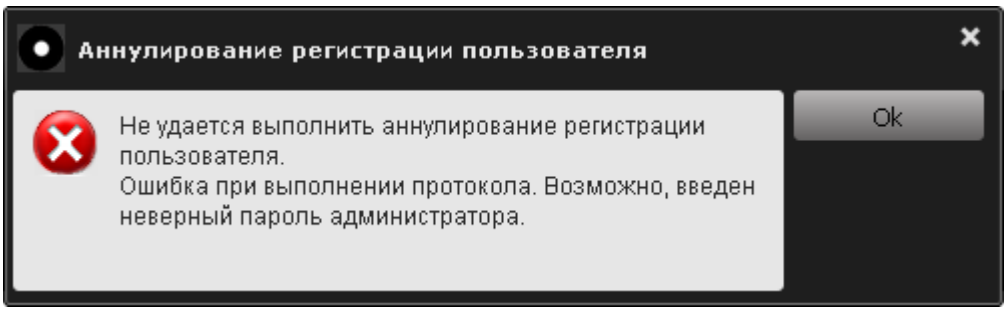


Рисунок 96 – Сообщение о невозможности выполнения аннулирования регистрации пользователя СН

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 97):

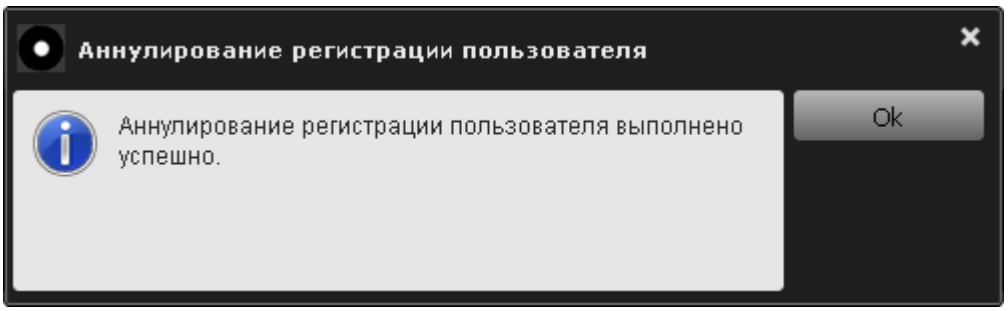


Рисунок 97 – Сообщение об успешном аннулировании регистрации пользователя СН

Для завершения операции необходимо нажать кнопку <Ok>.

ВНИМАНИЕ! Во избежание неполадок с устройством необходимо обеспечить бесперебойную подачу питания на протяжении выполнения данной операции.

3.16 Завершение работы ПАК «ПАЖ»

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 консолей.

Чтобы завершить работу с консолью администратора ПАК «ПАЖ», необходимо нажать правой кнопкой мыши на значок СН в трее (рисунок 3) и выбрать в появившемся окне пункт «Выход» (рисунок 4). После этого на экране появляется следующее сообщение (рисунок 98):

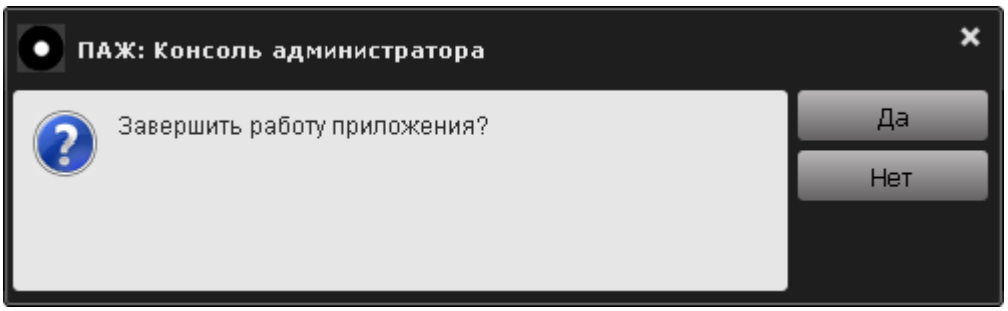


Рисунок 98 – Завершение работы консоли администратора

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

Чтобы завершить работу с консолью аудитора ПАК «ПАЖ», необходимо нажать правой кнопкой мыши на значок СН в трее (рисунок 3) и выбрать в появившемся окне пункт «Выход» (рисунок 4). После этого на экране появляется следующее сообщение (рисунок 99):

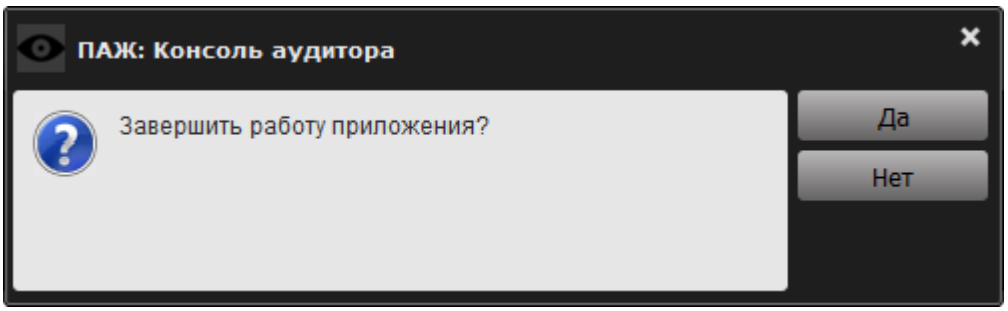


Рисунок 99 – Завершение работы консоли аудитора

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

Чтобы завершить работу с консолью пользователя ПАК «ПАЖ», необходимо нажать правой кнопкой мыши на значок СН в трее выбрать в появившемся окне пункт «Выход». После этого на экране появляется следующее сообщение (рисунок 100):

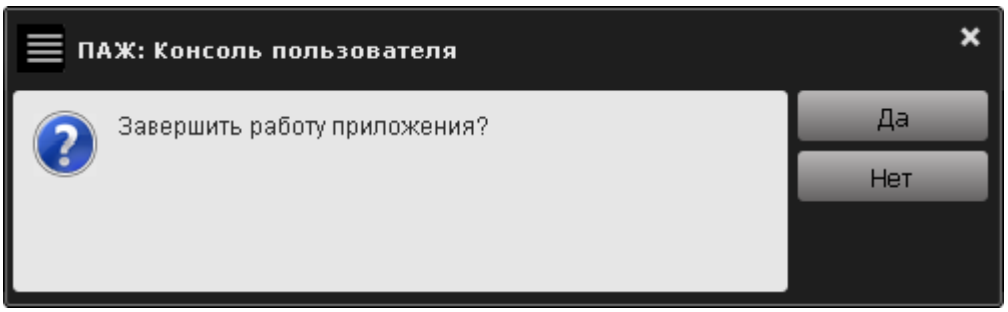


Рисунок 100 – Завершение работы консоли пользователя

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

4 Сценарии работы ПАК «ПАЖ»

4.1 Общие сведения

ПАК «ПАЖ» может использоваться в рамках реализации трех типов сценариев работы:

1) экспортирование файлов журналов приложений на закрытый диск ПАК «ПАЖ» с целью защищенного хранения и переноса на другие рабочие станции (например, для дальнейшего анализа);

2) экспортирование файлов журнала комплекса «Аккорд-АМДЗ» на закрытый диск ПАК «ПАЖ» с целью защищенного хранения и переноса на другие рабочие станции (например, для дальнейшего анализа);

3) интегрирование специальной библиотеки из состава ПО ПАК «ПАЖ» в ПО стороннего приложения с целью записи и защищенного хранения файлов журнала этого приложения на закрытом разделе диска ПАК «ПАЖ».

Процедуру экспорта[3)] журналов сторонних приложений на закрытый раздел диска СН «ПАЖ» выполняет пользователь СН «ПАЖ». При этом пользователь СН «ПАЖ» должен обладать правами доступа к каталогу, в котором хранятся файлы журнала.

Если в СН «ПАЖ» не зарегистрирован пользователь, то процедуру экспорта файлов журналов сторонних приложений может выполнить любое лицо, обладающее доступом к устройству и каталогу, в котором хранятся файлы журнала, без авторизации.

Процедуру экспорта журналов комплекса «Аккорд-АМДЗ» на закрытый раздел диска СН «ПАЖ» выполняет пользователь СН «ПАЖ» при совместном участии (авторизации) администратора ПАК «Аккорд».

Если в СН «ПАЖ» не зарегистрирован пользователь, то процедуру экспорта файлов журналов комплекса «Аккорд-АМДЗ» может выполнить любое лицо, обладающее доступом к устройству, без авторизации при совместном участии администратора ПАК «Аккорд».

Максимальный размер имени экспортируемого файла журнала составляет 230 символов (включая символы расширения).

---

3) Во время выполнения процедуры экспорта файлов журналов в ОС автоматически монтируется съемный диск, на котором расположен файл «requestshj.dat». Монтирование диска может сопровождаться отображением на экране компьютера окна, соответствующего диску. Это окно можно закрыть, никаких дополнительных действий предпринимать не нужно.

4.2 Экспортирование файлов журналов событий различных приложений

Для выполнения процедуры экспорта файлов журналов на закрытый раздел диска СН «ПАЖ» в рамках первого сценария работы СН необходимо запустить консоль пользователя (исполняемый файл startUserConsole.exe или исполняемый файл userConsole.exe в папке hardJournal).

Далее в консоли пользователя необходимо нажать кнопку <Экспортировать произвольные журналы…> (рисунок 83).

Если процедуру экспорта файлов выполняет пользователь СН «ПАЖ», то по нажатии кнопки <Экспортировать произвольные журналы…> на экране появляется окно ввода КА пользователя (рисунок 101).

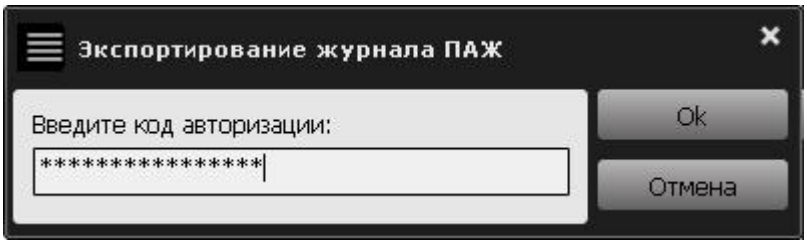


Рисунок 101 – Окно ввода КА пользователя

Необходимо ввести КА пользователя и нажать кнопку <Ok>.

Далее на экране появляется окно выбора файлов журналов (рисунок 102), в котором следует выбрать необходимый файл (или файлы) и нажать кнопку <Открыть>.

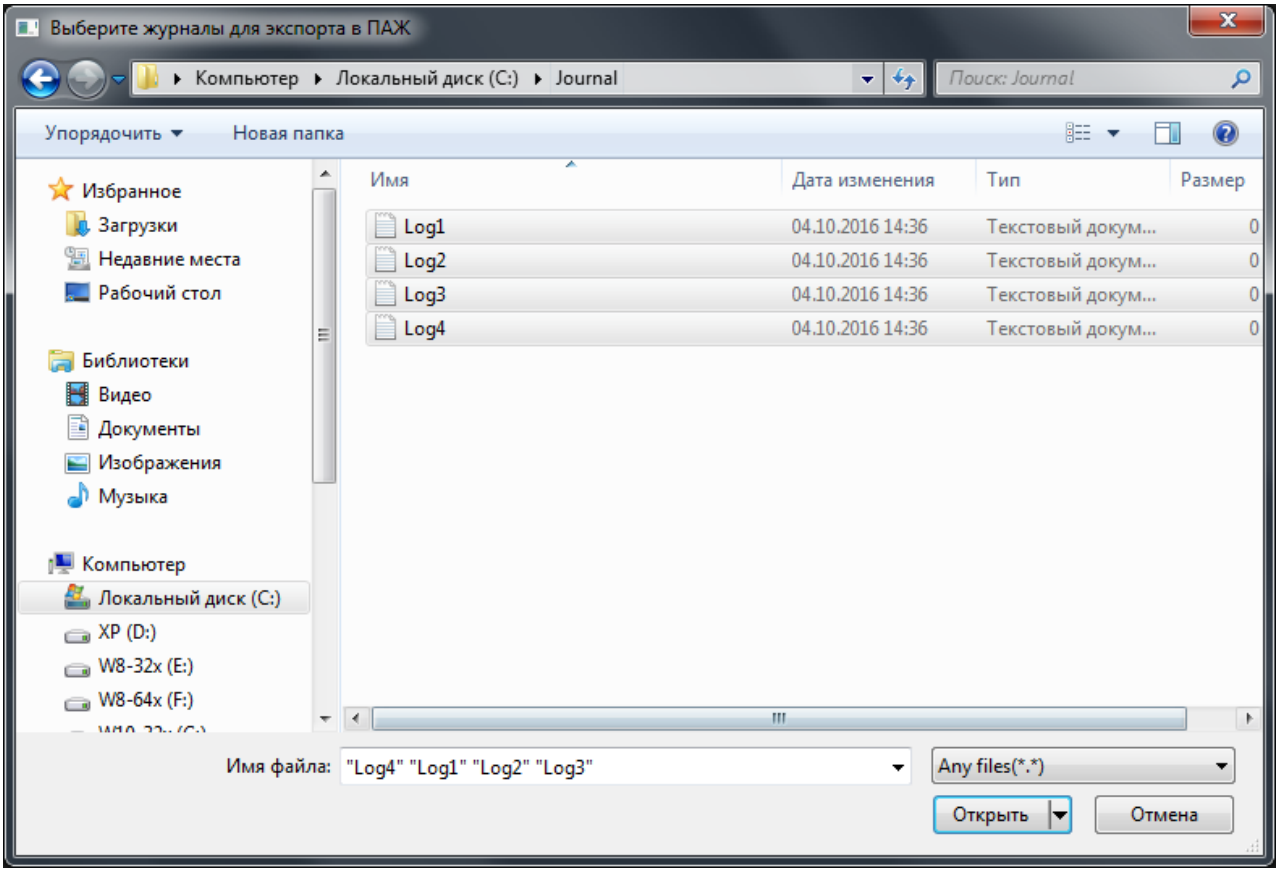


Рисунок 102 – Выбор файлов журналов сторонних приложений

В случае успешного завершения процедуры экспорта журналов сторонних приложений на закрытый диск СН «ПАЖ» на экране появляется сообщение:

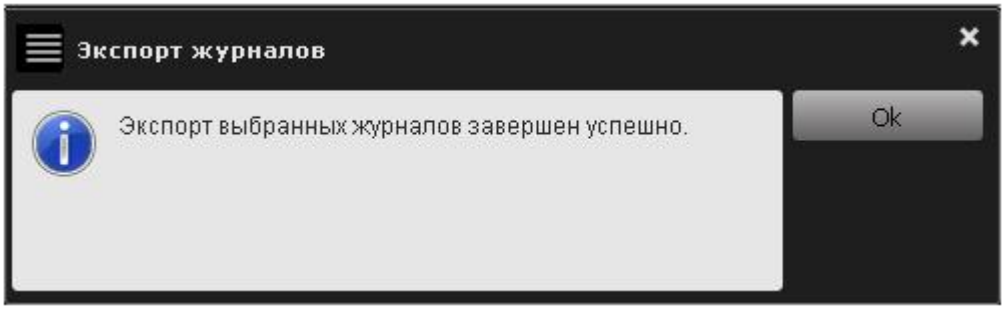


Рисунок 103 – Сообщение об успешном завершении процедуры экспорта журналов на закрытый диск СН «ПАЖ»

При экспортировании файлов журналов на закрытый раздел диска СН «ПАЖ» из директории C:\Windows\System32 РС с 64-битной ОС Windows необходимо в окне выбора файлов журналов (рисунок 102) указать директорию C:\Windows, затем в строке «Имя файла» ввести «sysnative» и нажать кнопку <Открыть>. Далее в появившемся на экране окне выбрать необходимые файлы журналов приложений[4)].

4.3 Экспортирование файлов журнала комплекса «Аккорд-АМДЗ»[5)]

ВНИМАНИЕ! При использовании ПАК «ПАЖ» в рамках второго сценария работы необходимо на РС установить и активировать ПАК «Аккорд-Win32» для 32-битных РС или ПАК «Аккорд-Win64» для 64-битных РС. При этом в качестве идентификатора для администратора «Аккорд-АМДЗ» должен быть назначен ТМ-идентификатор.

Для выполнения процедуры экспорта файлов журналов комплекса «Аккорд-АМДЗ» на закрытый раздел диска СН «ПАЖ» в рамках второго сценария работы СН необходимо запустить консоль пользователя (исполняемый файл startUserConsole.exe или исполняемый файл userConsole.exe в папке hardJournal, рисунок 83).

Далее в консоли пользователя необходимо нажать кнопку <Экспортировать журнал АМДЗ…> (рисунок 83).

Если процедуру экспорта файлов выполняет пользователь СН «ПАЖ», то по нажатии кнопки <Экспортировать журнал АМДЗ…> на экране

[4)] Описанная последовательность действий обусловлена особенностями работы 32-разрядных приложений в 64-разрядных ОС Windows.

[5)] Экспортирование файлов журналов комплекса «Аккорд-АМДЗ» может быть выполнено, если на РС установлен контроллер семейства «Аккорд-5МХ/5.5» («Аккорд-5МХ», «Аккорд-5.5», «Аккорд-5МР», «Аккорд-5.5Е») или контроллер семейства «Аккорд-GX» («Аккорд-GX», «Аккорд-GXM», «Аккорд-GXMH», «Аккорд-GXM.2») с драйвером версии 4.3.3.0 и выше в составе ПАК «Аккорд-Win32»/«Аккорд-Win64» с СПО версии 4.0.10.51 и выше.

появляется окно вода КА пользователя (рисунок 101). Необходимо ввести КА пользователя и нажать кнопку <Ok>.

Далее на запрос идентификатора администратора ПАК «Аккорд» следует предъявить идентификатор (рисунок 104).

Рисунок 104 – Требование предъявить идентификатор администратора ПАК «Аккорд»

В появившемся далее на экране окне нужно ввести пароль администратора ПАК «Аккорд» (рисунок 105).

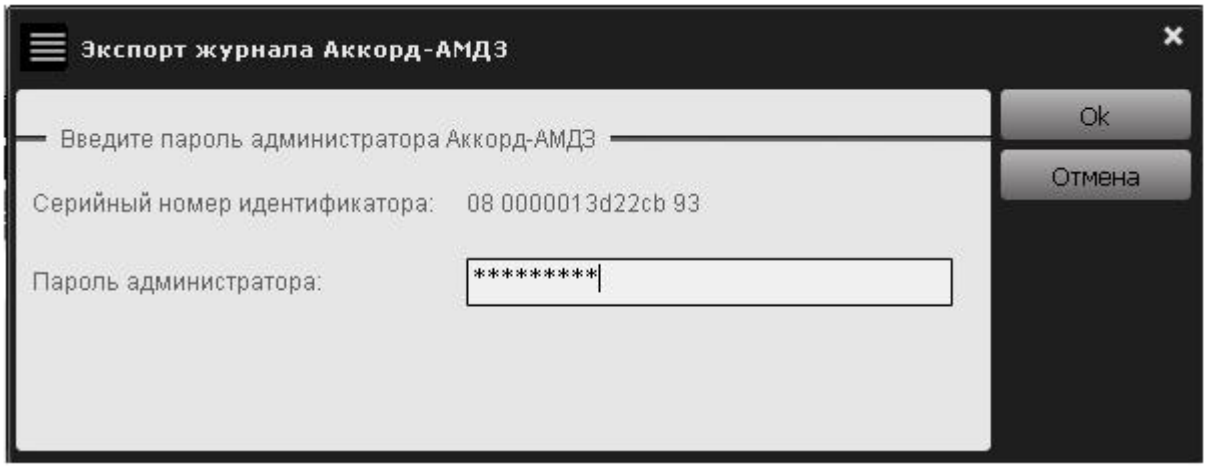


Рисунок 105 – Аутентификация администратора ПАК «Аккорд»

В случае успешного завершения процедуры экспорта журнала комплекса «Аккорд-АМДЗ» на закрытый диск СН «ПАЖ» на экране появляется сообщение:

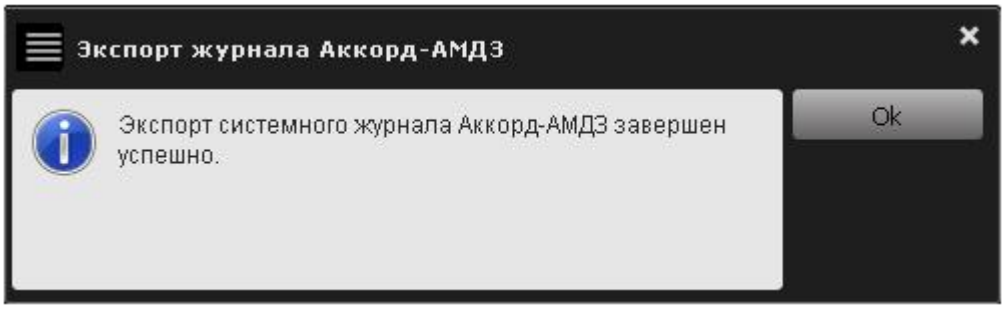


Рисунок 106 – Сообщение об успешном завершении процедуры экспорта журнала комплекса «Аккорд-АМДЗ» на закрытый диск СН «ПАЖ»

4.4 Интегрирование библиотеки в ПО стороннего приложения

В рамках третьего сценария работы ПАК «ПАЖ» выполняется интегрирование специальной API библиотеки hardJournal.dll, входящей в состав ПО ПАК «ПАЖ», в ПО стороннего приложения с целью записи и защищенного хранения файлов журнала этого приложения на закрытом разделе диска ПАК «ПАЖ».

API библиотека hardJournal.dll реализует выполнение следующих функций:

- инициализация СН «ПАЖ»;
- добавление записей в существующие файлы журналов приложений.

5 Перечень принятых сокращений и обозначений

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

6 Техническая поддержка

В случае необходимости консультации АО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 17-00 (по московскому времени) обращаться по телефонам: +7 (495) 994-49-96, +7 (495) 994-49-97, +7 (926) 762-17-72 или по адресам электронной почты: okbsapr@okbsapr.ru, secret@okbsapr.ru. Наш адрес в Интернете http://www.okbsapr.ru/.