ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс
«Идеальный токен»

Руководство администратора

11443195.4012.063 91

Листов 22

Москва
2014

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса «Идеальный токен» (далее по тексту – ПАК «Идеальный токен», или «Идеальный токен»), предназначенного для хранения абстрактных объектов данных[1] (далее – АОД, или пользовательские данные, или данные) в энергонезависимой памяти (ЭНП) аппаратного компонента комплекса и предоставляющего возможность применения этого компонента исключительно в выделенных сегментах сети, разрешенных владельцем.

ПАК «Идеальный токен» предназначен как для корпоративного, так и для личного использования.

При корпоративном использовании функции Администратора ПАК «Идеальный токен» выполняются назначенным должностным лицом, обладающим необходимыми знаниями и полномочиями.

В случае личного использования владелец одновременно является и Пользователем (оператором), и Администратором ПАК «Идеальный токен».

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

Перед установкой и эксплуатацией ПАК «Идеальный токен» необходимо внимательно ознакомиться с настоящим руководством.

Применение ПАК «Идеальный токен» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ.

[1] В качестве таких объектов могут выступать криптографические ключи пользователя (секретные симметричные ключи, закрытый и открытый ключи ключевой пары), цифровые сертификаты и другие данные в формате PKCS#11.

СОДЕРЖАНИЕ

1. Общие сведения

1.1. Состав и назначение ПАК «Идеальный токен»

ПАК «Идеальный токен» включает:

1) аппаратный компонент – USB-устройство «Идеальный токен» (далее по тексту – устройство «Идеальный токен», или устройство) со встроенным программным обеспечением (ПО);

2) программный компонент – специальное программное обеспечение (СПО) рабочей станции (РС), устанавливаемое на жесткий диск РС:

— утилита «Консоль администратора» (далее по тексту – Консоль администратора);

— утилита «Настройки пользователя» (далее по тексту – Настройки пользователя);

— сервис проверки регистрации.

Устройство «Идеальный токен» предназначено для хранения АОД. Основными элементами данного аппаратного модуля являются:

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

2) энергонезависимая флеш-память, используемая для хранения АОД.

ПАК «Идеальный токен» может использоваться на рабочих станциях типа IBM PC, функционирующих под управлением операционных систем (ОС) Windows XP (x32), Windows Server 2003 (x32), Windows 7 (x32), Windows 7 (x64).

СПО РС размещается на CD-диске, поставляемом в составе ПАК «Идеальный токен».

Основные особенности ПАК «Идеальный токен»:

- предусмотрена возможность задания правил доступа к защищаемой информации посредством формирования списка разрешенных РС;
- устройство «Идеальный токен» может использоваться в качестве хранилища ключей и сертификатов в том числе для средства криптографической защиты информации (СКЗИ) производства компании «КриптоПро»[1], для системы криптографической авторизации электронных документов (СКАД) «Сигнатура»[2] (включая версию 5.0).

ВНИМАНИЕ! В ПО СКЗИ «КриптоПро» устройство «Идеальный токен» отображается как «Идеальный токен»; в ПО СКАД «Сигнатура» – как персональное средство криптографической защиты информации (ПСКЗИ) ШИПКА. ПО СКАД «Сигнатура» версии 5.0 поддерживает считыватели ПСКЗИ ШИПКА старого и нового форматов. При работе через считыватель нового формата возможно хранение в устройстве «Идеальный токен» нескольких ключей.

[1] Взаимодействие с ПО КриптоПро осуществляется с использованием собственной библиотеки КриптоПро.

[2] Взаимодействие с СКАД «Сигнатура» осуществляется по интерфейсу PKCS#11.

ВНИМАНИЕ! «Идеальный токен» не может использоваться в качестве датчика случайных чисел для СКЗИ «КриптоПро».

1.2. Технические условия применения комплекса

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

- IBM PC совместимая ПЭВМ, работающая под управлением ОС Windows XP (x32), Windows Server 2003 (x32), Windows 7 (x32), Windows 7 (x64);
- свободный разъем USB.

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

1.3. Комплектность поставки ПАК «Идеальный токен»

ПАК «Идеальный токен» поставляется в составе:

- устройство «Идеальный токен» – 1шт.;
- CD-диск со специальным ПО;
- эксплуатационная документация на CD;
- паспорт – 1 брошюра;
- комплект упаковки.

2. Установка и настройка ПАК «Идеальный токен»

2.1. Порядок установки и настройки ПАК «Идеальный токен»

ВНИМАНИЕ! Не следует устанавливать СПО ПАК «Идеальный токен» на компьютер, на котором установлено СПО ПСКЗИ ШИПКА, – работа устройств может быть нарушена.

Установка ПАК «Идеальный токен» и его настройка в общем случае выполняется в несколько этапов:

- установка СПО РС на жесткий диск;
- подключение устройства «Идеальный токен» в разъем USB системного блока ПЭВМ;
- установка системного драйвера устройства;
- регистрация администратора;
- инициализация (начальное форматирование) устройства «Идеальный токен».

Особенности установки и настройки ПАК «Идеальный токен» как ключевого контейнера для СКАД «Сигнатура» и СКЗИ «КриптоПро» приведены в подразделе 2.7.

2.2. Установка программного обеспечения ПАК «Идеальный токен»

Для установки на жесткий диск ПЭВМ (РС) СПО следует запустить с CD программу ITSetup.exe (для 32-х битных ОС) или ITSetup64.exe (для 64-х битных ОС). Сначала на экран выводится окно выбора языка. В данный момент поддерживается вариант установки (и дальнейшей работы всех программных компонент) на двух языках – русском и английском. После выбора языка выполняется процедура начальной подготовки к установке и на экран выводится стартовое окно с общей информацией (рисунок 1).

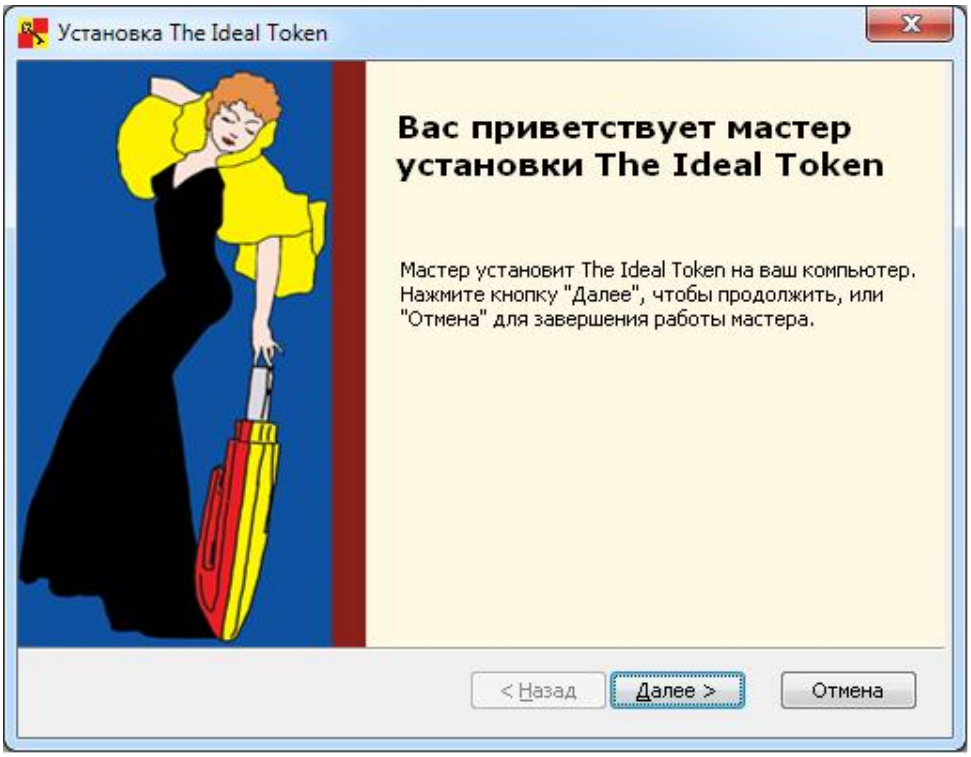

Рисунок 1 - Стартовое окно процедуры установки СПО

Для продолжения процедуры нужно щелкнуть левой клавишей мыши по кнопке <Далее>. Для прекращения установки следует выбрать кнопку <Отмена>.

Следующее окно – выбор папки установки ПО РС (рисунок 2). По умолчанию это папка C:\Program Files\OKB SAPR JSC\IdealToken (C:\Program Files (x86)\OKB SAPR JSC\IdealToken – для 64-битных версий ОС). Если необходимо установить ПО в другую папку, следует нажать кнопку <Обзор> и выбрать папку для установки вручную.

Для продолжения установки нужно нажать <Далее>, после чего выбрать кнопку <Установить>, чтобы начать установку. Если понадобилось изменить или просмотреть параметры установки, следует нажать кнопку <Назад>, а чтобы завершить работу мастера установки – кнопку <Отмена>.

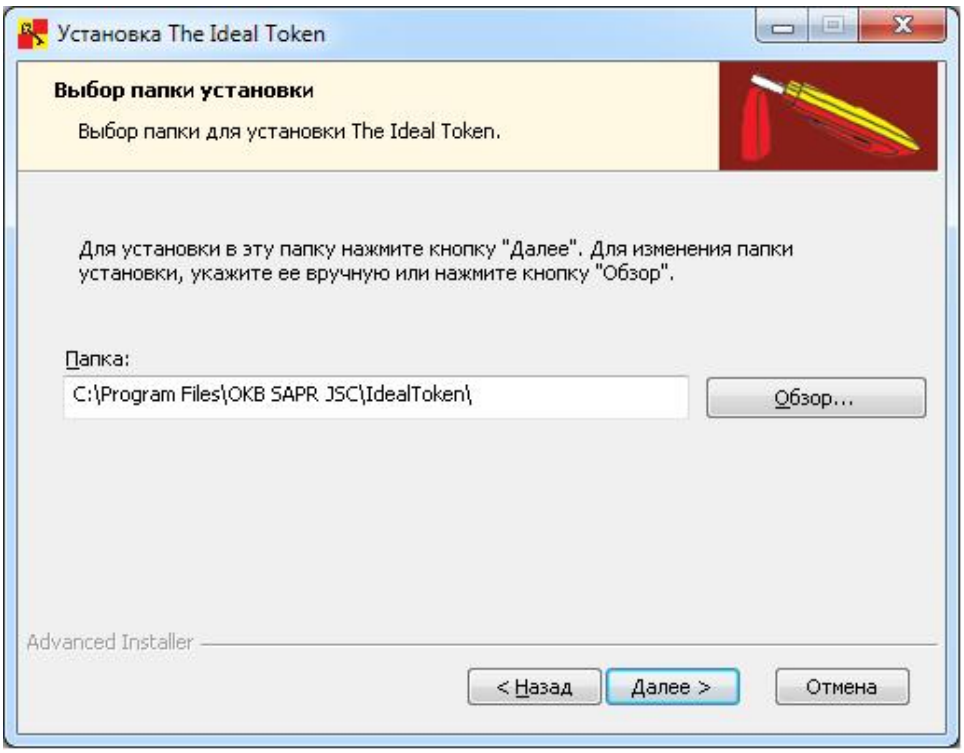

Рисунок 2 – Выбор папки установки

После успешного завершения установки на экран выводится сообщение о завершении работы мастера установки ПО (рисунок 3).

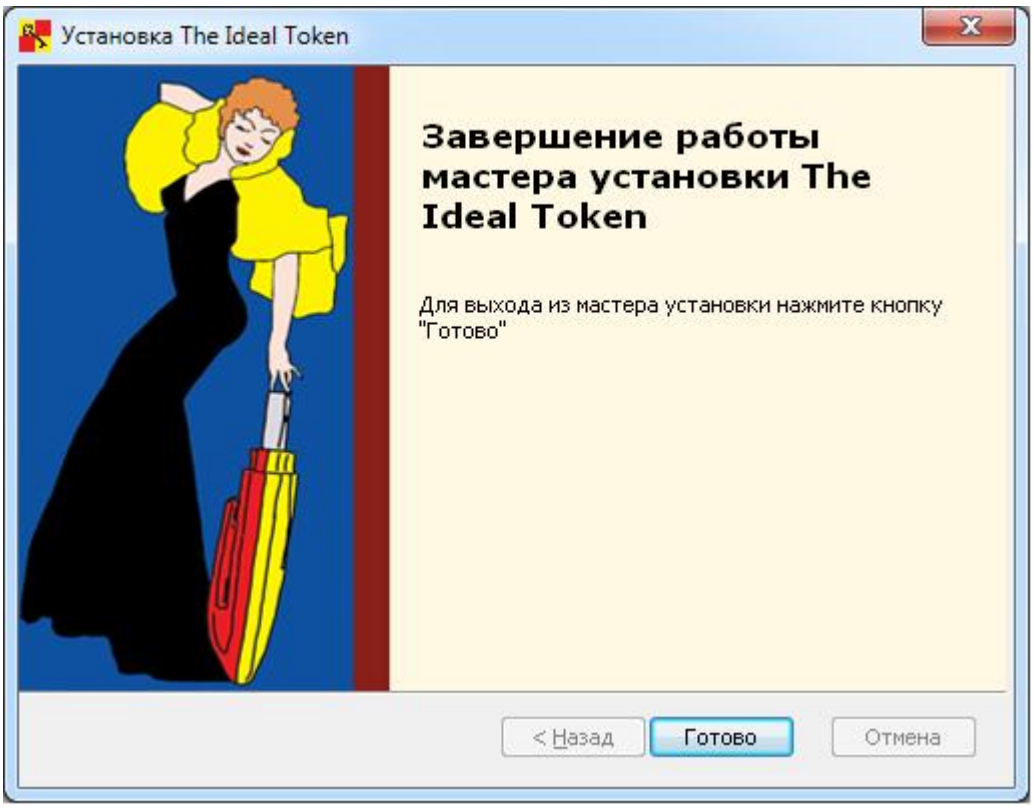

Рисунок 3 – Завершение работы мастера установки

Если при попытке установки СПО выдается окно «Изменение, восстановление или удаление установки» (рисунок 4), это значит, что на компьютере уже установлено СПО ПАК «Идеальный токен». Если при этом

устанавливается более новое СПО, то нужно выбрать «Удалить» для удаления старого.

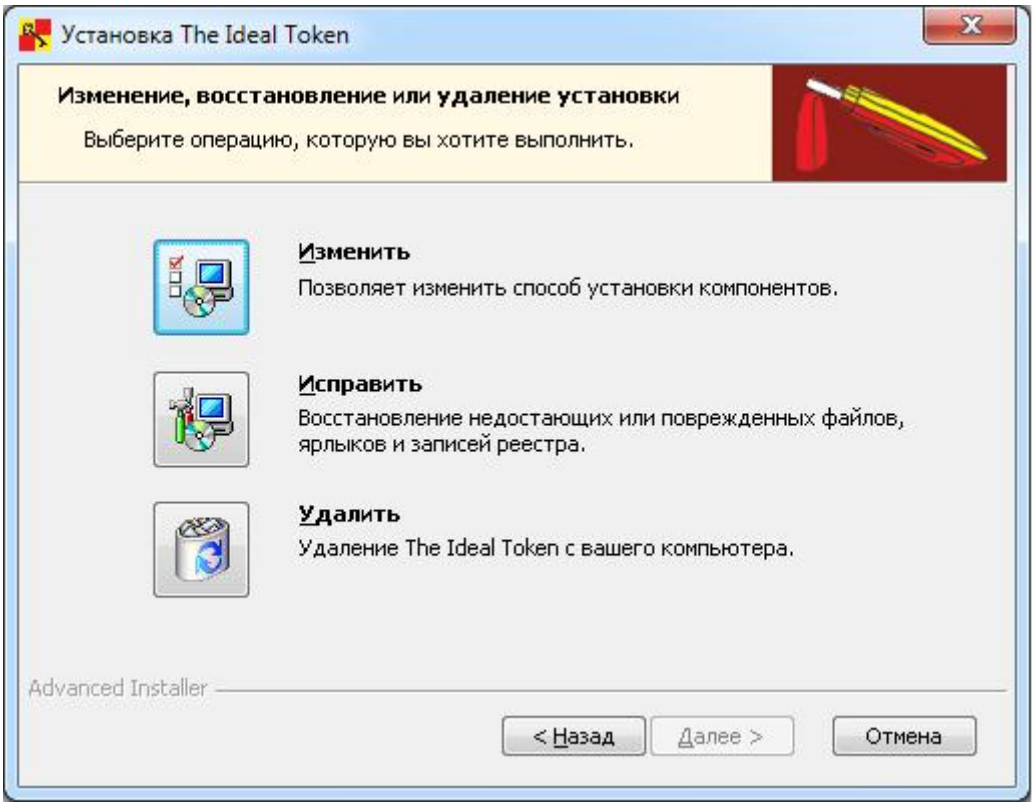

Рисунок 4 – Окно «Изменение, восстановление или удаление установки»

Удаление СПО ПАК «Идеальный токен» может быть выполнено стандартно, как и для любого другого ПО: <Пуск>-<Настройка>-<Панель управления>-<Установка и удаление программ>-<The Ideal Token>-<Удалить>. Удаление СПО можно выполнить и таким образом: <Пуск>-<Программы>-<Идеальный токен>-<Удалить>.

2.3. Подключение устройства «Идеальный токен»

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

2.4. Установка системного драйвера

При первом подключении устройства «Идеальный токен» к USB-порту происходит установка системного драйвера:

- если на PC установлена ОС Windows XP/2003, необходимо установить обновление Microsoft для устройства чтения карт USB (KB967048-v2). Его можно получить с использованием механизмов, предусмотренных Microsoft для распространения обновлений, а в случае отсутствия такой возможности – запустить из папки установки СПО ПАК «Идеальный токен»;

• если на PC установлена ОС Windows 7, системный драйвер, как правило, устанавливается автоматически.

2.5. Регистрация администратора

Регистрация администратора относится к числу обязательных процедур. Для выполнения этой процедуры необходимо запустить Консоль администратора (исполняемый файл ITAdminConsole.exe в папке IdealToken, или <Пуск>-<Консоль администратора>, или <Пуск>-<Все программы>-<Идеальный токен>-<Консоль администратора>). На экран выводится окно Консоли администратора (рисунок 5). Если в устройстве еще не был зарегистрирован администратор, активны только пункты меню <Регистрация Администратора> и <О программе>.

Рисунок 5 – Консоль администратора

Далее необходимо нажать кнопку <Регистрация Администратора>. На экране появляется окно регистрации (рисунок 6).

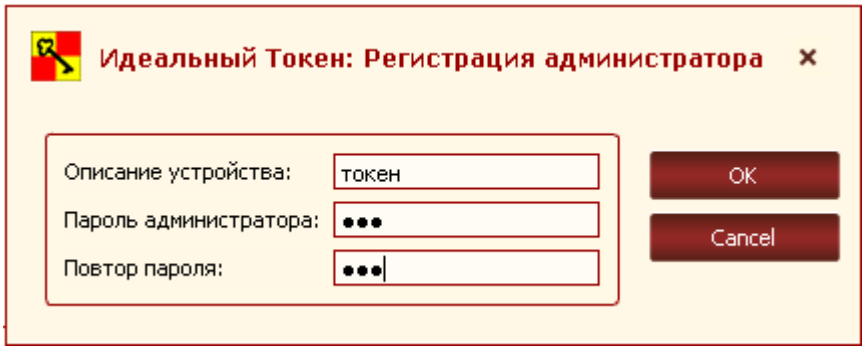

Рисунок 6 – Окно регистрации администратора

В появившемся диалоговом окне необходимо задать имя устройства «Идеальный токен» и установить пароль администратора с подтверждением. Для завершения операции регистрации нужно нажать кнопку <OK>, для отмены операции – кнопку <Cancel>.

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

В случае если пароль администратора не совпадает с повторно введенным паролем, выводится соответствующее сообщение об ошибке (рисунок 7). Следует нажать кнопку <ОК> и ввести корректное подтверждение пароля администратора.

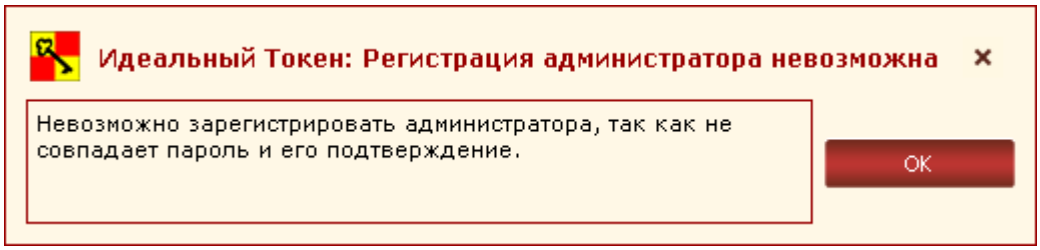

Рисунок 7 – Сообщение об ошибке при подтверждении пароля

Если произведена попытка регистрации администратора без указания имени устройства, выдается сообщение о невозможности регистрации администратора без задания описания устройства (рисунок 8).

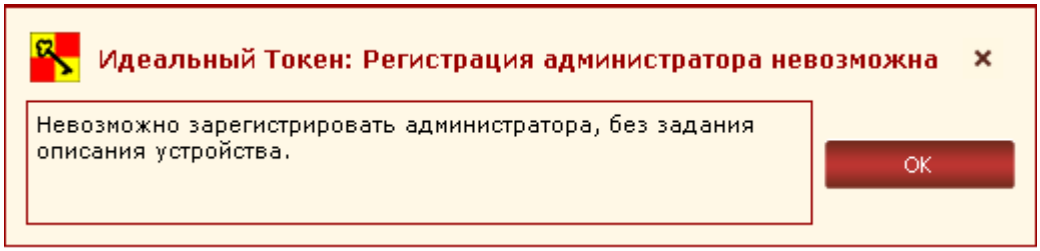

Рисунок 8 – Сообщение об ошибке при задании описания устройства

Если при регистрации администратора введены все необходимые данные, выводится сообщение о завершении процедуры регистрации (рисунок 9), а пароль администратора и имя устройства «Идеальный токен» передаются в устройство и сохраняются в его внутренней памяти.

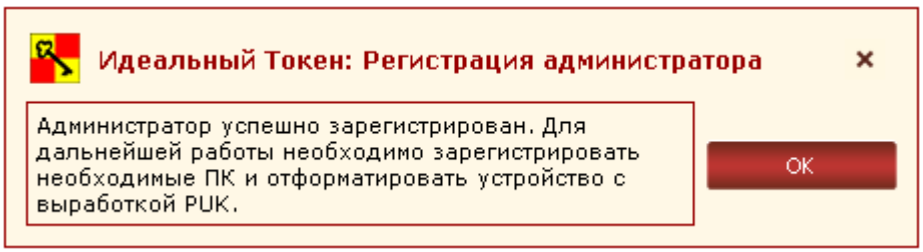

Рисунок 9 – Успешная регистрация администратора

Пароль администратора необходим для выполнения любых процедур в рамках администрирования ПАК «Идеальный токен», включая смену пароля администратора (подробнее о смене пароля администратора см. 3.4).

ВНИМАНИЕ! Необходимо запомнить или надежно сохранить пароль администратора, знание которого позволяет получать доступ к функциям администрирования ПАК «Идеальный токен». Важно помнить о

необходимости сохранения пароля администратора недоступным для третьих лиц!

Далее функция регистрации администратора блокируется, в графе «Описание» отображается имя устройства «Идеальный токен» и становятся доступными остальные функции администрирования (рисунок 10).

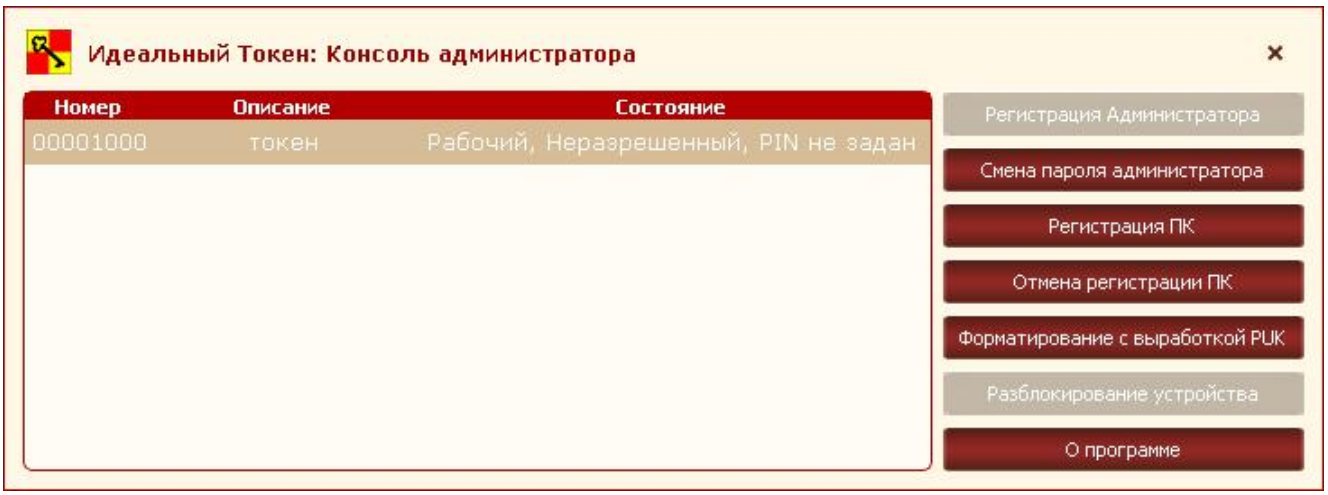

Рисунок 10 - Консоль администратора с доступными опциями

После регистрации компьютера администратором и установки пользователем PIN-кода устройства в колонке «Состояние» Консоли администратора отображается: «Рабочий, Разрешенный» (рисунок 11).

Рисунок 11 – Консоль администратора после регистрации пользователя

2.6. Начальное форматирование устройства «Идеальный токен»

В процессе начального форматирования, выполняемого администратором, формируется PUK -код (8 символов), необходимый для восстановления возможности получения доступа к пользовательской информации при блокировании устройства «Идеальный токен» (в случае если количество неудачных попыток авторизации превысит 3 раза).

Для проведения процедуры начального форматирования устройства «Идеальный токен» необходимо в Консоли администратора (рисунок 5) выбрать пункт <Форматирование с выработкой PUK>. В появившемся окне необходимо ввести пароль администратора и нажать кнопку <ОК>.

Если пароль администратора указан неверно, на экран выводится оповещение об ошибке при вводе пароля (рисунок 12).

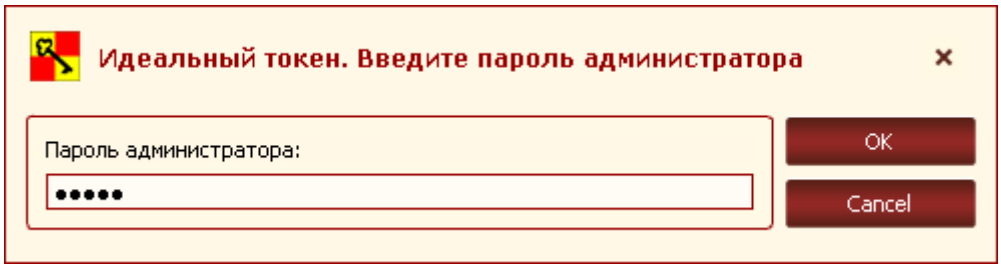

Рисунок 12 – Оповещение об ошибке при вводе пароля администратора

Необходимо нажать кнопку <ОК> и повторить попытку форматирования устройства «Идеальный токен».

При успешном проведении процедуры форматирования устройства на экран выводится сообщение с PUK-кодом (рисунок 13).

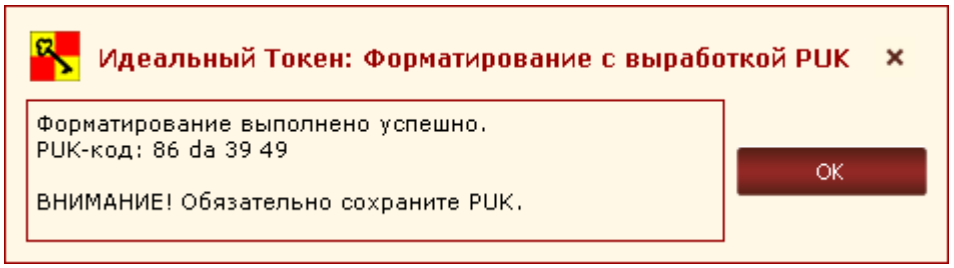

Рисунок 13 – Выработанный PUK-код устройства

ВНИМАНИЕ! Необходимо надежно сохранить PUK-код, знание которого позволяет получать доступ к функции разблокирования устройства «Идеальный токен». Важно также сохранить его недоступным для третьих лиц!

2.7. Настройка ПАК «Идеальный токен» как ключевого контейнера для СКЗИ

2.7.1. Настройка ПАК «Идеальный токен» как ключевого контейнера для СКАД «Сигнатура»

Подробная информация о порядке работы администратора ПАК «Идеальный токен» с СКАД «Сигнатура» приведена в документации на СКАД «Сигнатура».

2.7.2. Настройка ПАК «Идеальный токен» как ключевого контейнера для КриптоПро

В настоящий момент реализована поддержка КриптоПро CSP 3.6 (далее – КриптоПро CSP).

Для корректной работы ПО КриптоПро CSP необходимо установить ДО установки СПО ПАК «Идеальный токен».

В случае инсталляции ПО КриптоПро CSP класса КС2 необходимо в окне последних приготовлений (рисунок 14) установить флаг «Зарегистрировать биологический датчик случайных чисел».

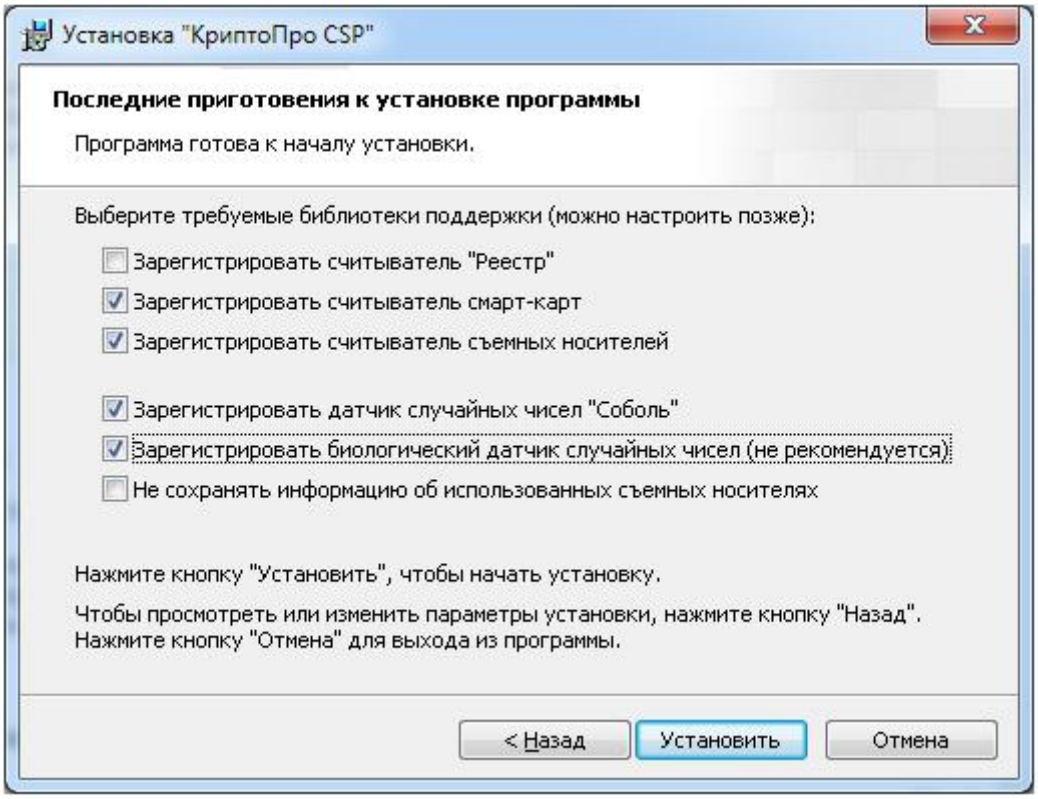

Рисунок 14 – Окно последних приготовлений к установке КриптоПро CSP

Изменение других параметров установки для работы с ПАК «Идеальный токен» не требуется.

Установка КриптоПро CSP классов КС1 и КС3 выполняется с параметрами по умолчанию.

Подробная информация о порядке работы администратора ПАК «Идеальный токен» с КриптоПро CSP приведена в документации на КриптоПро CSP.

3. Управление устройствомУстройство «Идеальный токен»

3.1. Добавление компьютера в список разрешенных

Для добавления персонального компьютера (ПК) в список разрешенных для работы с устройством «Идеальный токен» необходимо в Консоли администратора (рисунок 10) выбрать пункт <Регистрация ПК>, после чего на экране появится окно регистрации ПК (рисунок 15).

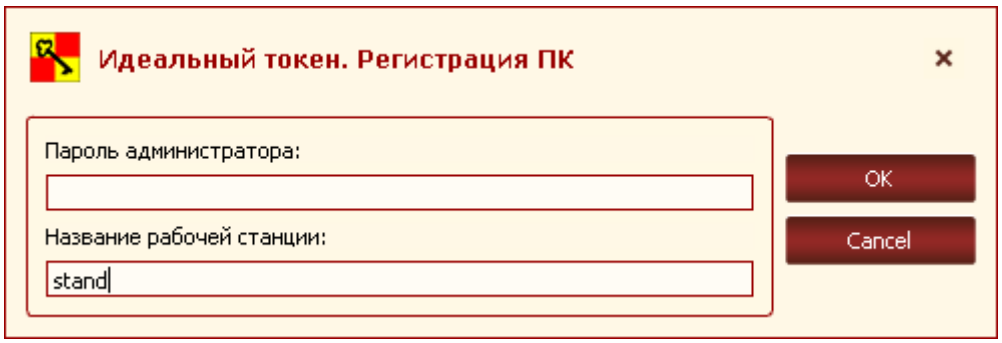

Рисунок 15 - Окно регистрации ПК

В появившемся окне необходимо ввести пароль администратора и название добавляемой РС (текущей или удаленной). По умолчанию в графе «Название рабочей станции» указывается имя текущей РС.

При первом подключении устройства «Идеальный токен» к удаленной РС из числа разрешенных внутреннее ПО устройства производит считывание и сохранение информации о параметрах оборудования данной РС.

Если при добавлении РС неверно указан пароль администратора, на экран выводится оповещение об ошибке при установке списка разрешенных РС (рисунок 16).

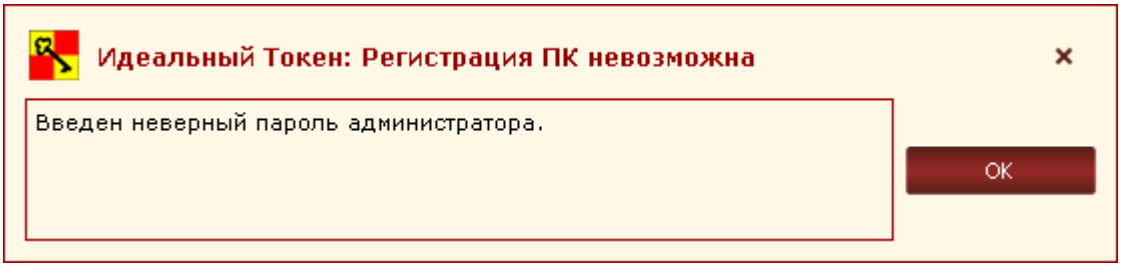

Рисунок 16 – Сообщение об ошибке в процессе ввода пароля администратора

Необходимо нажать кнопку <ОК> и повторить попытку добавления РС.

Если операция установки списка разрешенных РС выполнена корректно, то на экране отображается сообщение об успешном добавлении РС в список разрешенных (рисунок 17).

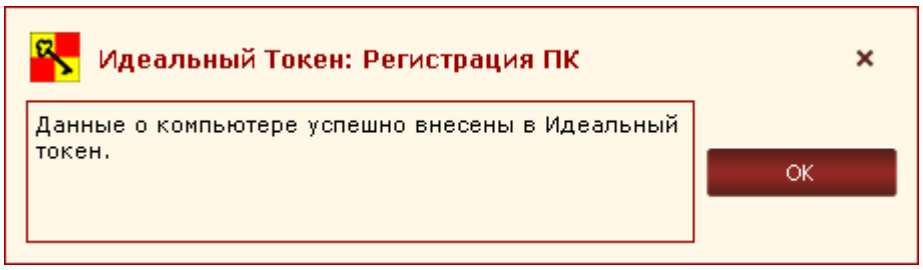

Рисунок 17 – Сообщение об успешном добавлении РС в список разрешенных

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

ВНИМАНИЕ! При корпоративном применении ПАК «Идеальный токен» в целях безопасности рекомендуется, чтобы первое подключение устройства «Идеальный токен» к РС выполнял администратор.

3.2. Удаление компьютера из списка разрешенных

ВНИМАНИЕ! Возможно удаление из списка разрешенных только текущей РС. Поэтому при необходимости проведения такой процедуры устройство «Идеальный токен» следует подключать непосредственно к удаляемой из списка РС.

Если необходимо удалить РС из числа разрешенных, в Консоли администратора (рисунок 5) следует выбрать пункт <Отмена регистрации ПК>, при этом будет выведено окно для ввода пароля администратора (рисунок 18).

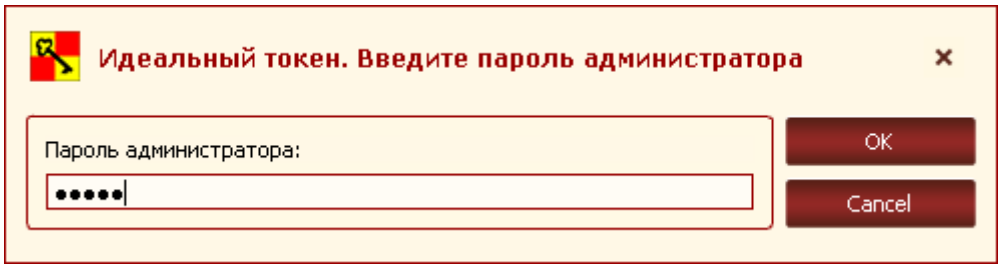

Рисунок 18 – Окно удаления РС из списка разрешенных

Если пароль администратора указан неверно, на экран выводится оповещение об ошибке (рисунок 19).

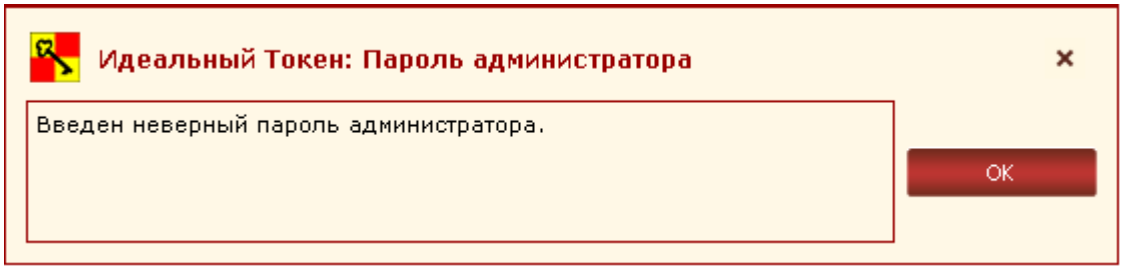

Рисунок 19 - Сообщение об ошибке в процессе ввода пароля администратора

Необходимо нажать кнопку <OK> и повторить попытку удаления РС.

В случае успешного удаления РС из списка разрешенных на экране появляется сообщение об успешном завершении процедуры отмены регистрации ПК (рисунок 20).

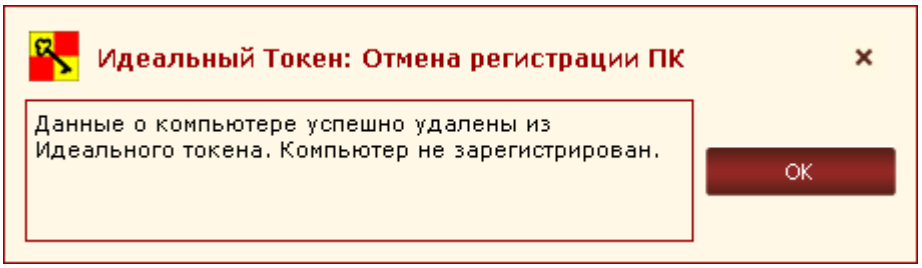

Рисунок 20 - Сообщение об успешном удалении РС из списка разрешенных

3.3. Разблокирование устройства «Идеальный токен»

В случае если количество неудачных попыток авторизации пользователя больше трех, устройство «Идеальный токен» блокируется. Администратор может разблокировать его с помощью PUK-кода. Если значение PUK-кода утеряно, разблокировать устройство администратор может только с помощью функции форматирования устройства.

3.4. Смена пароля администратора

В случае необходимости смены пароля администратора (например, в случае его компрометации) в Консоли администратора (рисунок 10) следует нажать кнопку <Смена пароля администратора>. После выбора этой функции на экране появляется окно, показанное на рисунке 21.

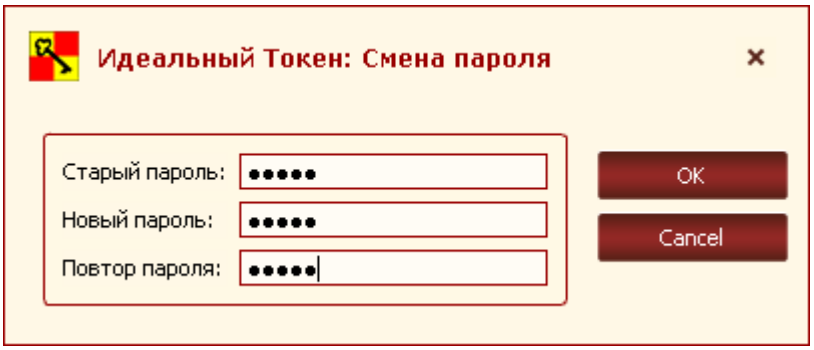

Рисунок 21 - Окно смены пароля администратора

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 <Cancel> - для ее отмены.

Если подтверждение пароля введено некорректно, на экране появляется предупреждение (рисунок 22):

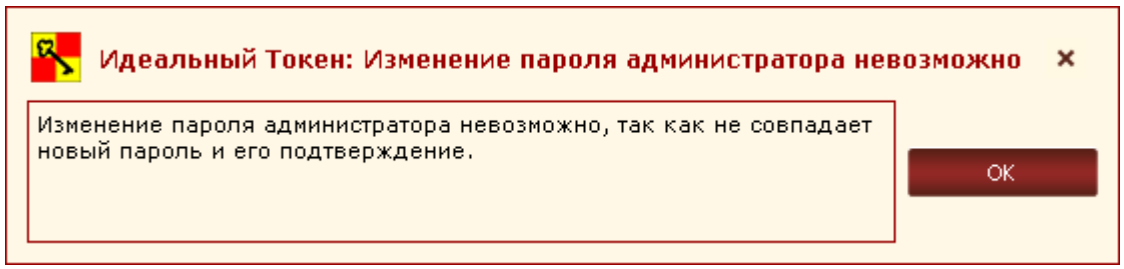

Рисунок 22 - Предупреждение о том, что подтверждение пароля администратора не совпадает с паролем администратора

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

Если же старый пароль введен некорректно, на экране появляется сообщение о вводе некорректного пароля (рисунок 23).

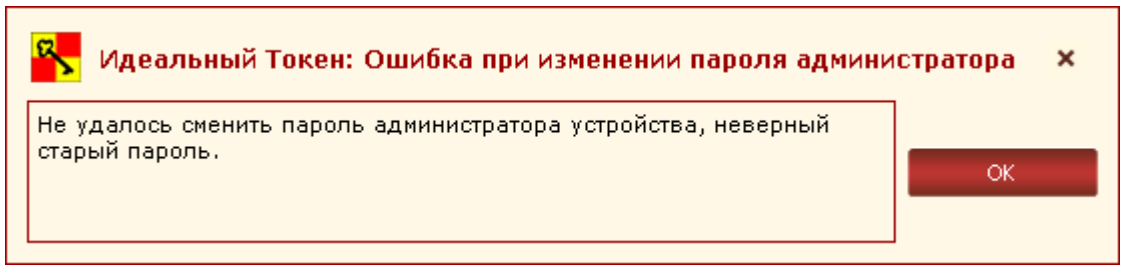

Рисунок 23 - Сообщение о вводе некорректного старого пароля

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

Если операция смены пароля администратора выполнена успешно, на экране отображается оповещение об успешной смене пароля (рисунок 24):

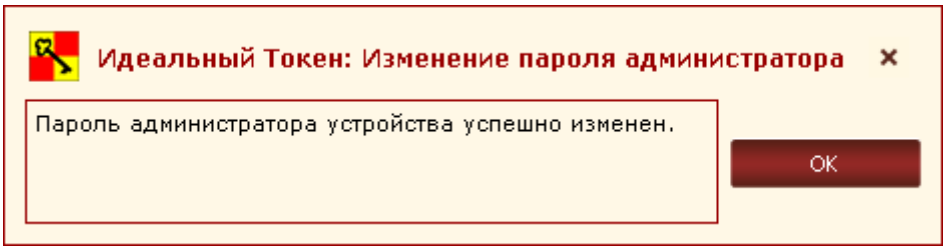

Рисунок 24 - Оповещение об успешной смене пароля

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

3.5. Завершение работы

Чтобы завершить работу с ПАК «Идеальный токен», необходимо завершить работу СПО РС и извлечь устройство «Идеальный токен».

4. Рекомендации по организации безопасного применения ПАК «Идеальный токен»

4.1. Общее описание рекомендаций

При применении ПАК «Идеальный токен» 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 «Идеальный токен» 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 25). Данная операция может быть выполнена для рабочих станций, не включенных в домен.

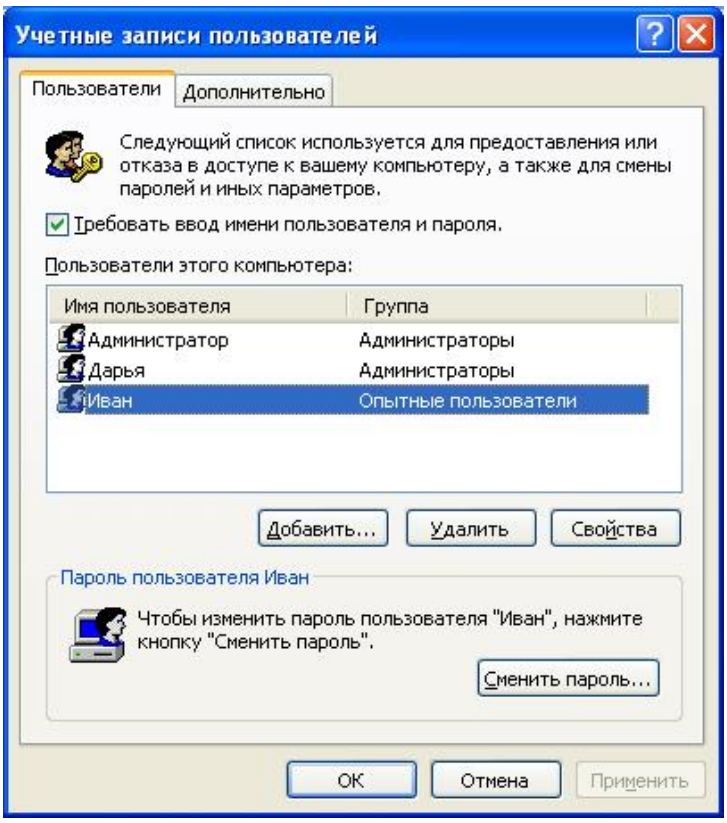

Рисунок 25 – Окно настроек учетных записей пользователей

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 26).

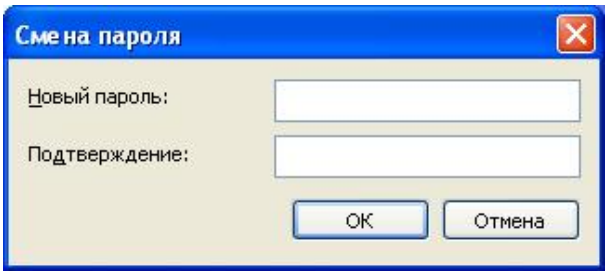

Рисунок 26 – Окно смены пароля пользователя для входа в ОС

4.3. Включение режима автоматической блокировки экрана

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

•*при работе в Windows XP:* в меню <Пуск>-<Панель управления>-<Экран>-<Заставка> следует установить галочку «Начинать с экрана приветствия» и выставить необходимый интервал времени неактивности (рисунок 27).

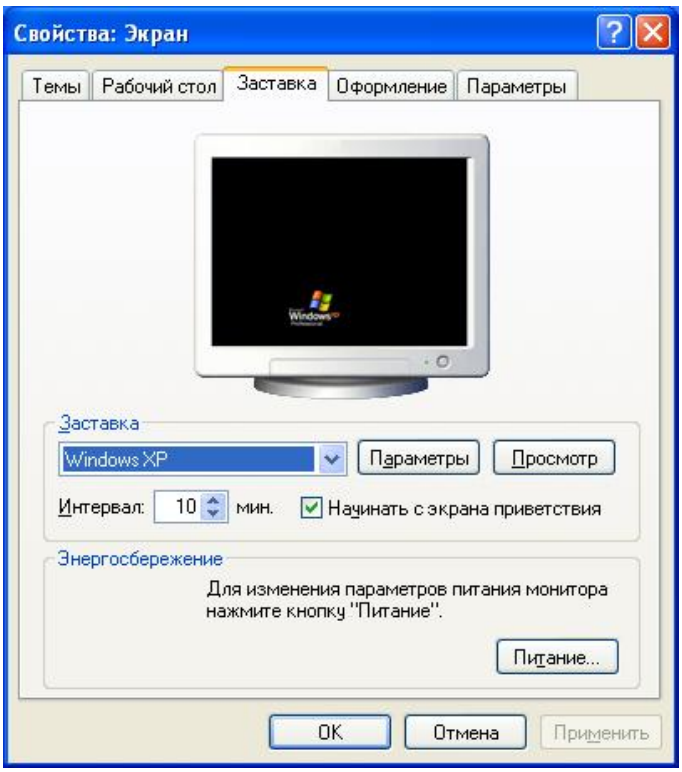

Рисунок 27 – Окно настройки заставки экрана в ОС Windows XP

•*при работе в Windows 7:* в меню <Пуск>-<Панель управления>-<Персонализация>-<Заставка> следует установить флаг «Начинать с экрана входа в систему» и выставить необходимый интервал времени неактивности (рисунок 28).

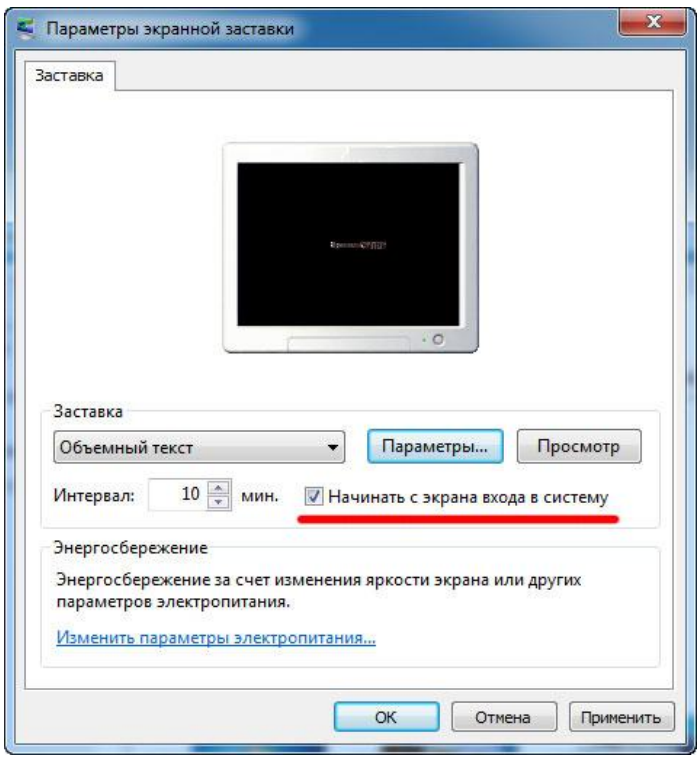

Рисунок 28 - Окно настройки заставки экрана в ОС Windows 7

5. Перечень принятых сокращений и обозначений

АОД	–	абстрактные объекты данных;
ОС	–	операционная система;
ПАК	–	программно-аппаратный комплекс;
ПК	–	персональный компьютер;
ПО	–	программное обеспечение;
РС	–	рабочая станция;
СКЗИ	–	средство криптографической защиты информации;
PIN	–	Personal Identification Number;
PUK	–	Personal Unblocking Key;
USB	–	Universal Serial Bus.