Код Безопасности

Средство защиты информации

SECRET NET 7

Руководство пользователя

RU.88338853.501410.015 92

Почтовый адрес:	**105318, Россия, Москва, а/я 101 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для пользователей компьютеров с установленным программным обеспечением изделия "Средство защиты информации Secret Net 7" RU.88338853.501410.015 (далее — система Secret Net, Secret Net).

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения.

Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Типовые операции

При работе на защищенном компьютере часто выполняются следующие операции:

Заполнение текстовых полей. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранный символ в строке ввода клавишами <Backspace> или <Delete> и повторите ввод.

Ввод пароля. Вводимые символы пароля не отображаются в явном виде, а замещаются другим символом — обычно точкой или звездочкой. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

Предъявление персонального идентификатора. Персональным идентификатором называется устройство, применяемое в составе программно-аппаратных средств идентификации и аутентификации. Персональный идентификатор предназначен для хранения служебной информации о пользователе. Как правило, идентификатор выполнен в виде электронного ключа или брелока. Если пользователю был присвоен персональный идентификатор, некоторые операции могут быть выполнены пользователем только после предъявления идентификатора. В системе могут использоваться идентификаторы разных типов, что обусловливает различия в способах их предъявления. Инструкции по применению и правильному предъявлению идентификатора следует получить у администратора.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем Учебного центра можно по электронной почте (edu@itsecurity.ru).

Глава 1
Общие сведения

Что нужно знать

Система Secret Net расширяет функциональные возможности ОС Windows по управлению доступом к ресурсам и правами пользователей.

Прежде чем приступить к работе на защищенном компьютере, рекомендуется ознакомиться с изложенными в этом документе базовыми понятиями и описанием порядка работы с системой.

Центральную роль в управлении системой защиты играет администратор безопасности. Администратор определяет права пользователя на доступ к ресурсам компьютера.

В системе могут использоваться аппаратные средства (например, идентификаторы eToken), на которых записана служебная информация для идентификации пользователя.

Что необходимо иметь

Перед началом работы на защищенном компьютере необходимо:

1. Получить у администратора имя пользователя и пароль для входа в систему. Администратор безопасности также может выдать вам персональный идентификатор, который потребуется для входа в систему. Кроме того, для входа в режиме усиленной аутентификации может использоваться отдельный ключевой носитель, содержащий ключевую информацию. Ключевым носителем может быть персональный идентификатор, ключевая дискета, флеш-карта или USB-флеш-накопитель.
2. Выяснить у администратора, какими правами и привилегиями вы сможете пользоваться при работе в системе.

Что важно помнить

Во избежание затруднительных ситуаций следуйте двум общим рекомендациям:

1. Запомните свое имя в системе и пароль. Никому не передавайте персональный идентификатор и ключевой носитель, а пароль никому не сообщайте.
2. Во всех сложных ситуациях, которые вы сами не в состоянии разрешить, обращайтесь к администратору безопасности. Если имеющихся прав доступа к ресурсам недостаточно для эффективного выполнения должностных обязанностей, обращайтесь к администратору безопасности.

Глава 2
Загрузка компьютера и вход в систему

Чтобы начать сеанс работы, необходимо загрузить компьютер и выполнить процедуру входа в систему. На компьютере, защищенном Secret Net, загрузка и вход в систему выполняются, как правило, без существенных отличий от стандартного порядка. Необходимость выполнения пользователем дополнительных действий может возникнуть, если на компьютере установлен программно-аппаратный комплекс "Соболь" или действуют ограничения для входа в систему.

Вход пользователя в систему может осуществляться по-разному. Применение нужного способа зависит от оснащенности системы защиты средствами аппаратной поддержки и наличия у пользователей персональных идентификаторов.

Ниже в таблице перечислены способы входа в систему при различных режимах идентификации пользователей.

Режим	Способ входа в систему	Условия применения
По имени	Только стандартный способ входа в ОС Windows (см. стр.**10**)	В системах, не оснащенных аппаратными средствами контроля входа
Только по идентификатору	Только с предъявлением персонального идентификатора (см. стр.**10**)	В системах, оснащенных аппаратными средствами, когда у всех пользователей есть персональные идентификаторы
Смешанный	Стандартный способ входа в ОС Windows или с предъявлением персонального идентификатора	В системах, оснащенных аппаратными средствами, когда еще не всем пользователям выданы персональные идентификаторы

В стандартном и смешанном режимах входа Secret Net допускает работу с персональными идентификаторами, активированными средствами ОС Windows (например, Smart Card, eToken и пр.). Сведения об использовании идентификаторов в ОС Windows см. в документации на операционную систему. В режиме "Только по идентификатору" можно использовать персональные идентификаторы, активированные средствами Secret Net, но не ОС Windows. Для всех пользователей компьютера устанавливается единый режим входа.

Если применяются средства аппаратной поддержки системы защиты, администратор выдает каждому пользователю персональный идентификатор (в зависимости от типа применяемого средства — идентификаторы eToken, iKey, Rutoken, JaCarta или iButton). При необходимости компьютер оснащается дополнительным устройством для считывания информации, содержащейся в персональном идентификаторе.

"Предъявить" персональный идентификатор означает привести его в соприкосновение со считывающим устройством.

Примечание.

Для доступа к памяти USB-ключа или смарт-карты необходимо указывать специальный пароль — PIN-код. По умолчанию идентификатор защищен "стандартным" PIN-кодом, который задан производителем устройства. Если стандартный PIN-код не изменен, система Secret Net автоматически осуществляет доступ к памяти идентификатора при его предъявлении. В том случае, если администратор сменил стандартный PIN-код на другой (нестандартный), при каждом предъявлении идентификатора система выводит запрос на ввод PIN-кода. Администратор обязан сообщить вам нестандартный PIN-код при передаче идентификатора.

Внимание!
Не забывайте PIN-код, его утрата делает невозможным дальнейшее использование идентификатора.

В персональном идентификаторе также может быть записан пароль пользователя и ключевая информация, необходимая для входа в систему в режиме усиленной аутентификации по ключу.

Загрузка и вход в систему при использовании ПАК "Соболь"

Если на компьютере установлен программно-аппаратный комплекс "Соболь", который функционирует в режиме интеграции с системой Secret Net, загрузка компьютера и вход пользователя в систему могут выполняться с использованием одного персонального идентификатора.

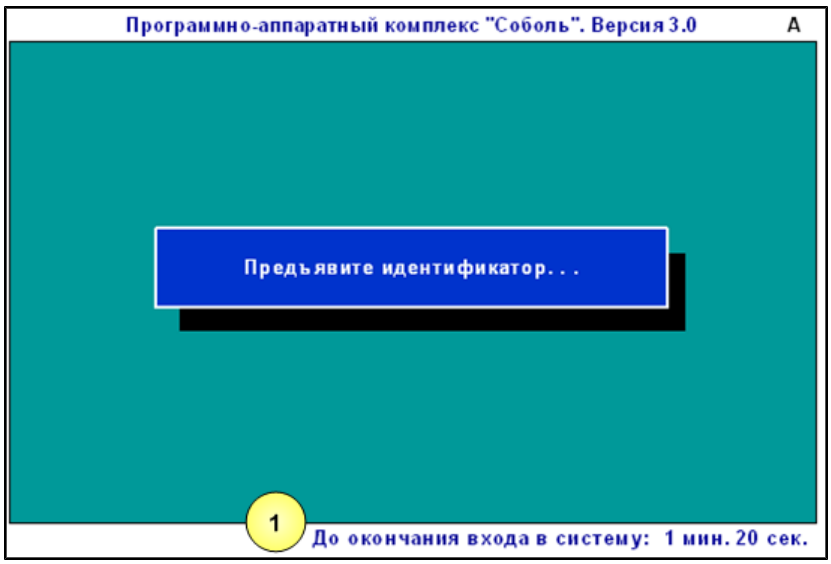
В этом случае ваши действия зависят от того, записан ли в идентификатор пароль пользователя и является ли этот пароль актуальным для ОС Windows:

- если в идентификаторе записан актуальный для ОС Windows пароль, то он считывается при входе в комплекс "Соболь" и затем учитывается при входе в ОС Windows;
- если в идентификаторе записан неактуальный для ОС Windows пароль (например, пароль был изменен, но его новое значение не было записано в идентификатор), то считывание из идентификатора этого пароля позволяет войти в комплекс "Соболь", но не в ОС Windows. В этом случае вам нужно ввести актуальный пароль при входе в ОС Windows;
- если в идентификаторе не записан пароль, то вам необходимо дважды ввести пароль: при входе в комплекс "Соболь" и затем при входе в ОС Windows.

Для загрузки компьютера и входа в систему:

1. Включите питание компьютера.

   На экране появится запрос персонального идентификатора:



Пояснение.
На рисунке выносками обозначены элементы: 1 — строка сообщений.

Обратите внимание на следующие особенности процедуры входа:

- При включенном режиме автоматического входа в строке сообщений будет отсчитываться время в секундах, оставшееся до автоматического входа в комплекс "Соболь", после которого начнется загрузка операционной системы.

- Если включен режим ограничения времени, в строке сообщений будет отсчитываться время в минутах и секундах, оставшееся до предъявления идентификатора и ввода пароля. Если вы не успели за отведенное время выполнить эти действия, на экране появится сообщение "Время сеанса входа в систему истекло". Чтобы повторить попытку входа, нажмите клавишу <Enter>, а затем — любую клавишу.

2. Предъявите свой персональный идентификатор.

Если в идентификаторе нет пароля, на экране появится диалог для его ввода:

- Введите пароль для входа в комплекс "Соболь".

Примечание.
На экране каждый символ пароля отображается как "*" (звездочка). Помните, что при вводе пароля различаются строчные и прописные буквы. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <Backspace> или <Delete> и заново повторите ввод символов.

- Нажмите клавишу <Enter>.

  Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и снова предъявите идентификатор. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.

Внимание!
Учитывайте, что число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение в текущем сеансе входа, то при следующей попытке входа в строке сообщений появится сообщение "Ваш вход в систему запрещен: Вы превысили предел неудачных попыток входа", после чего компьютер будет заблокирован. В этом случае обратитесь за помощью к администратору.

После успешного предъявления идентификатора (и ввода правильного пароля, если это необходимо) выполняется тестирование датчика случайных чисел. При обнаружении ошибок в строке сообщений появится сообщение об этом. Если после перезагрузки компьютера тестирование датчика случайных чисел вновь завершилось с ошибкой, обратитесь за помощью к администратору.

Перед загрузкой операционной системы проводится контроль целостности файлов (если это предусмотрено).

Если проверка завершена успешно, начнется загрузка операционной системы. При обнаружении ошибок на экране появятся сообщения об ошибках. Если в строке сообщений появилось сообщение "Компьютер заблокирован", выключите компьютер и обратитесь за помощью к администратору.

3. Далее на этапе загрузки операционной системы ваши действия зависят от того, какая информация о пароле содержится в персональном идентификаторе. Возможны следующие варианты:

- пароль, считанный из идентификатора при входе в комплекс "Соболь", является актуальным для ОС Windows;
- в идентификаторе не записан пароль или идентификатор содержит другой пароль, не актуальный для ОС Windows.

Ситуация 1	**Если в идентификаторе содержится актуальный пароль,** то после успешной проверки прав пользователя выполняется вход в систему без запроса пароля

Ситуация 2	**Если в идентификаторе нет пароля или содержится другой пароль,** появится диалог для ввода учетных данных пользователя, где будет отображаться имя пользователя — владельца предъявленного идентификатора

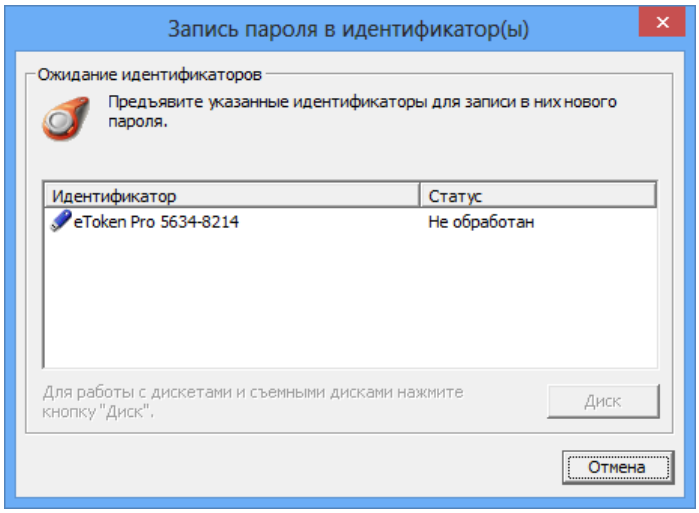
Введите актуальный пароль в поле "Пароль" и нажмите кнопку "→" или "OK".

Если введенный вами пароль правильный и хранение пароля в идентификаторе **не** предусмотрено, выполняется вход в систему.

Если введенный вами пароль правильный и актуальный пароль нужно записать в идентификатор — на экране появится соответствующий запрос. В этом случае выполните следующие действия:

- Нажмите кнопку "Да" в окне запроса.

  На экране появится диалог, содержащий наименование вашего идентификатора.



- Для записи пароля предъявите идентификатор.

  В результате успешной записи нового пароля в идентификатор его статус в списке изменится на "Обработан". После этого идентификатор можно изъять из считывателя.
- Нажмите в диалоге кнопку "Закрыть".

После закрытия диалога выполняется вход в систему.

Варианты входа в систему

При входе в систему пользователь должен указать учетные данные, необходимые для его идентификации. После ввода учетных данных система аутентифицирует пользователя, и при успешном завершении аутентификации предоставляется возможность работы пользователя в системе.

Процедура входа начинается при появлении на экране приглашения для входа в систему. В зависимости от действующих механизмов защиты и ограничений, установленных администратором, действия пользователя для входа в систему могут различаться.

Внимание!

Во время загрузки компьютера до появления экрана приветствия (приглашение на вход в систему) не рекомендуется нажимать какие-либо клавиши на клавиатуре. Некоторые клавиши могут активировать специальные режимы загрузки, требующие административные полномочия для работы. Чтобы избежать возникновения проблемных ситуаций, выполняйте действия в строгом соответствии с представленным описанием.

Стандартный режим входа

При стандартном режиме входа порядок действий пользователя совпадает с принятым в ОС Windows.

Для входа в стандартном режиме:

1. Перед входом в систему в зависимости от операционной системы компьютера появляется экран блокировки, экран приветствия или приглашение на вход. Чтобы начать процедуру входа, выполните соответствующее действие:
   - на компьютере с ОС Windows 8 или Windows Server 2012 — отключите экран блокировки, если он отображается (для этого, например, нажмите любую клавишу). Проверьте имя учетной записи, предлагаемой ОС для входа. Если требуется указать другую учетную запись, перейдите к списку входивших пользователей (для этого, например, нажмите клавишу <Esc>) и выберите нужное имя или элемент "Другой пользователь". На экране появятся поля для ввода учетных данных пользователя;
   - на компьютере с ОС Windows 7/Vista или Windows Server 2008 — выберите нужное имя учетной записи или элемент "Другой пользователь". На экране появятся поля для ввода учетных данных пользователя;
   - на компьютере с ОС Windows XP или Windows Server 2003 — нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>. На экране появится диалог для ввода учетных данных пользователя.
2. Укажите ваши учетные данные:
   - при необходимости введите полное имя пользователя с указанием имени компьютера или домена в поле "Пользователь";
   - введите пароль пользователя в поле "Пароль" или оставьте это поле пустым, если вам разрешено входить в систему без пароля.

   Примечание.
   В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <Backspace> или <Delete> и заново повторите ввод символов.
3. Нажмите кнопку "→" или "ОК".

   Если учетные данные введены правильно, выполняется вход в систему.

Вход по идентификатору

При использовании для входа в систему персонального идентификатора, активированного средствами Secret Net, система автоматически определяет имя пользователя, которому присвоен идентификатор.

Для входа по идентификатору:

1. Перед входом в систему в зависимости от операционной системы компьютера появляется экран блокировки, экран приветствия или приглашение на вход. После этого система готова к считыванию данных из идентификатора. Предъявите свой персональный идентификатор.

   Примечание.
   Если идентификатор защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".
2. Реакция системы защиты зависит от информации о пароле пользователя, содержащейся в персональном идентификаторе. Возможны следующие варианты:
   - идентификатор содержит актуальный пароль пользователя;

- в идентификаторе не записан пароль или идентификатор содержит другой пароль, не совпадающий с паролем пользователя (например, из-за того, что срок действия пароля истек и он был заменен, но не записан в персональный идентификатор).

Ситуация 1	**Если в идентификаторе содержится актуальный пароль,** то после успешной проверки прав пользователя выполняется вход в систему без запроса пароля
Ситуация 2	**Если в идентификаторе нет пароля или содержится другой пароль,** появится диалог для ввода учетных данных пользователя, где будет отображаться имя пользователя — владельца предъявленного идентификатора

Введите актуальный пароль в поле "Пароль" и нажмите кнопку "→" или "ОК".

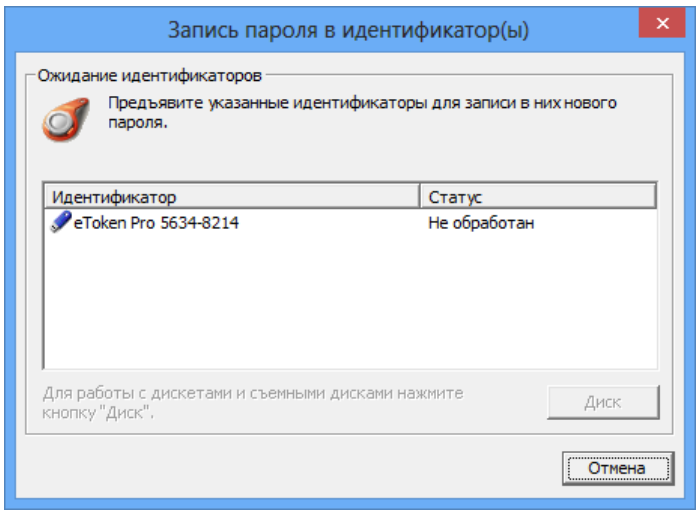
Примечание.
В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

Если введенный вами пароль правильный и хранение пароля в идентификаторе **не** предусмотрено, выполняется вход в систему.

Если введенный вами пароль правильный и его нужно записать в идентификатор вместо старого пароля, на экране появится соответствующий запрос. В этом случае выполните следующие действия:

- Нажмите кнопку "Да" в окне запроса.

  На экране появится диалог, содержащий список идентификаторов, в которые система предлагает записать новый пароль.



- Для записи пароля последовательно предъявите идентификаторы.

  Примечание.
  Если идентификатор защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

  В результате успешной записи нового пароля в идентификатор его статус в списке изменится на "Обработан". После этого идентификатор можно изъять из считывателя.

- По окончании обработки всех идентификаторов нажмите в диалоге кнопку "Закрыть".

После закрытия диалога выполняется вход в систему.

Вход в систему при полномочном разграничении доступа

Если действует механизм полномочного управления доступом (см. стр.**24**), при входе в систему осуществляется дополнительная проверка полномочий пользователя. Ограничения на вход устанавливаются в следующих случаях:

- к компьютеру подключены устройства с назначенной категорией конфиденциальности;
- включен режим контроля потоков конфиденциальной информации.

Вход при наличии устройств с категорией конфиденциальности

Администратор может назначить определенным устройствам категории конфиденциальности. Если на момент входа пользователя в систему к компьютеру подключены устройства с заданными категориями конфиденциальности, осуществляется проверка уровня допуска пользователя и категорий устройств. При обнаружении устройства, категория конфиденциальности которого выше, чем ваш уровень допуска, вход в систему запрещается с выдачей соответствующего сообщения.

Вход в режиме контроля потоков

Если в подсистеме полномочного управления доступом включен режим контроля потоков конфиденциальной информации, то после успешной проверки прав пользователя на вход в систему на экране появится диалог для выбора уровня конфиденциальности сеанса (сессии).

Выбирая уровень конфиденциальности, вы указываете системе категорию конфиденциальности документов, с которыми собираетесь работать в текущем сеансе.

При включенном режиме контроля потоков осуществляется более строгая проверка наличия устройств с заданными категориями конфиденциальности. Вход в систему запрещается в следующих случаях:

- обнаружены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя;
- обнаружены устройства с различными категориям конфиденциальности;
- обнаружены устройства с категорией конфиденциальности выше, чем категория "неконфиденциально", при конфигурационном входе в систему.

> **Примечание.**
> Конфигурационный вход в систему необходимо сделать один раз — после создания или переименования учетной записи пользователя. Такой вход должен быть выполнен в неконфиденциальной сессии.

В том случае, если к компьютеру подключено устройство, которому назначена категория конфиденциальности ниже или равная уровню допуска пользователя, вход возможен только с уровнем сессии, равным категории устройства.

Более подробную информацию о работе в системе в условиях полномочного разграничения доступа см. на стр.**28**.

Особенности входа при усиленной аутентификации

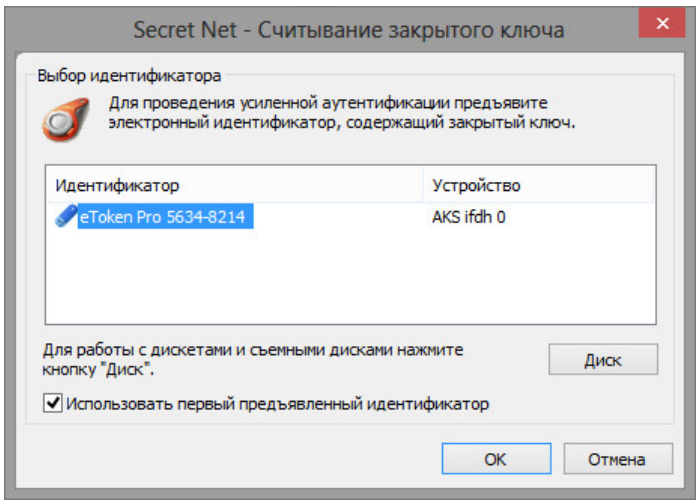
В системе Secret Net предусмотрены следующие режимы аутентификации пользователей:

Режим	Описание
Стандартная аутентификация	При входе пользователя выполняется стандартная аутентификация ОС Windows

Режим	Описание
Усиленная аутентификация по ключу	Кроме стандартной аутентификации ОС Windows, дополнительно выполняется аутентификация по ключевой информации, хранящейся на ключевом носителе пользователя (персональный идентификатор, ключевая дискета, USB-флеш-накопитель и т. п.)
Усиленная аутентификация по паролю	Кроме стандартной аутентификации ОС Windows, дополнительно выполняется аутентификация по паролю пользователя средствами системы Secret Net

При усиленной аутентификации по паролю для выполнения проверки пароль должен быть сохранен в базе данных системы Secret Net. Сохранение выполняется автоматически при смене пароля администратором, а также при смене пароля самим пользователем. Однако возможны ситуации рассинхронизации паролей пользователя, когда текущий и сохраненный пароли не совпадают. В таких случаях система выдает запросы на синхронизацию паролей.

Если в системе включен режим усиленной аутентификации по ключевой информации, сгенерированной средствами Secret Net, то при любом режиме входа в систему на экране появится диалог "Считывание закрытого ключа". Диалог не появится только в одном случае — если вход был выполнен по идентификатору, содержащему нужную ключевую информацию.



Предъявите ключевой носитель, который содержит нужный ключ.

Процедура загрузки ключевой информации зависит от вида используемого ключевого носителя (персональный идентификатор или съемный диск) и от вашей уверенности в том, с какого ключевого носителя следует провести загрузку.

Если вы используете персональный идентификатор и уверены в том, с какого идентификатора хотите загрузить ключевую информацию, — предъявите этот персональный идентификатор.

Если вы используете персональный идентификатор, но не уверены в том, с какого идентификатора хотите загрузить ключевую информацию:

- в диалоге удалите отметку из поля "Использовать первый предъявленный идентификатор";
- последовательно предъявляйте идентификаторы, пока в диалоге не появятся сведения об идентификаторе с нужным серийным номером;
- для загрузки ключевой информации нажмите кнопку "ОК".

Если вы используете в качестве ключевого носителя дискету (или другой съемный диск):

- вставьте дискету в дисковод (подключите съемный диск) и нажмите кнопку "Диск";
- выберите в списке идентификаторов нужную строку и нажмите кнопку "ОК".

Не прерывайте контакт ключевого носителя со считывателем до окончания процесса загрузки ключевой информации. После появления на экране сообщений, сопутствующих загрузке операционной системы (например, "Получение параметров пользователя"), ключевой носитель можно изъять из считывателя.

Как действовать в проблемных ситуациях

При нарушениях правил входа система защиты прерывает процедуру входа. Ниже приведены сообщения системы защиты и ОС Windows при неверных действиях пользователя или сбоях системы при входе.

Неправильное имя пользователя.
Неправильное имя пользователя или пароль.

Причина. Указанное имя пользователя отсутствует в базе данных системы или введен неправильный пароль.

Действия пользователя. Проверьте состояние переключателя регистра клавиатуры (верхний/нижний) и переключателя раскладки клавиатуры (рус./лат.).

Если допущена ошибка при вводе, повторите ввод имени и пароля. Количество попыток ввода пароля может быть ограничено администратором. Если количество попыток превышено, система выдаст об этом сообщение и заблокирует компьютер. В этом случае следует обратиться к администратору.

Если вы забыли свой пароль, обратитесь за помощью к администратору.

Вход в систему запрещен. Ошибка аутентификации Secret Net.
Неверный пароль или имя пользователя.

Причина. Включен режим усиленной аутентификации по паролю, требующий совпадения введенного пароля с паролем, который хранится в базе данных Secret Net. Введенные учетные данные не совпадают с сохраненными значениями.

Действия пользователя. Проверьте правильность ввода учетных данных (см. выше) и при необходимости повторите ввод правильных значений.

Если имя пользователя и пароль введены правильно, ситуация может быть связана с рассинхронизацией паролей. То есть в базе данных Secret Net хранится старый пароль, не обновленный после смены на новый пароль. В этом случае введите свой предыдущий пароль. На экране появится диалог "Ввод пароля", предлагающий ввести новый пароль. Для входа в систему и синхронизации паролей введите новый пароль и оставьте отметку в поле "Синхронизировать пароли".

Пароль в идентификаторе не совпадает с текущим. Хотите ли вы записать в идентификатор текущий пароль?

Причина. В персональном идентификаторе записан пароль, отличный от имеющегося в системе.

Действия пользователя. Вы можете обновить пароль в идентификаторах (см. стр. 18) или отложить выполнение этой операции. Рекомендуется обновлять пароль, не откладывая выполнение этой операции.

Персональный идентификатор пользователя не зарегистрирован на этом компьютере.
Неверный формат данных в персональном идентификаторе.
В персональном идентификаторе записан неверный пароль.
Введен неверный PIN персонального идентификатора.

Причина. При входе в систему предъявлен идентификатор, не принадлежащий входящему пользователю или не содержащий нужной информации.

Возможно, идентификатор испорчен или чтение данных из идентификатора было выполнено с ошибкой.

Действия пользователя. Повторите процедуру входа, предъявив нужный идентификатор. Добейтесь правильного контакта персонального идентификатора со считывающим устройством.

Если ошибка устойчиво повторяется, обратитесь за помощью к администратору.

Истек срок действия пароля.

Причина. При входе в систему указан пароль, срок действия которого истек. Сообщение носит предупреждающий характер.

Действия пользователя. Закройте окно сообщения и смените пароль (см. стр.**18**).

Не найден контроллер домена.
Сбой при установлении доверительных отношений между доменами.
Системная ошибка при аутентификации пользователя.
Ошибка при локальной аутентификации.

Причина. Информация, необходимая для входа в систему, указана правильно, но вход в систему невозможен из-за отсутствия в сети нужных компонентов, нарушений сетевого взаимодействия или других системных ошибок.

Действия пользователя. Выясните у администратора причину отсутствия в сети нужных компонентов и повторите попытку входа после устранения причины.

В некоторых случаях возможна работа с компьютером в автономном режиме, без доступа к сетевым ресурсам. Для продолжения работы в автономном режиме нажмите кнопку "OK".

Вход в систему запрещен. К системе подключены устройства, к которым у вас нет допуска: <список устройств с описанием>.
Для входа в систему отключите недоступные вам устройства.

Причина. К компьютеру подключены устройства, категория конфиденциальности которых выше вашего уровня допуска.

Действия пользователя. Отключите указанные устройства. При необходимости снятия запрета на использование устройств обратитесь к администратору.

Вход в систему запрещен. Конфликт категорий конфиденциальности устройств: <список устройств с описанием>.
Для входа в систему отключите конфликтующие устройства.

Причина. К компьютеру подключены устройства с разными категориями конфиденциальности, что недопустимо при работе в режиме контроля потоков.

Действия пользователя. Отключите устройства, которым назначена категория конфиденциальности, отличающаяся от нужного вам уровня конфиденциальности сессии.

К системе подключены устройства: <описание устройств>. Вход в систему возможен только с уровнем <категория конфиденциальности устройств>. Продолжить?

Причина. К компьютеру подключены устройства, которым назначена категория конфиденциальности. При работе в режиме контроля потоков уровень конфиденциальности сессии должен совпадать с этой категорией.

Действия пользователя. Чтобы открыть сессию с уровнем конфиденциальности, равным категории устройств, выберите продолжение операции. Если требуется открыть сессию с другим уровнем конфиденциальности, отключите указанные устройства.

Вход в систему запрещен. Текущий вход на данный компьютер является конфигурационным и должен быть выполнен с минимальным уровнем конфиденциальности сессии. Подключенные устройства: <список устройств с описанием>. Для входа в систему отключите устройства с повышенной категорией конфиденциальности.

Причина. Учетная запись, от имени которой выполняется вход, является новой. При работе в режиме контроля потоков для этой учетной записи требуется выполнить вход в неконфиденциальной сессии. Вход невозможно выполнить, так как к компьютеру подключены устройства с назначенной категорией конфиденциальности, отличающейся от категории "неконфиденциально".

Действия пользователя. Отключите указанные устройства и выполните вход в неконфиденциальной сессии. После входа в систему завершите текущий сеанс работы пользователя, выполнив процедуру выхода из системы, и снова подключите устройства. При следующем входе в систему вам будет доступна возможность открытия сессии с уровнем конфиденциальности, равным категории устройств.

Компьютер заблокирован системой защиты. Причины блокировки: <*сведения о причинах*>.
Для разблокирования компьютера обратитесь к администратору.

Причина. К блокировке компьютера, выполненной системой Secret Net, могут привести следующие причины: нарушения, связанные с контролем целостности защищаемых объектов, изменение аппаратной конфигурации, ошибки функционального контроля, загрузка неверной ключевой информации при усиленной аутентификации и пр.

Действия пользователя. Снять блокировку компьютера может только администратор, обратитесь к нему за помощью.

Глава 3
Защита от несанкционированного доступа к компьютеру

Временная блокировка компьютера

Если вам необходимо временно прервать работу на компьютере, то для защиты от несанкционированного использования совсем необязательно его выключать. Можно воспользоваться функцией временной блокировки компьютера, при которой блокируются клавиатура и экран монитора.

Включить режим временной блокировки можно следующими способами:

- стандартный способ с помощью клавиатуры;
- с использованием идентификатора, предъявленного для входа в систему.

Перед включением режима блокировки рекомендуется сохранить сделанные изменения в открытых документах.

Примечание.
Компьютер может перейти в режим временной блокировки автоматически, если в течение определенного времени не использовались клавиатура и мышь. Такое время называется интервалом неактивности. Активация автоматической блокировки выполняется стандартно для ОС Windows.

Для включения блокировки стандартным способом:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.
2. В появившемся стандартном диалоге нажмите кнопку "Блокировка" ("Блокировать компьютер").

Для включения блокировки с использованием идентификатора:

1. Переведите компьютер в обычный режим работы, при котором на экране отображаются рабочий стол и панель задач.
2. Извлеките из считывателя идентификатор, который был предъявлен для входа в систему.

Примечание.
Блокировка при изъятии идентификатора осуществляется, если администратор безопасности настроил для компьютера соответствующую реакцию. Функция блокировки действует в локальном сеансе работы пользователя, если идентификатор активирован средствами Secret Net и пользователь предъявил этот идентификатор для входа в систему.

Снятие временной блокировки компьютера пользователем

Разблокировать компьютер, находящийся в режиме временной блокировки, может работающий на нем пользователь или администратор безопасности.

На компьютере под управлением ОС Windows XP или Windows Server 2003:
Если разблокировку компьютера проводит администратор, то сеанс работы пользователя будет принудительно завершен с потерей несохраненных данных.

Для разблокирования компьютера стандартным способом:

1. В зависимости от операционной системы компьютера выполните соответствующее действие:
   - на компьютере с ОС Windows 8 или Windows Server 2012 — отключите экран блокировки (для этого, например, нажмите любую клавишу). На экране появится имя пользователя заблокированного сеанса и поле для ввода пароля;

- на компьютере с ОС Windows 7/Vista или Windows Server 2008 — выберите учетную запись пользователя заблокированного сеанса. На экране появится поле для ввода пароля;
- на компьютере с ОС Windows XP или Windows Server 2003 — нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>. На экране появится диалог для ввода учетных данных пользователя заблокированного сеанса.

2. Введите пароль и нажмите кнопку "→" или "OK".

Для разблокирования компьютера с использованием идентификатора:

1. Предъявите идентификатор. Если идентификатор остался подключенным к считывателю со времени включения режима блокировки, извлеките идентификатор и снова подключите его к считывателю.

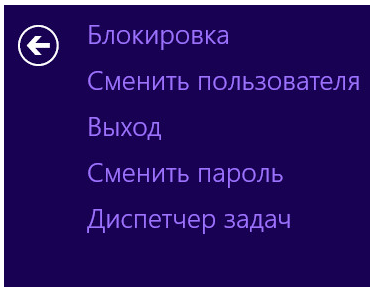
   Если в идентификаторе хранится ваш пароль, компьютер будет разблокирован. При отсутствии пароля на экране появится диалог для ввода учетных данных, где будет отображаться имя текущего пользователя.
2. Введите пароль в поле "Пароль" и нажмите кнопку "→" или "OK".

Смена пароля

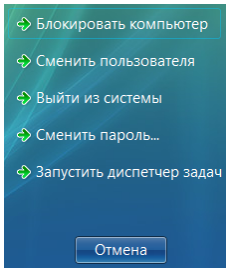
Для смены пароля:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.

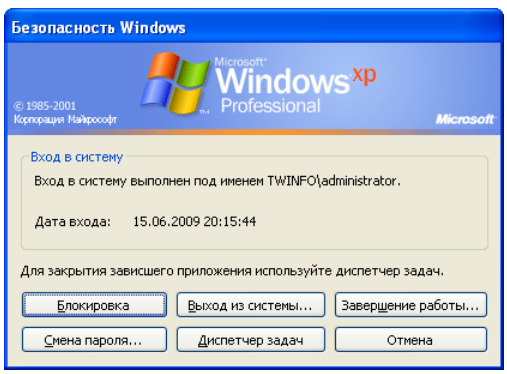
   Появится экран с оперативными командами ОС:
   - на компьютере с ОС Windows 8 или Windows Server 2012:



   - на компьютере с ОС Windows 7/Vista или Windows Server 2008:



   - на компьютере с ОС Windows XP или Windows Server 2003:

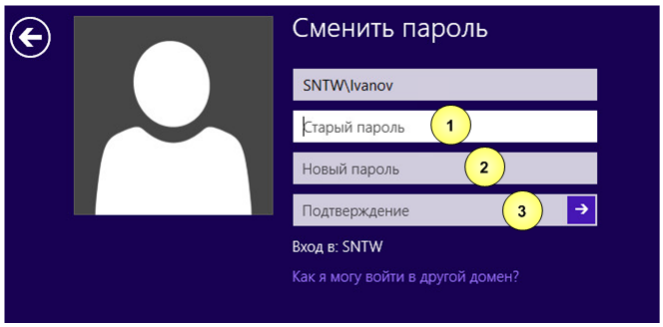


2. Нажмите кнопку "Сменить пароль" ("Смена пароля").

Если установленная политика паролей запрещает вам менять пароль, на экране появится сообщение об ошибке и процедура смены пароля будет прервана. В этом случае для смены пароля обратитесь к администратору.

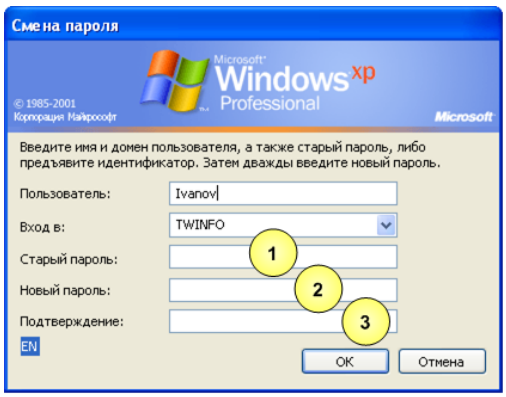
Если же вам разрешено менять пароль, то на экране появится диалог:

- на компьютере с ОС Windows 8 или Windows Server 2012:



- на компьютере с ОС Windows 7/Vista или Windows Server 2008:

- на компьютере с ОС Windows XP или Windows Server 2003:



Пояснение.
На рисунках выносками обозначены элементы: 1 — поле для ввода текущего пароля; 2 — поле для ввода нового пароля; 3 — поле для подтверждения (повторного ввода) нового пароля.

3. При необходимости измените язык ввода (сведения о текущем языке отображает индикатор ENG/РУС или EN/RU), после чего заполните поля диалога:

- в поле "Старый пароль" введите ваш текущий пароль в системе;
- в поле "Новый пароль" введите новый пароль;
- повторите ввод нового пароля в поле "Подтверждение".

Примечание.
В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

Внимание!
Если вам присвоен персональный идентификатор, для которого включен режим хранения пароля и разрешено использование для входа в комплекс "Соболь", то в этом случае пароль не должен содержать символы кириллицы. Иначе после обработки идентификатора будет утеряна возможность его использования для входа в комплекс "Соболь".

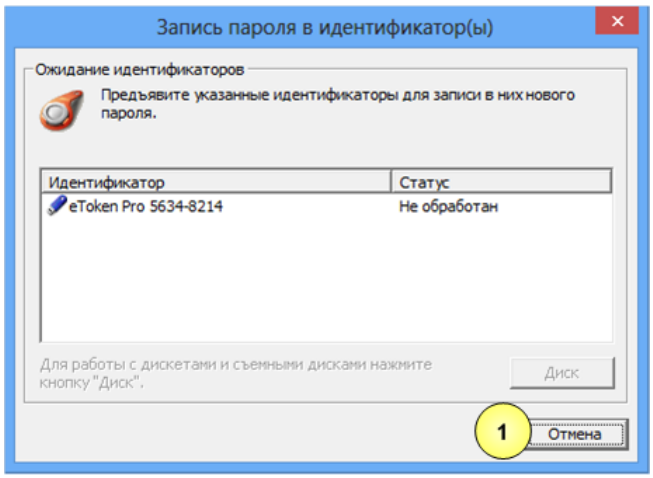
4. Нажмите кнопку "→" или "ОК".

Примечание.
Если требования, предъявляемые в системе к паролям, нарушены или старый пароль указан неправильно, на экране появится сообщение об ошибке. Нажмите кнопку "ОК" в окне сообщения и повторите ввод паролей, указав их правильно.

Если поля диалога смены пароля были заполнены правильно, на экране появится сообщение об успешном изменении пароля.

5. Нажмите кнопку "ОК".

Если ваш старый пароль хранится в персональном идентификаторе или вы используете этот идентификатор для входа в комплекс "Соболь", на экране появится диалог со списком ваших персональных идентификаторов:



Пояснение.
На рисунках выносками обозначены элементы: 1 — кнопка для отмены записи нового пароля в идентификаторы.

6. Для смены пароля или записи новой служебной информации, необходимой при входе в комплекс "Соболь", последовательно предъявите каждый идентификатор. (В случае отмены записи информации в персональный идентификатор, который используется для входа в комплекс "Соболь", вход в комплекс "Соболь" будет возможен только по старому паролю.)

Примечание.
Если идентификатор защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

В результате успешной записи нового пароля в идентификатор его статус изменится на "Обработан". После этого идентификатор можно изъять из считывателя.

7. По окончании обработки всех идентификаторов закройте диалог нажатием кнопки "Закрыть".

Работа с ключевой информацией

Ключевая информация пользователя размещается на ключевом носителе — в персональном идентификаторе, на ключевой дискете или другом съемном носителе (например, USB-флеш-накопитель). Она необходима для усиленной аутентификации при входе пользователя в систему. В данной главе приводятся сведения о работе с ключевой информацией, сгенерированной средствами системы Secret Net.

Срок действия ключевой информации устанавливается администратором. За некоторое время до окончания срока действия пользователю выдаются сообщения о необходимости смены ключевой информации. По истечении этого срока ключ становится недействительным и **не** может использоваться. Для возобновления работы с ключевой информацией необходимо ее сменить. Эта операция выполняется каждым пользователем самостоятельно.

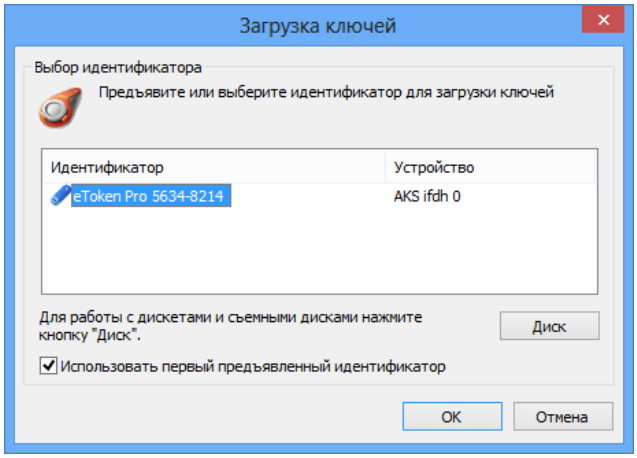
Смена ключевой информации

Смена ключевой информации на ключевом носителе возможна только по окончании минимального срока действия личной ключевой информации.

Для смены ключевой информации:

1. Вызовите контекстное меню пиктограммы Secret Net, находящейся в системной области панели задач ОС Windows, и выберите команду "Сменить ключи".

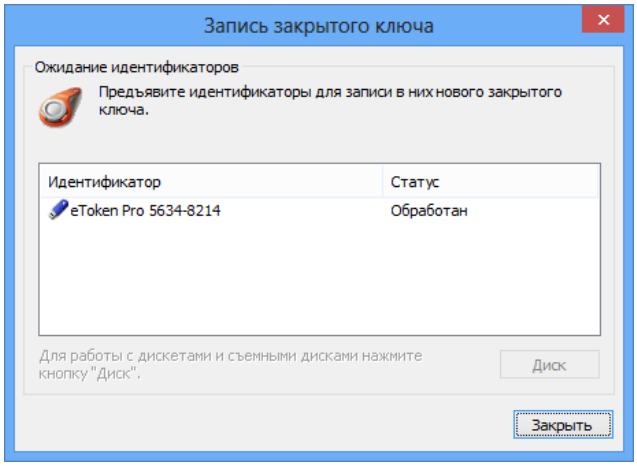
   На экране появится диалог:



2. Предъявите один из ключевых носителей, содержащий текущую ключевую информацию. В зависимости от вида ключевого носителя (персональный идентификатор или съемный диск) выполните одно из действий:
   - если вы используете персональный идентификатор, предъявите его;
   - если вы используете в качестве ключевого носителя съемный диск, вставьте дискету в дисковод, а съемный диск в разъем USB-порта, и нажмите кнопку "Диск".

   Совет.
   Если подключено несколько съемных дисков одновременно, то для продолжения процедуры выберите в списке строку с названием нужного диска и нажмите кнопку "ОК".

   Не прерывайте контакт ключевого носителя со считывателем до окончания чтения ключевой информации. Затем на экране появится диалог, содержащий список ваших ключевых носителей, в которые предлагается записать новую ключевую информацию.



3. Последовательно предъявите все ключевые носители. Если вы используете в качестве ключевого носителя съемный диск — вставьте дискету в дисковод или подключите диск к разъему USB-порта и нажмите кнопку "Диск".

   Примечание.
   Если идентификатор защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

   В результате успешной записи ключевой информации на носитель его статус в списке изменится на "Обработан". После этого ключевой носитель можно изъять из считывателя.

4. По окончании обработки всех носителей нажмите кнопку "Закрыть".

   Если не все ключевые носители были обработаны успешно, то после нажатия кнопки "Закрыть" (или "Отмена") на экране появится окно запроса.

   Для записи актуальной ключевой информации на необработанные ключевые носители нажмите кнопку "Да" и повторите действие **3**.

Как действовать в проблемных ситуациях

При нарушении правил управления ключевой информацией система защиты прерывает выполняемую операцию. Ниже приведены сообщения системы в таких случаях.

Ошибка чтения с персонального идентификатора. Повторить операцию?
Закрытый ключ не загружен.

Причина. Произошел разрыв контакта между считывающим устройством и персональным идентификатором, либо съемный диск извлечен из дисковода или отключен от USB-порта до окончания чтения.

Действия пользователя. Восстановите контакт между считывающим устройством и персональным идентификатором или вставьте дискету в дисковод, а съемный диск подключите к USB-порту. Нажмите кнопку "ОК".

Предъявленный персональный идентификатор не принадлежит текущему пользователю.
Электронный идентификатор не предъявлен.
Неизвестный тип электронного идентификатора.

Причина. Вы предъявили персональный идентификатор, принадлежащий другому пользователю.

Действия пользователя. Предъявите свой персональный идентификатор.

Срок действия ключа истек.

Причина. Истек срок действия ключевой информации, необходимой для усиленной аутентификации.

Действия пользователя. Смените ключевую информацию по запросу системы.

У пользователя нет ключа.
У пользователя отсутствует открытый ключ.
У пользователя отсутствуют электронные идентификаторы.

Причина. Администратор не выдал вам ключевой носитель с ключевой информацией.

Действия пользователя. Обратитесь за помощью к администратору.

Глава 4
Работа в условиях разграничения доступа к ресурсам

Система Secret Net располагает рядом механизмов разграничения доступа пользователей к локальным и сетевым ресурсам компьютера, которые дополняют средства, предоставляемые ОС Windows.

Механизмы разграничения доступа

Механизмы защиты, обеспечивающие разграничение доступа к ресурсам, перечислены в следующей таблице.

Механизм	Защищаемые ресурсы
Избирательное разграничение доступа	Устройства, каталоги и файлы
Полномочное разграничение доступа	Устройства, каталоги и файлы на дисках с файловой системой NTFS
Замкнутая программная среда	Исполняемые файлы на локальных дисках компьютера и подключенных сетевых дисках

Избирательное разграничение доступа

Избирательное разграничение доступа к локальным ресурсам компьютера осуществляется на основании предоставления прав доступа и привилегий пользователям.

Для разграничения доступа к каталогам и файлам на локальных дисках используется механизм дискреционного управления доступом к ресурсам файловой системы. Для дисков, портов и других устройств используется механизм разграничения доступа к устройствам.

Администратор может установить разрешения и запреты на выполнение операций с определенными ресурсами файловой системы или устройствами. Возможности по разграничению доступа зависят от типов ресурсов. Разграничение доступа пользователей не осуществляется полностью или частично для ресурсов, имеющих особую специфику использования или необходимых для функционирования компьютера. Например, не ограничивается доступ к процессору и оперативной памяти, отсутствуют некоторые возможности разграничения доступа для портов ввода/вывода, нельзя изменять разрешающие права доступа для корневого каталога системного диска и всего системного каталога.

Разграничение доступа пользователей к устройствам с назначенными категориями конфиденциальности или уровнями конфиденциальности сессий осуществляется с использованием механизма полномочного управления доступом.

Полномочное разграничение доступа

Механизм полномочного управления доступом обеспечивает:

- разграничение доступа пользователей к информации, которой назначена категория конфиденциальности (конфиденциальная информация);
- контроль подключения и использования устройств с назначенными категориями конфиденциальности;
- контроль потоков конфиденциальной информации в системе;

- контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;
- контроль печати конфиденциальных документов.

По умолчанию в системе предусмотрены следующие категории конфиденциальности: "неконфиденциально" (для общедоступной информации), "конфиденциально" и "строго конфиденциально". При необходимости администратор может увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации.

При попытке доступа пользователя (или программы, запущенной пользователем) к ресурсу сопоставляется уровень допуска пользователя с категорией конфиденциальности ресурса. Доступ к ресурсу разрешается, если его категория конфиденциальности не выше уровня допуска пользователя.

Режим контроля потоков

Подсистема полномочного управления доступом может работать в режиме контроля потоков конфиденциальной информации, который обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации.

При включенном режиме контроля потоков возможность использования устройств и доступа к конфиденциальным файлам определяется уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему (см. стр.12).

Замкнутая программная среда

При работе в условиях замкнутой программной среды администратором для каждого пользователя устанавливается перечень программ, разрешенных для запуска. При запуске программ, не входящих в перечень, в журнале регистрируются события несанкционированного доступа (НСД). Замкнутая программная среда может использоваться в "жестком" или "мягком" режимах работы.

При "жестком" режиме работы замкнутой среды пользователь может работать только с программами, включенными в перечень разрешенных ему для запуска. Запуск других программ система блокирует, предупреждая пользователя сообщением об отказе в доступе к устройству или файлу.

Если требуется расширить перечень разрешенных для запуска программ, необходимо обратиться к администратору безопасности, который обладает правом предоставлять пользователям доступ к ресурсам информационной системы.

При "мягком" режиме работы замкнутой среды запуск программ, не включенных в перечень разрешенных для запуска, не блокируется. "Мягкий" режим работы замкнутой среды используется на этапе внедрения системы Secret Net с целью сбора информации о программах, которые используют пользователи.

Что нужно знать перед началом работы

Перед началом работы в системе необходимо у администратора безопасности получить информацию о предоставленных правах для выполнения ваших должностных обязанностей. Ниже в таблице перечислены основные сведения, которые требуются при использовании различных механизмов защиты.

Механизм	Необходимая информация
Избирательное разграничение доступа	Разрешенные для доступа сетевые и локальные ресурсы (диски, каталоги, файлы, принтеры, коммуникационные порты, дисководы, приводы и пр.). Разрешенные для выполнения операции с ресурсами (просмотр, добавление, удаление и пр.). Разрешенные для подключения устройства

Механизм	Необходимая информация
Полномочное разграничение доступа	Уровень допуска к конфиденциальной информации. Предоставленные привилегии. Доступные для работы файлы, их размещение. Требования, которые необходимо соблюдать при работе с конфиденциальными документами
Замкнутая программная среда	Перечень программ, разрешенных для запуска

Как действовать в проблемных ситуациях

Настройку работы механизмов разграничения доступа выполняет администратор. Обратитесь к нему за помощью, если вам не удалось:

- запустить нужную программу;
- открыть каталог или файл;
- сохранить или удалить файл, распечатать документ;
- подключить к компьютеру нужное устройство и т. п.

Изменение прав доступа к каталогам и файлам

Если включен механизм дискреционного управления доступом к ресурсам файловой системы, для каталогов и файлов на локальных дисках компьютера действуют права доступа, контролируемые системой Secret Net. Права доступа устанавливают разрешения и запреты на выполнение определенных операций с ресурсами: чтение, запись, выполнение, удаление и изменение прав доступа.

Права могут быть заданы явно или наследоваться от вышестоящего элемента иерархии в файловой системе. Явно заданные права имеют более высокий приоритет по сравнению с наследуемыми правами.

Примечание.
Режим наследования прав доступа принудительно включается для ресурса при его перемещении в другой логический раздел или для созданной копии ресурса. В этом случае, даже если в исходном размещении для ресурса были явно заданы права доступа, в новом размещении будут действовать права от вышестоящего каталога, поскольку включается режим наследования. Если каталог или файл перемещается в пределах своего логического раздела, явно заданные права доступа сохраняются для этого объекта.

По умолчанию для всех пользователей действуют разрешающие права доступа к любым ресурсам на чтение, запись, выполнение и удаление. Изменять права доступа к ресурсам могут следующие категории пользователей:

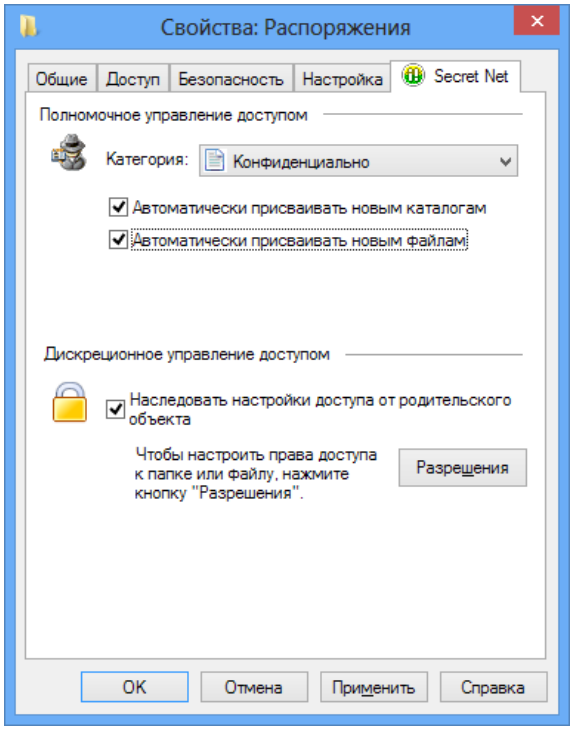
- администраторы безопасности или уполномоченные сотрудники, которым предоставлена привилегия "Управление правами доступа" — привилегия дает возможность изменять права доступа для всех ресурсов (независимо от установленных прав доступа к самим ресурсам);
- администраторы ресурса — пользователи, для которых установлено разрешение на изменение прав доступа к этому ресурсу.

Первоначальное назначение администраторов ресурсов осуществляет пользователь с привилегией "Управление правами доступа". Далее администраторы ресурсов управляют правами доступа для соответствующих ресурсов, устанавливая разрешения и запреты на выполнение операций остальными пользователями.

Процедура выполняется с использованием программы "Проводник" ОС Windows.

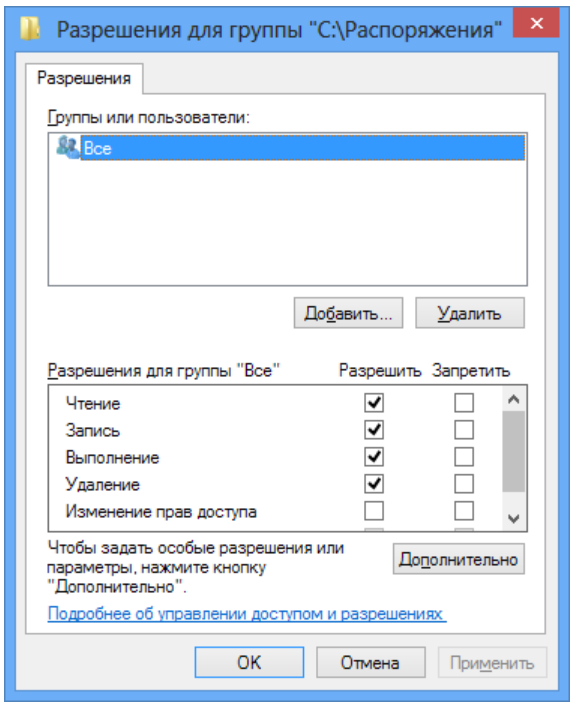
Для изменения прав доступа к ресурсу:

1. В программе "Проводник" вызовите контекстное меню ресурса (каталога или файла) и выберите команду "Свойства". В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".



2. Если установлена отметка в поле "Наследовать настройки доступа от родительского объекта" (то есть для ресурса включен режим наследования прав), удалите отметку из поля, чтобы явно указать права доступа. Если отметка отсутствует или необходимо ознакомиться с наследуемыми правами доступа — нажмите кнопку "Разрешения".

   На экране появится диалог ОС Windows "Разрешения...". В диалоге используются те же методы работы, как в аналогичных стандартных средствах ОС Windows.



3. При необходимости отредактируйте список учетных записей в верхней части диалога с помощью кнопок "Добавить" и "Удалить".
4. Для изменения параметров доступа выберите в списке нужную учетную запись и затем расставьте разрешения и запреты на выполнение операций. Если требуется получить дополнительные сведения (например, об источнике

наследуемых параметров) или настроить особые параметры (включая параметры аудита операций с ресурсом) — нажмите кнопку "Дополнительно" и выполните нужные действия в появившемся окне дополнительных параметров безопасности ОС Windows.

5. По окончании настройки закройте ранее открытые диалоги с помощью кнопки "ОК".

Правила работы с конфиденциальными ресурсами

Полномочное разграничение доступа пользователей к ресурсам с назначенными категориями конфиденциальности основано на следующем подходе:

- каталогам и файлам на дисках с файловой системой NTFS, а также устройствам назначаются категории конфиденциальности (по умолчанию в системе представлены категории "неконфиденциально", "конфиденциально" и "строго конфиденциально");
- каждому пользователю назначается один из возможных уровней допуска к конфиденциальной информации. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов;
- доступ пользователя к ресурсу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности ресурса. Например, пользователь с уровнем допуска "конфиденциально" имеет доступ только к файлам категорий "конфиденциально" и "неконфиденциально".

Ниже в таблице сопоставлены правила работы механизма полномочного управления доступом, действующие при отключенном и включенном режиме контроля потоков конфиденциальной информации.

Без контроля потоков	**При контроле потоков**
Доступ к устройствам	
Запрещен вход пользователя в систему, если подключены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя	Запрещен вход пользователя в систему, если подключены устройства: • с категорией конфиденциальности выше, чем уровень допуска пользователя; • с различными категориями конфиденциальности; • с категорией конфиденциальности выше, чем категория "неконфиденциально", при первом входе пользователя на данном компьютере (конфигурационный вход)
Запрещено подключение устройства, если его категория конфиденциальности выше, чем уровень допуска работающего пользователя	Запрещено подключение устройства, если его категория конфиденциальности отличается от уровня сессии работающего пользователя
Разрешено функционирование всех сетевых интерфейсов	Запрещено использование сетевых интерфейсов, для которых текущий уровень конфиденциальности сессии не указан в списке разрешенных уровней
Отсутствуют ограничения по доступу к устройствам, для которых включен режим доступа "без учета категории конфиденциальности"	
Доступ к файлам	
Если задана категория конфиденциальности для устройства, содержащего файл, при доступе к этому файлу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности файла	
Запрещен доступ к файлу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего файл	

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><td>Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла</td><td>Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла</td></tr>
<tr><td>Запрещено удаление конфиденциального файла с помещением в "Корзину"</td><td>Запрещено удаление любого файла с помещением в "Корзину"</td></tr>
<tr><td colspan="2">Доступ к каталогам</td></tr>
<tr><td colspan="2">Если задана категория конфиденциальности для устройства, содержащего каталог, при доступе к этому каталогу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности каталога</td></tr>
<tr><td colspan="2">Запрещен доступ к каталогу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего каталог</td></tr>
<tr><td colspan="2">Конфиденциальные файлы размещаются в каталогах, имеющих категорию конфиденциальности не ниже категории конфиденциальности файла. Например, в каталоге с категорией "конфиденциально" могут размещаться как неконфиденциальные файлы, так и файлы с категорией "конфиденциально"</td></tr>
<tr><td colspan="2">Пользователь, не имеющий доступ к файлу, может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть файл. Поэтому названия конфиденциальных файлов не должны содержать конфиденциальную информацию</td></tr>
<tr><td>Запрещено удаление конфиденциального каталога с помещением в "Корзину"</td><td>Запрещено удаление любого каталога с помещением в "Корзину"</td></tr>
<tr><td colspan="2">Наследование категории конфиденциальности каталога</td></tr>
<tr><td>Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении (перезаписи), копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога</td><td>Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении, копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога.
Ограничение: устанавливаемая категория конфиденциальности должна быть равна текущему уровню конфиденциальности сессии</td></tr>
<tr><td>Если отключен режим автоматического присвоения категории конфиденциальности:
при создании, сохранении или копировании подкаталогу/файлу присваивается категория "неконфиденциально";
при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности вышестоящего каталога). Для перемещения подкаталогов требуется соответствующая привилегия пользователя</td><td>Если отключен режим автоматического присвоения категории конфиденциальности:
при создании, сохранении или копировании подкаталогу/файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога;
при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение подкаталога/файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога и уровень конфиденциальности сессии)</td></tr>
</table>

Без контроля потоков	При контроле потоков
Каталоги с отключенным режимом автоматического присвоения категории конфиденциальности целесообразно использовать для хранения файлов с различными категориями конфиденциальности (меньшими или равными категории конфиденциальности каталога). Чтобы исключить неожиданное изменение категорий конфиденциальности файлов после выполнения операций с ними, рекомендуется использовать каталоги, для которых установлено одинаковое состояние режима автоматического присвоения категории	
Работа в приложениях	
Приложению присваивается уровень конфиденциальности, равный наивысшей категории конфиденциальности среди открытых в приложении файлов. Уровень конфиденциальности приложения не снижается после закрытия конфиденциального файла и сохраняется до закрытия приложения	Приложению присваивается уровень конфиденциальности, равный текущему уровню сессии пользователя. Разрешается открывать файлы не выше этого уровня. Категория файлов с более низким уровнем конфиденциальности повышается до уровня конфиденциальности сессии (повышение категории происходит при сохранении файла)
Некоторые приложения при запуске автоматически обращаются к определенным файлам. Например, к ранее открывавшимся файлам в приложении. При этом не происходит непосредственное открытие файла (документа). В силу особенностей механизма полномочного управления доступом при таких обращениях к конфиденциальным файлам пользователю предлагается повысить уровень конфиденциальности приложения до категории файлов. В таких случаях, если не планируется работать с предложенным уровнем конфиденциальности, достаточно отказаться от повышения уровня конфиденциальности приложения	
Изменение категории конфиденциальности ресурса	
Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше своего уровня допуска (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)	Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше уровня конфиденциальности сессии (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)
Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше уровня допуска пользователя; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше уровня допуска пользователя; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше уровня допуска пользователя	Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше текущего уровня сессии; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше текущего уровня сессии; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше текущего уровня сессии
Печать конфиденциальных документов	

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><td>Если включен режим контроля печати:
пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы;
пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей уровень допуска пользователя</td><td>Если включен режим контроля печати:
пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (если документ не редактировался);
пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей текущий уровень сессии</td></tr>
<tr><td colspan="2">Если отключен режим контроля печати конфиденциальных документов, любому пользователю, имеющему доступ к конфиденциальным документам, разрешен вывод этих документов на печать независимо от наличия у него привилегии "Печать конфиденциальных документов". При этом документы распечатываются без грифа конфиденциальности</td></tr>
<tr><td colspan="2">При включенном режиме контроля печати конфиденциальные документы можно выводить на печать в любых приложениях, использующих стандартные методы настройки параметров печати (например, MS Word или MS Excel). При выводе на печать документы автоматически маркируются (добавляется гриф)</td></tr>
<tr><td colspan="2">Вывод на внешние носители</td></tr>
<tr><td>Пользователь, имеющий доступ к конфиденциальным документам, может копировать файлы или сохранять их содержимое на любые носители независимо от наличия привилегии "Вывод конфиденциальной информации"</td><td>Пользователь, не обладающий привилегией "Вывод конфиденциальной информации", не может копировать конфиденциальные файлы или сохранять их содержимое на внешние носители.
Устройство считается внешним носителем, если для него включен режим доступа "без учета категории конфиденциальности" и файловая система для хранения данных отличается от NTFS</td></tr>
</table>

Управление конфиденциальными ресурсами

Доступ к содержимому конфиденциального файла предоставляется пользователю, если категория конфиденциальности файла не превышает уровень допуска пользователя. При этом категория конфиденциальности, заданная для устройства, на котором располагается файл, также анализируется и имеет более высокий приоритет по сравнению с категорией конфиденциальности файла. Если категория файла ниже категории конфиденциальности устройства — система считает категорию файла равной категории устройства. При обратной ситуации, когда категория файла превышает категорию конфиденциальности устройства, такое состояние расценивается как некорректное, и доступ к файлу запрещается.

Присвоение пользователям уровней допуска и назначение категорий конфиденциальности устройствам осуществляет администратор. Пользователь в пределах своих полномочий может изменять категории каталогов и файлов.

Изменение категорий конфиденциальности каталогов и файлов

Возможность назначения категории конфиденциальности для каталогов и файлов поддерживается на дисках с файловой системой NTFS.

Для изменения категории конфиденциальности каталога или файла вы должны обладать привилегией "Управление категориями конфиденциальности". Если у вас нет такой привилегии, вы можете только повышать категории для файлов, но не выше своего уровня допуска или уровня конфиденциальности сеанса (при

этом повышение категории файла возможно, если его категория конфиденциальности ниже, чем категория каталога).

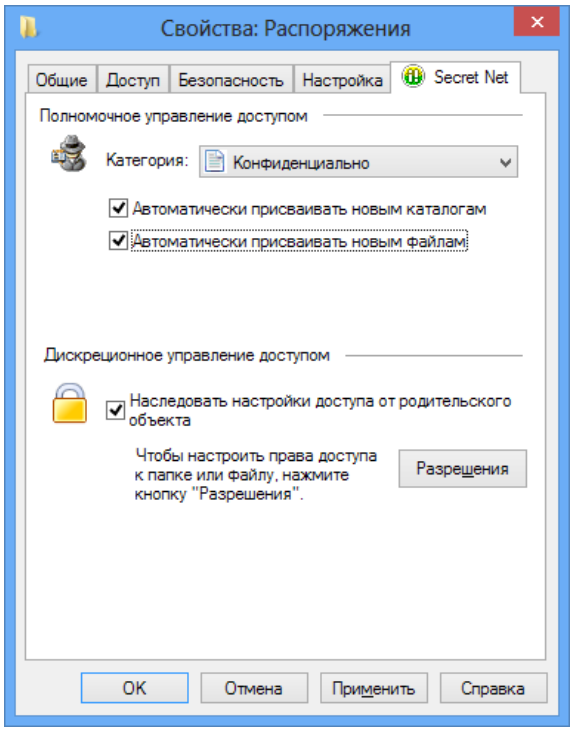
Внимание! Учитывайте следующие общие рекомендации:

- категории конфиденциальности, отличающиеся от самой низшей категории (по умолчанию — "неконфиденциально"), не следует присваивать системным каталогам, каталогам, в которых размещается прикладное программное обеспечение, а также каталогу "Мои документы" и всем подобным ему;
- во избежание непроизвольного повышения категорий конфиденциальности файлов храните файлы в каталогах с категорией конфиденциальности, равной категории конфиденциальности файлов. При этом учитывайте категорию конфиденциальности устройства, на котором располагаются эти объекты, так как категория устройства имеет более высокий приоритет.

Процедура выполняется с использованием программы "Проводник" ОС Windows.

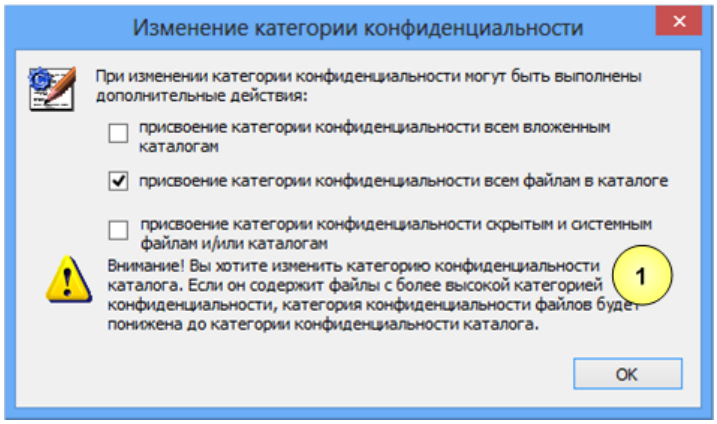
Для изменения категории конфиденциальности каталогов:

1. В программе "Проводник" вызовите контекстное меню каталога (группы выбранных каталогов) и выберите команду "Свойства". В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".



2. Укажите необходимые значения параметров:
   - Выберите в раскрывающемся списке поля "Категория" нужную категорию конфиденциальности.
   - Чтобы выбранная категория в дальнейшем автоматически присваивалась создаваемым подкаталогам и/или файлам, установите отметки в полях "Автоматически присваивать новым каталогам" и/или "Автоматически присваивать новым файлам".
3. Нажмите кнопку "OK".

   Если в каталоге (каталогах) имеются файлы и подкаталоги, на экране появится диалог, предлагающий изменить категории конфиденциальности файлам и подкаталогам:



Пояснение.
На рисунке выносками обозначены элементы: 1 — предупреждение, выводимое в тех случаях, когда категория каталога понижается.

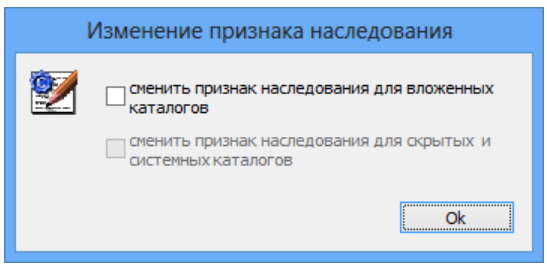
- Если требуется присвоить подкаталогам выбранную категорию конфиденциальности, а также изменить для подкаталогов состояние параметров "Автоматически присваивать новым каталогам" и "Автоматически присваивать новым файлам", отметьте поле "присвоение категории конфиденциальности всем вложенным каталогам".
- Если требуется, чтобы всем вложенным файлам (за исключением скрытых и системных) была присвоена выбранная для каталога категория конфиденциальности, отметьте поле "присвоение категории конфиденциальности всем файлам в каталоге". При наличии отметки в первом поле действие будет выполнено и для файлов, находящихся в подкаталогах.
- Если требуется, чтобы категория конфиденциальности была также присвоена скрытым и системным файлам, отметьте поле "присвоение категории конфиденциальности скрытым и системным файлам".

Внимание!
Во избежание нарушений в работе системы без особой необходимости не рекомендуется присваивать скрытым и системным файлам категории конфиденциальности, отличающиеся от самой низшей категории (по умолчанию — "неконфиденциально").

- Нажмите кнопку "OK".

Пояснение.
Если в каталоге и подкаталогах имеются файлы, категория конфиденциальности которых выше назначаемой каталогу, то категории конфиденциальности таких файлов будут автоматически понижены до категории конфиденциальности, назначаемой каталогу.

Если для каталога, содержащего подкаталоги, изменено значение параметра "Автоматически присваивать новым каталогам" или "Автоматически присваивать новым файлам", а категория конфиденциальности каталога осталась прежней, на экране появится диалог:

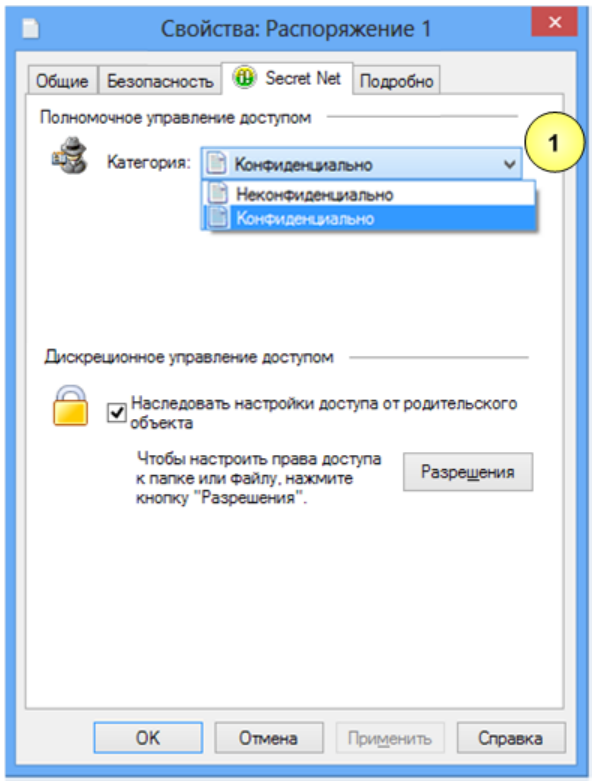


- Если требуется изменить для подкаталогов состояние параметров "Автоматически присваивать новым каталогам" и "Автоматически присваивать новым файлам", отметьте поле "сменить признак наследования для вложенных каталогов".

- Если требуется изменить состояние параметров "Автоматически присваивать новым каталогам" и "Автоматически присваивать новым файлам" также и для скрытых и системных каталогов, установите отметку в поле второго выключателя.
- Нажмите кнопку "OK".

Для изменения категории конфиденциальности файлов:

1. В программе "Проводник" вызовите контекстное меню файла (группы выбранных файлов) и выберите команду "Свойства". В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".



Пояснение.
На рисунке выносками обозначены элементы: 1 — поле со списком тех категорий конфиденциальности, которые могут быть присвоены файлу данным пользователем в данном каталоге.

2. Выберите в раскрывающемся списке поля "Категория" нужную категорию конфиденциальности файла (файлов).
3. Нажмите кнопку "OK".

Работа с конфиденциальным документом

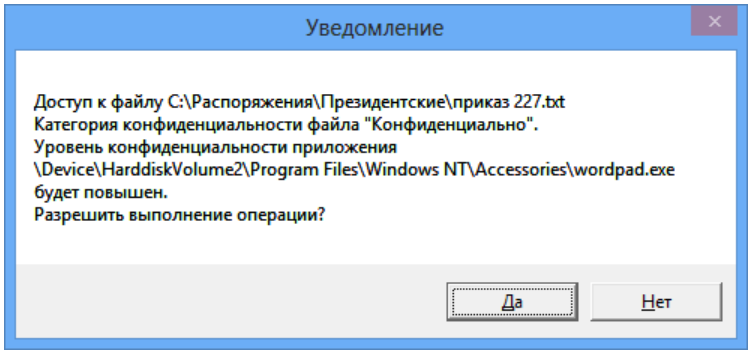
Прежде чем начать работу с конфиденциальными документами в программе редактирования (например, MS Word), рекомендуется сохранить и закрыть все ранее открытые неконфиденциальные документы.

Открытие документа

Для открытия конфиденциального документа:

1. Запустите программу редактирования документов.
2. Выберите в программе команду открытия файла и в стандартном диалоге "Открытие документа" выберите конфиденциальный документ.

   Если контроль потоков конфиденциальной информации отключен, на экране появится сообщение:



Подобный запрос выводится всякий раз, когда открывается документ с категорией конфиденциальности выше уровня конфиденциальности приложения.

3. Нажмите кнопку "Да" для открытия документа.

Сохранение документа

При сохранении конфиденциального документа под тем же или под другим именем необходимо учитывать, что категория конфиденциальности файла документа всегда остается прежней, если документ сохраняется в каталоге, категория конфиденциальности которого равна категории документа, и для каталога включен режим "Автоматически присваивать новым файлам".

Внимание!

Для сохранения категории конфиденциальности документа рекомендуется сохранять его в каталоги не ниже категории конфиденциальности документа. Иначе возможны такие ситуации:

- если документ сохраняется в каталог с более низкой категорией конфиденциальности и для каталога включен режим "Автоматически присваивать новым файлам", то категория конфиденциальности документа понижается до категории конфиденциальности каталога;
- если документ сохраняется в неконфиденциальный каталог или в конфиденциальный каталог, для которого отключен режим "Автоматически присваивать новым файлам", то файлу документа присваивается категория конфиденциальности "неконфиденциально".

Печать документа с маркером системы Secret Net

Если в Secret Net включен режим маркировки документов при печати, то в распечатываемые документы автоматически могут добавляться специальные маркеры (грифы), содержащие сведения о документе.

Маркер представляет собой набор из полей данных, которые могут быть помещены на каждой странице документа (над текстом и под текстом), а также в конце распечатанного документа. Исходные маркеры, предусмотренные в системе, можно оформить в соответствии с требованиями вашей организации.

В маркерах используются поля следующих типов:

- обязательные поля, которые заполняются системой автоматически (например, "Дата", "Файл");
- настраиваемые поля, которые заполняются пользователем перед отправкой документа на печать (например, "Учетный номер").

Для печати документа с маркером:

1. Откройте документ в программе редактирования.
2. Выберите в программе команду печати документа.

   На экране появится стандартный диалог для определения параметров печати.
3. Настройте параметры и нажмите кнопку отправки на печать.

   На экране появится диалог для ввода значений в настраиваемые поля маркера.
4. Задайте значения полей и нажмите кнопку "OK".

Документ будет распечатан вместе с маркером.

Оповещения о несанкционированном доступе

Система Secret Net может оповещать пользователя компьютера о возникновении событий, имеющих признаки несанкционированного доступа (к компьютеру, к ресурсам и пр.). В качестве локального оповещения осуществляется подача звукового сигнала и кратковременный вывод пиктограммы предупреждения в правом верхнем углу экрана.

Администратор по своему усмотрению может сам включить или отключить режим локального оповещения или предоставить возможность управления режимом пользователям.

Для включения или отключения режима локального оповещения:

- Вызовите контекстное меню пиктограммы Secret Net, находящейся в системной области панели задач ОС Windows, и выберите команду "Уведомления об НСД". Если слева от команды отображается отметка, это означает, что оповещение о несанкционированном доступе включено.

Примечание.
Если администратор включил или отключил режим локального оповещения для всех пользователей компьютера, возможность изменения состояния режима недоступна для пользователя.