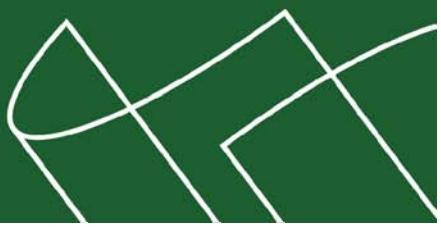
Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6



Руководство пользователя

RU.88338853.501410.007 92

Почтовый адрес:	**127018, г. Москва, ул. Сущёвский Вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Введение

Данное руководство предназначено для пользователей компьютеров с установленным программным обеспечением изделия "Средство защиты информации Secret Net 6" RU.88338853.501410.007 (далее — система Secret Net 6, Secret Net 6).

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) 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. Некоторые примечания могут и 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, брелока и т. п. 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 и hotline@infosec.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@infosec.ru).

Глава 1
Общие сведения

Что нужно знать

Система Secret Net 6 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, USB-ключ 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. Таким ключевым носителем может быть, например, персональный идентификатор, ключевая дискета, Flash-карта, USB Flash-накопитель.

Имя	Для идентификации пользователя
Пароль	Для проверки подлинности пользователя
Персональный идентификатор	Для идентификации пользователя, хранения пароля и ключевой информации, необходимой для входа в систему, когда включен режим усиленной аутентификации
Ключевая дискета, Flash-карта, USB Flash-накопитель	Для хранения ключевой информации, необходимой для входа в систему, когда включен режим усиленной аутентификации

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
Вход в систему

На компьютере, защищенном Secret Net 6, предусмотрены 2 режима аутентификации пользователей:

Режим	Описание
Стандартная аутентификация	Выполняется по паролю пользователя
Усиленная аутентификация	Вначале выполняется аутентификация по ключевой информации, хранящейся на ключевом носителе пользователя (персональный идентификатор, ключевая дискета, USB Flash-накопитель и т. п.), а затем — стандартная

Существует несколько способов входа пользователя в систему. Выбор способа зависит от оснащенности системы защиты средствами аппаратной поддержки и наличия у пользователей персональных идентификаторов (см. табл. ниже).

Режим	Способ входа в систему	Условия применения
Стандартный	Только стандартный способ входа в ОС Windows (см. стр. 7)	В системах, не оснащенных аппаратными средствами контроля входа
Только по идентификатору	Только с предъявлением персонального идентификатора (см. стр. 7)	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 6 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 6, 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 — USB-ключи eToken, iKey, Rutoken или идентификаторы 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. Идентификатор iButton необходимо приложить к считывателю, а USB-ключ надо вставить в разъем USB-порта.

Для доступа к памяти USB-ключа необходимо указывать специальный пароль — PIN-код. По умолчанию USB-ключ защищен "стандартным" PIN-кодом, который задан производителем устройства. Если стандартный PIN-код не изменен, система Secret Net 6 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.

Не забывайте PIN-код, его утрата делает невозможным дальнейшее использование USB-ключа.

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

Варианты входа в систему

Стандартный режим входа

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

Для входа в стандартном режиме:

1. В зависимости от операционной системы компьютера, при появлении экрана приветствия (приглашение на вход в систему) выполните соответствующее действие:
   - на компьютере с ОС Windows Vista/2008/7 — активируйте учетную запись с именем нужного пользователя или активируйте элемент "Другой пользователь";
   - на компьютере с ОС Windows 2000/XP/2003 — нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.

   На экране появится диалог для ввода учетных данных пользователя.
2. Укажите ваши учетные данные:
   - при необходимости введите имя пользователя в поле "Пользователь";
   - введите пароль пользователя в поле "Пароль" или оставьте это поле пустым, если вам разрешено входить в систему без пароля.

   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 6, система автоматически определяет имя пользователя, которому присвоен идентификатор.

Для входа по идентификатору:

1. При появлении экрана приветствия (приглашение на вход в систему) предъявите свой персональный идентификатор.

   Если в качестве идентификатора используется USB-ключ, который 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".

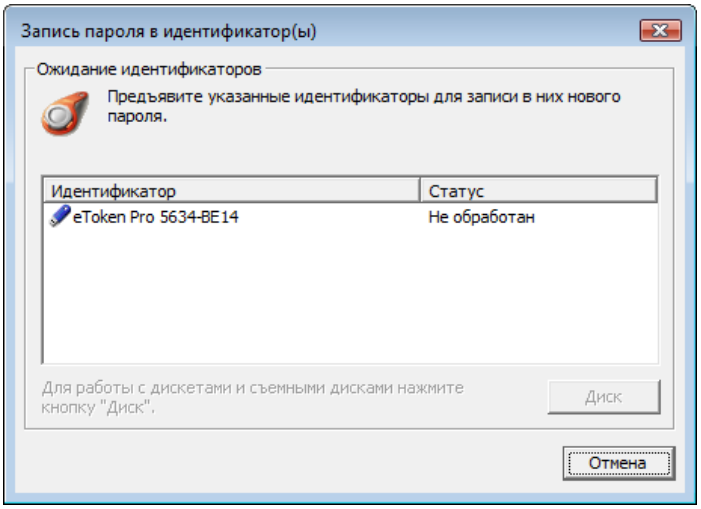
В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

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.

  Если в качестве идентификатора используется USB-ключ, который защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

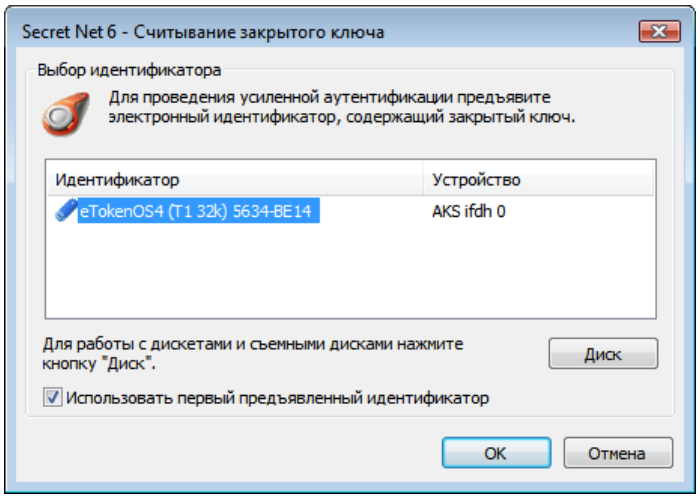
  В результате успешной записи нового пароля в идентификатор его статус в списке изменится на "Обработан". После этого идентификатор можно изъять из считывателя.

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

После закрытия диалога выполняется вход в систему.

Особенности входа при усиленной аутентификации

Если в системе включен режим усиленной аутентификации по ключевой информации, сгенерированной средствами Secret Net 6, 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.

Вход в режиме контроля потоков

Если в подсистеме полномочного разграничения доступа включен режим контроля потоков конфиденциальной информации, то при любом режиме входа в систему (стандартном, смешанном или по идентификатору) после успешной проверки прав пользователя на вход в систему на экране появится диалог для выбора уровня конфиденциальности сеанса.

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

Более подробная информация о работе подсистемы полномочного разграничения доступа содержится в разделе **"Правила работы с конфиденциальными ресурсами"** (см. стр. 21).

Вход в систему при использовании комплекса "Соболь"

Если на компьютере установлен программно-аппаратный комплекс "Соболь", который функционирует в режиме интеграции с системой Secret Net 6, загрузка компьютера и вход пользователя в систему могут выполняться с использованием одного персонального идентификатора.

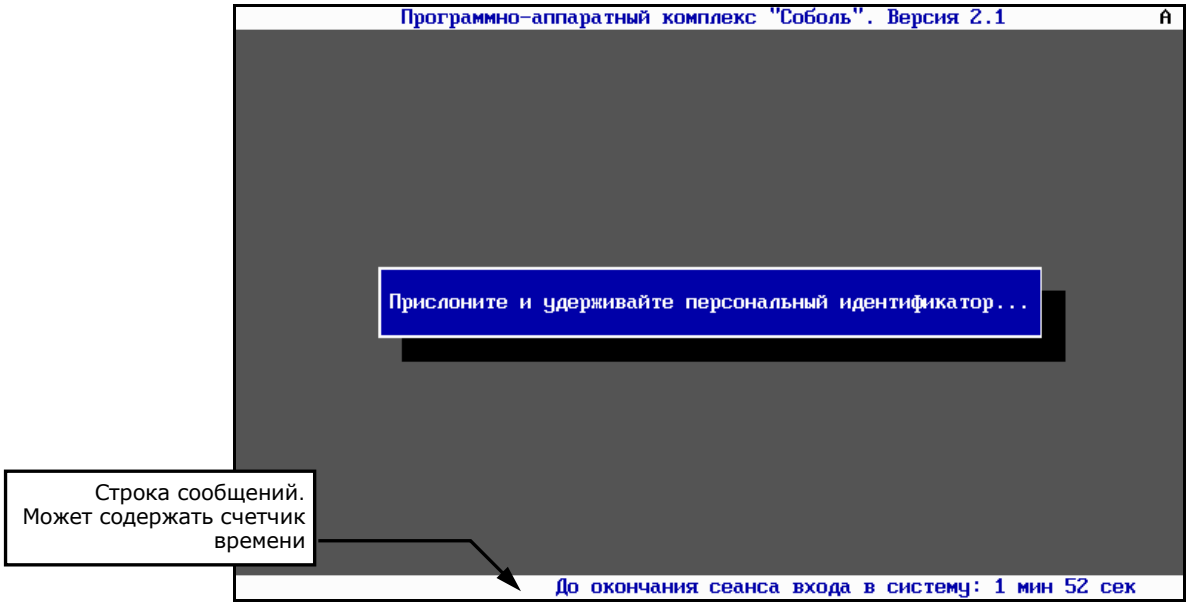
В этом случае ваши действия зависят от того, записан ли в идентификатор пароль пользователя и является ли этот пароль актуальным для ОС Windows:

- 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:



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 для 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".

  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.

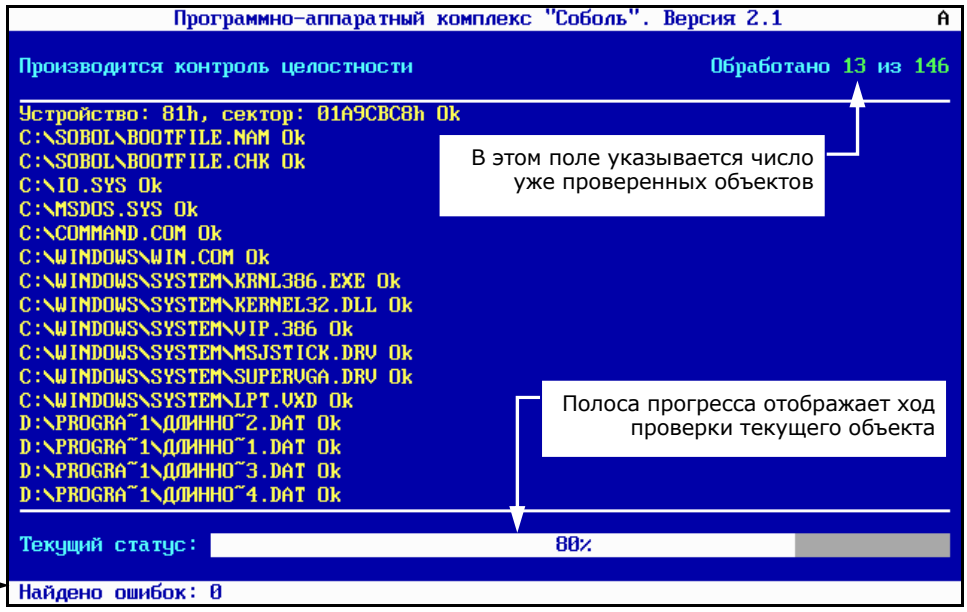
- Нажмите клавишу <Enter>.

  Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и повторите еще раз действие **2**. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.

Учитывайте, что число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение в текущем сеансе входа, тогда 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. Нажмите любую клавишу. Для перезагрузки компьютера еще раз нажмите любую клавишу. 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".

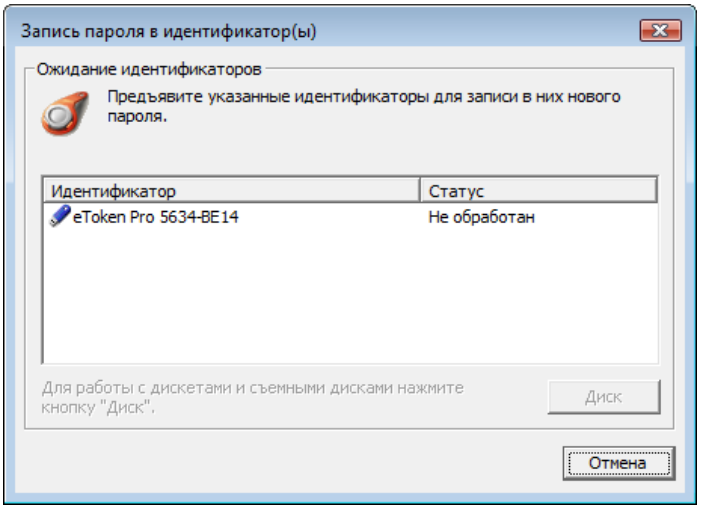
В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

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

Если введенный вами пароль правильный и 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.

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. Там же указаны причины их появления и рекомендуемые действия пользователя.

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.

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. 13) 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. 13).

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".

Компьютер заблокирован системой защиты. Причины блокировки: … . Для разблокирования компьютера обратитесь к администратору.

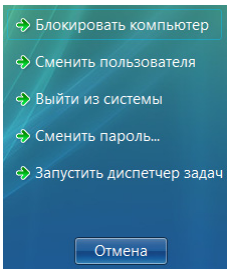
Причина. К блокировке компьютера, выполненной системой Secret Net 6, могут привести следующие причины: нарушения, связанные с контролем целостности защищаемых объектов, изменение аппаратной конфигурации, ошибки функционального контроля, загрузка неверной ключевой информации при усиленной аутентификации и пр.

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

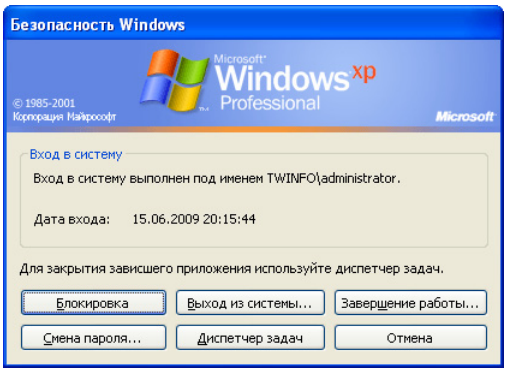
Смена пароля

Для смены пароля:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.
   На экране появится диалог:
   - на компьютере с ОС Windows Vista/2008/7:



- на компьютере с ОС Windows 2000/XP/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 за помощью к администратору.

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

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

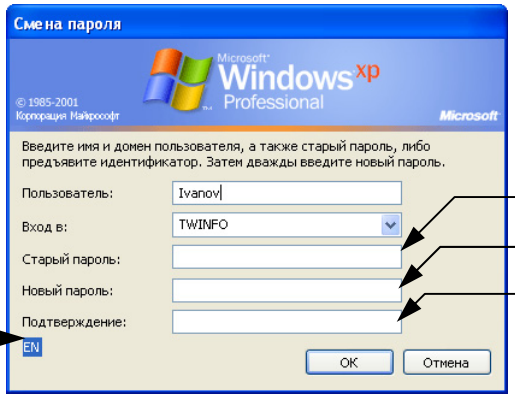
Введите текущий пароль

Введите новый пароль

Повторно введите новый пароль

При вводе пароля обратите внимание на состояние индикатора EN/RU

- на компьютере с ОС Windows 2000/XP/2003:



Введите текущий пароль

Введите новый пароль

Повторно введите новый пароль

При вводе пароля обратите внимание на состояние индикатора EN/RU

3. 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".

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 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".

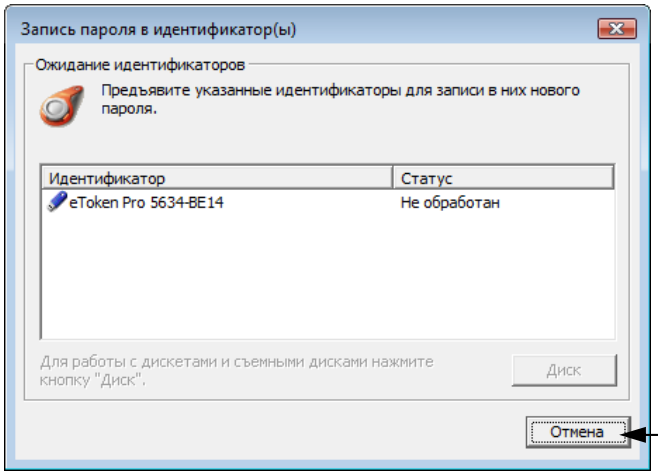
4. Нажмите кнопку "→" или "ОК".

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:



Если требуется отказаться от записи нового пароля в идентификаторы, нажмите эту кнопку

Пояснение. В случае отказа от записи информации в персональный идентификатор, который используется для входа в комплекс "Соболь", вход в комплекс "Соболь" будет возможен только по старому паролю.

6. Для смены пароля или записи новой служебной информации, необходимой при входе в комплекс "Соболь", последовательно предъявите каждый идентификатор.

Если в качестве идентификатора используется USB-ключ, который 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".

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 блокируется клавиатура и экран монитора.

Заблокировать компьютер можно вручную (см. ниже).

Автоматическая блокировка компьютера включается в том случае, если в течение определенного времени не использовались клавиатура и мышь. Такое время называется интервалом неактивности. Активация механизма автоматической блокировки выполняется стандартными средствами ОС Windows.

Для временной блокировки компьютера вручную:

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

   Компьютер будет заблокирован, а на экране появится соответствующее сообщение.

Если предварительно был настроен механизм автоматической блокировки, то по истечении времени, равного заданному интервалу неактивности, на экране заблокированного компьютера появится выбранная заставка.

Разблокировать компьютер может только работающий на нем пользователь или администратор безопасности.

На компьютере под управлением ОС Windows 2000/XP/2003: если разблокировку компьютера проводит администратор, то сеанс работы пользователя будет принудительно завершен с потерей несохраненных данных.

Для разблокирования компьютера:

Вариант 1

Если вам выдан персональный идентификатор, предъявите его.

Компьютер будет разблокирован, если в идентификаторе есть пароль. Если в персональном идентификаторе отсутствует пароль, введите его с клавиатуры в появившемся на экране диалоге и нажмите кнопку "→" или "OK".

Вариант 2

1. В зависимости от операционной системы компьютера выполните соответствующее действие:
   - на компьютере с ОС Windows Vista/2008/7 — активируйте учетную запись с именем текущего пользователя;
   - на компьютере с ОС Windows 2000/XP/2003 — нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.

   На экране появится диалог для ввода учетных данных пользователя, где будет отображаться имя текущего пользователя.
2. Введите пароль в поле "Пароль" и нажмите кнопку "→" или "OK".

Глава 3
Работа с ключевой информацией

Ключевая информация пользователя размещается на ключевом носителе — в персональном идентификаторе, на ключевой дискете или другом съемном носителе (например, USB Flash-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 6.

Срок действия ключевой информации устанавливается администратором. За некоторое время до окончания срока действия ключевой информации при каждой ее загрузке будет появляться сообщение о том, что ключевую информацию необходимо сменить. По истечении этого срока ключ становится недействительным и не может быть загружен в систему. Для возобновления работы с ключевой информацией необходимо ее сменить. Эта операция выполняется каждым пользователем самостоятельно (см. стр. 17).

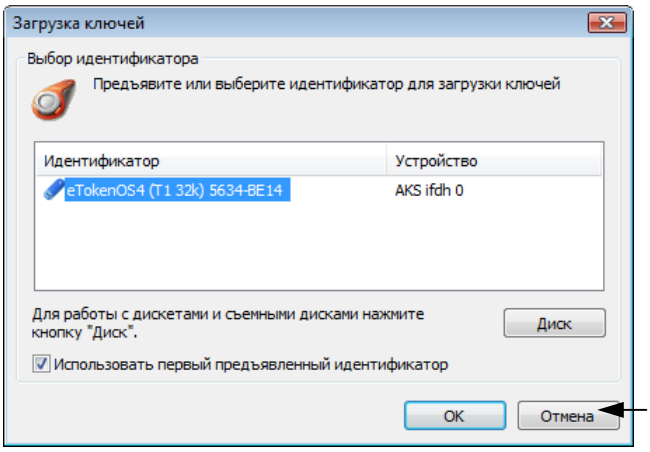
Смена ключевой информации

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 6, находящейся в системной области панели задач ОС Windows, и активируйте команду "Сменить ключи".

   На экране появится диалог:

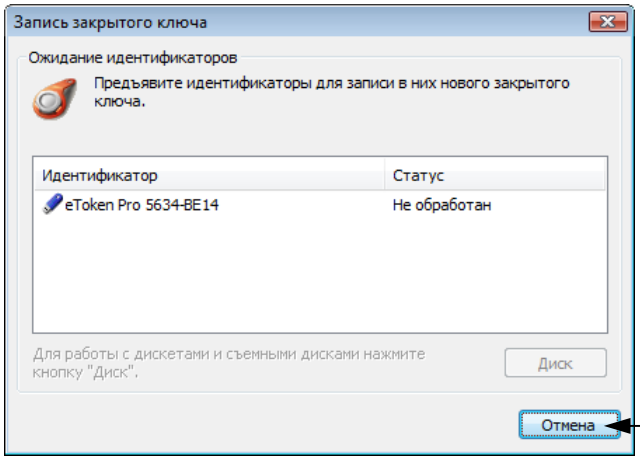


Если требуется отказаться от смены ключей, нажмите эту кнопку

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 загрузки ключевой информации. По окончании загрузки на экране появится диалог, который содержит список ваших ключевых носителей, в которые предлагается записать новую ключевую информацию.



Нажатие этой кнопки приведет к отказу от записи новой ключевой информации на носители

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".

   Если в качестве идентификатора используется USB-ключ, который 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 и выдает сообщение. Причины прерывания и ваши действия по их устранению приведены в следующей таблице.

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

Причина. Произошел разрыв контакта между считывающим устройством и персональным идентификатором или 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 ограничения доступа к ресурсам

Система Secret Net 6 располагает рядом механизмов разграничения доступа пользователей к локальным и сетевым ресурсам компьютера, которые дополняют средства, предоставляемые ОС Windows для ресурсов файловой и операционной систем.

Механизмы разграничения доступа

Табл. 1. Механизмы разграничения доступа

Механизм	Защищаемые ресурсы
Избирательное разграничение доступа	Аппаратные ресурсы (локальные устройства, в т. ч. последовательные и параллельные порты; локальные, сменные и логические диски; устройства, подключаемые к шинам USB, PCMCIA, IEEE 1394, Secure Digital)
Полномочное разграничение доступа	Ресурсы файловой системы NTFS и NTFS5 на локальных (постоянных и сменных) и подключенных сетевых дисках компьютера
Замкнутая программная среда	Исполняемые файлы на локальных дисках компьютера и подключенных сетевых дисках

Избирательное разграничение доступа

Управление избирательным доступом к ресурсам компьютера осуществляется путем предоставления прав пользователям компьютера. В соответствии с этим механизмом администратор определяет, кто из пользователей может получить доступ к ресурсу и какой тип доступа ему может быть предоставлен.

Для разграничения доступа к ресурсам файловой системы и операционной системы используются стандартные средства ОС Windows. Кроме того, в систему Secret Net 6 включены средства разграничения доступа к локальным устройствам компьютера — последовательным и параллельным портам, локальным, сменным и логическим дискам, устройствам, подключаемым к шинам USB, PCMCIA, IEEE 1394, Secure Digital.

Полномочное разграничение доступа

В режиме полномочного разграничения доступа система обеспечивает:

- разграничение доступа пользователей к конфиденциальной информации;
- контроль потоков конфиденциальной информации;
- контроль вывода конфиденциальной информации на внешние носители;
- контроль вывода конфиденциальной информации на печать.

При организации полномочного разграничения доступа для каждого пользователя компьютера устанавливается некоторый уровень допуска к конфиденциальной информации, определяющий его права на доступ к конфиденциальным данным. Всем конфиденциальным каталогам и файлам на локальных и сетевых дисках назначаются соответствующие категории конфиденциальности. Принятые по умолчанию названия категорий конфиденциальности могут быть изменены администратором 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.

При включенном режиме контроля потоков конфиденциальной информации пользователю самому предоставляется возможность выбрать (но не выше уровня до-

пуска) уровень конфиденциальности сеанса, тем самым заявив о категории конфиденциальности документов, с которыми он собирается работать (см. стр. 9). В этом случае доступ пользователя к конфиденциальным файлам определяется не уровнем допуска, а уровнем конфиденциальности сеанса.

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" режиме 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 6 с целью сбора информации о программах, которые используют пользователи.

Что нужно знать и иметь перед началом работы

Перед началом работы в системе администратор безопасности должен предоставить вам все необходимые права для выполнения ваших должностных обязанностей и проинформировать вас о предоставленных правах.

При использовании ...	**вам необходимо знать** ...
избирательного разграничения доступа	• к каким сетевым и локальным ресурсам компьютера (дискам, каталогам, файлам, принтерам, коммуникационным портам, дисководам, приводам и т. д.) вы имеете право доступа; • какие операции вам разрешено выполнять с этими ресурсами (просматривать, добавлять, удалять и т. д.); • какие устройства вам разрешено подключать.
полномочного разграничения доступа	• ваш уровень допуска к конфиденциальной информации; • предоставленные вам привилегии; • доступные для работы файлы, их размещение; • требования, которые необходимо соблюдать при работе с конфиденциальными документами.
замкнутой программной среды	• перечень программ, которые вам разрешено запускать.

Как действовать в проблемных ситуациях

Если вам не удалось:

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

обратитесь к администратору и опишите ему возникшую ситуацию!

Правила работы с конфиденциальными ресурсами

Общие принципы

Полномочное разграничение доступа пользователей к ресурсам файловой системы NTFS (NTFS5) основано на следующем подходе:

- каждому каталогу или файлу на локальных и сетевых дисках назначается одна из трех категорий конфиденциальности (по умолчанию категории имеют названия "неконфиденциально", "конфиденциально" и "строго конфиденциально");
- каждому пользователю назначается один из трех возможных уровней допуска к конфиденциальной информации. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов[1];
- доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла. Например, пользователь с уровнем допуска "конфиденциально" имеет доступ только к файлам категорий "конфиденциально" и "неконфиденциально".

При отсутствии доступа к файлу пользователь может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть на чтение сам файл.

Режимы работы

Подсистема полномочного разграничения доступа может работать в режиме контроля потоков конфиденциальной информации.

Контроль потоков конфиденциальной информации предназначен:

- для предотвращения несанкционированного копирования или перемещения конфиденциальных файлов в другие, неконфиденциальные каталоги;
- для предотвращения несанкционированного копирования отдельных частей конфиденциальных файлов в другие, неконфиденциальные файлы;
- для предотвращения несанкционированной записи конфиденциальных файлов на любые носители информации (встроенные и сменные).

Администратор безопасности может включить или отключить режим контроля потоков конфиденциальной информации. В зависимости от того, включен или отключен этот режим работы, различаются правила работы с конфиденциальными ресурсами.

При включенном режиме контроля потоков конфиденциальной информации пользователю самому предоставляется возможность выбрать (но не выше своего уровня допуска) уровень конфиденциальности сеанса, для указания категории конфиденциальности документов, с которыми он собирается работать (см. стр. 9). В этом случае доступ пользователя к конфиденциальным файлам определяется не уровнем допуска, а уровнем конфиденциальности сеанса.

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

Без контроля потоков	При контроле потоков
Доступ к файлам	
Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла	Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла
Запрещено удаление конфиденциального файла с помещением в "Корзину"	Запрещено удаление любого файла с помещением в "Корзину"

[1] Названия категорий конфиденциальности и уровней допуска, предлагаемые по умолчанию, могут быть изменены администратором безопасности в соответствии со стандартами, принятыми в вашей организации.

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><td colspan="2">Доступ к каталогам</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, то при создании, сохранении, копировании или перемещении файла в каталог файлу присваивается категория конфиденциальности каталога</td><td>Если включен режим автоматического присвоения категории конфиденциальности, то при создании, сохранении, копировании или перемещении файла в каталог файлу 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 файлу присваивается категория "неконфиденциально";
при перемещении файла внутри логического раздела файл сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога).</td><td>Если отключен режим автоматического присвоения категории конфиденциальности:
при создании, сохранении или копировании файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога;
при перемещении файла внутри логического раздела файл сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога и уровень конфиденциальности сессии).</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">Работа в приложениях</td></tr>
<tr><td>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. Чтобы сохранить файл с более низкой категорией конфиденциальности, чем текущий уровень приложения, необходимо закрыть приложение и открыть его заново</td><td>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)</td></tr>
<tr><td colspan="2">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 разграничения доступа, при таких обращениях к конфиденциальным и строго конфиденциальным файлам пользователю предлагается повысить уровень конфиденциальности приложения до уровня конфиденциальности этих файлов. В таких случаях, если не планируется работать с предложенным уровнем конфиденциальности, достаточно отказаться от повышения уровня конфиденциальности приложения</td></tr>
</table>

Без контроля потоков	При контроле потоков
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	
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.	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.
Если отключен режим контроля печати, 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	
При включенном режиме контроля печати для печати конфиденциальных документов можно использовать только приложения MS Word или MS Excel. Печать из других приложений блокируется. При печати в документы автоматически добавляется выбранный гриф конфиденциальности	
Вывод на внешние носители	
Пользователь, имеющий доступ к конфиденциальным документам, может копировать файлы или сохранять их содержимое на любые носители независимо от наличия привилегии "Вывод конфиденциальной информации"	Пользователь, **не** обладающий привилегией "Вывод конфиденциальной информации", не может копировать конфиденциальные файлы или сохранять их содержимое на внешние носители. Внешними носителями считаются: • **в базовом режиме контроля вывода информации** — любые встроенные и съемные носители информации с файловой системой, отличной от NTFS (например, жесткий диск или дискета с FAT); • **в расширенном режиме контроля вывода информации** — любые встроенные носители информации с файловой системой, отличной от NTFS (например, жесткий диск с FAT), а также любые съемные носители информации (например, дискета с NTFS или FAT).

Управление конфиденциальными ресурсами

Изменение категории конфиденциальности ресурса

Для изменения категории конфиденциальности каталога или файла в режиме полномочного разграничения доступа вы должны обладать привилегией "Управление категориями конфиденциальности". Если у вас нет такой привилегии, вы можете только повысить категорию конфиденциальности файла, но не выше своего уровня допуска или уровня конфиденциальности сеанса (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога).

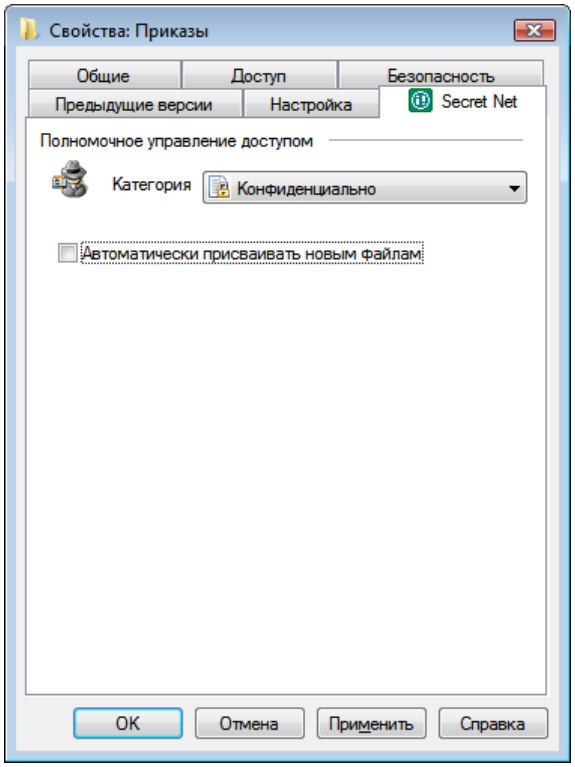
Внимание! Учитывайте следующие общие рекомендации:

- не присваивайте категории "конфиденциально" и "строго конфиденциально" 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.

Процедура выполняется с использованием программы "Проводник" ОС Windows.

Для изменения категории конфиденциальности каталога:

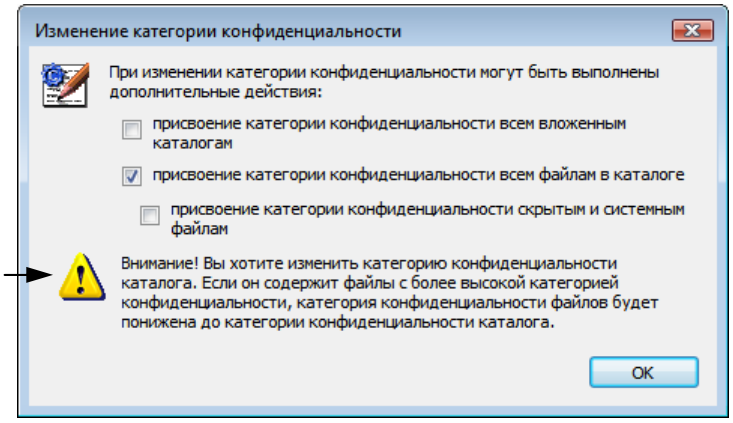
1. В программе "Проводник" вызовите контекстное меню каталога и активируйте команду "Свойства". В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".



2. Укажите необходимые значения параметров:
   - Выберите в раскрывающемся списке поля "Категория" нужную категорию конфиденциальности для каталога.
   - Выберите режим автоматического присвоения категории конфиденциальности файлам каталога, установив параметр "Автоматически присваивать новым файлам" в положение "Включено" или "Выключено".
3. Нажмите кнопку "OK".

Если каталог содержит файлы и подкаталоги, на экране появится диалог, предлагающий изменить категории конфиденциальности файлам и подкаталогам:

Это предупреждение добавляется в тех случаях, когда категория каталога понижается



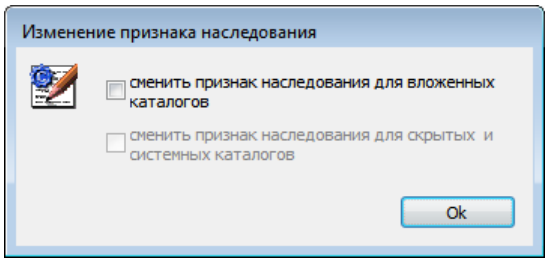
- Если требуется присвоить подкаталогам выбранную для каталога категорию конфиденциальности, а также изменить для подкаталогов состояние параметра "Автоматически присваивать новым файлам", поставьте отметку в поле "присвоение категории конфиденциальности всем вложенным каталогам".
- Если требуется, чтобы всем файлам в каталоге, а также и в подкаталогах (только при условии, что первый выключатель содержит отметку), за исключением скрытых и системных файлов, была присвоена выбранная для каталога категория конфиденциальности, поставьте отметку в поле "присвоение категории конфиденциальности всем файлам в каталоге".
- Если требуется, чтобы категория конфиденциальности была также присвоена находящимся в каталоге и подкаталогах скрытым и системным файлам, поставьте отметку в поле "присвоение категории конфиденциальности скрытым и системным файлам".

Во избежание нарушений в работе системы без особой необходимости не рекомендуется присваивать скрытым и системным файлам категории "конфиденциально" и "строго конфиденциально".

- Нажмите кнопку "OK".

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

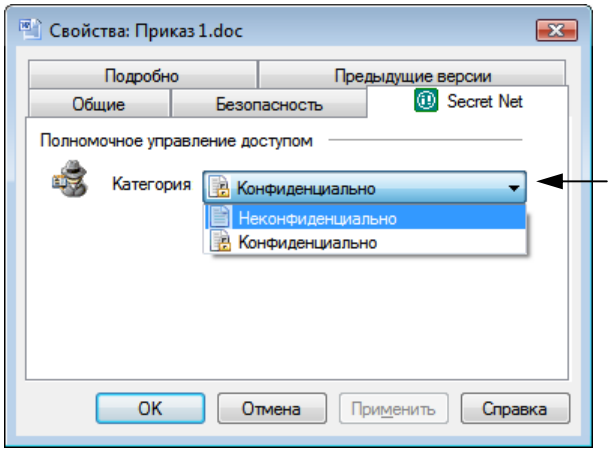
Если для каталога, содержащего подкаталоги, изменено значение параметра "Автоматически присваивать новым файлам", а категория конфиденциальности каталога осталась прежней, на экране появится диалог:



- Если требуется изменить для подкаталогов состояние параметра "Автоматически присваивать новым файлам", поставьте отметку в поле "сменить признак наследования для вложенных каталогов".
- Если требуется изменить состояние параметра "Автоматически присваивать новым файлам" также и для скрытых и системных каталогов, поставьте отметку в поле второго выключателя.
- Нажмите кнопку "OK".

Для изменения категории конфиденциальности файла:

1. Вызовите программу "Проводник".
2. Вызовите контекстное меню файла и активируйте в нем команду "Свойства".
3. В появившемся на экране окне "Свойства" перейдите к диалогу "Secret Net".



Список этого поля содержит перечень тех категорий конфиденциальности, которые могут быть присвоены файлу данным пользователем в данном каталоге

4. Выберите в раскрывающемся списке поля "Категория" нужную категорию конфиденциальности файла.
5. Нажмите кнопку "OK".

Работа с конфиденциальным документом в MS Word и MS Excel

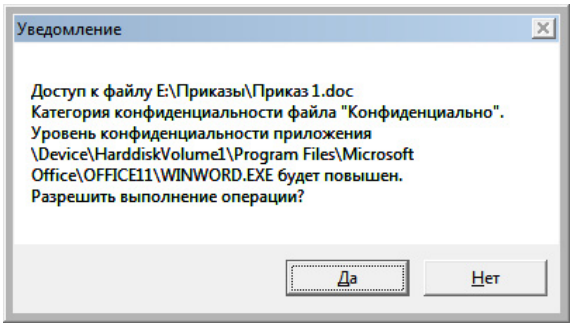
Прежде чем начать работу с конфиденциальными документами в MS Word или MS Excel, рекомендуется сохранить и закрыть все ранее открытые неконфиденциальные документы.

Открытие документа

Для открытия конфиденциального документа:

1. Запустите MS Word или MS Excel.
2. Активируйте 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".

Важно. 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 конфиденциального документа из MS Word

Если в Secret Net 6 включен режим контроля печати конфиденциальных документов, то при печати в MS Word конфиденциальный документ маркируется грифом конфиденциальности.

Гриф конфиденциальности состоит из групп полей, которые могут быть помещены на каждой странице документа (над текстом и под текстом), а также в конце конфиденциального документа. В состав системы входят два грифа (Гриф # 1 и Гриф # 2), примеры документов с этими грифами приведены ниже (см. стр. 29). В вашей организации могут быть разработаны грифы в соответствии с принятым у вас стандартом.

Предлагаемые Secret Net грифы содержат поля двух типов:

- обязательные поля, которые заполняются системой автоматически (например, "Исполнитель", "Дата", "Документ");

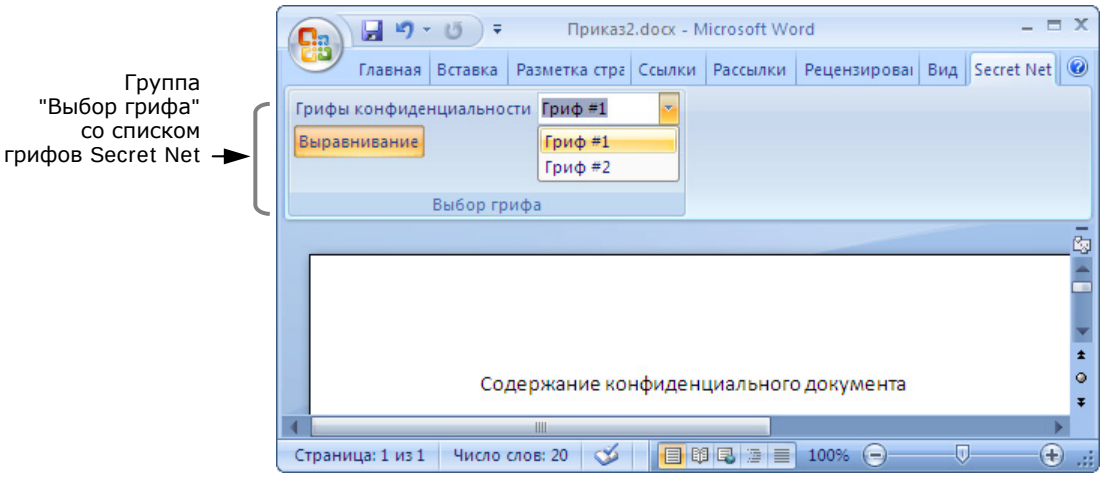
  Пояснение. При печати в поле "Исполнитель" грифа конфиденциальности подставляется значение параметра "Полное имя" пользователя, выполняющего печать документа.

- настраиваемые поля (например, "Учетный номер", "Экземпляр №"), которые заполняются пользователем перед отправкой документа на печать.

  Значения, введенные в настраиваемые поля, не сохраняются в документе, поэтому при следующем выводе на печать настраиваемые поля должны быть заполнены снова.

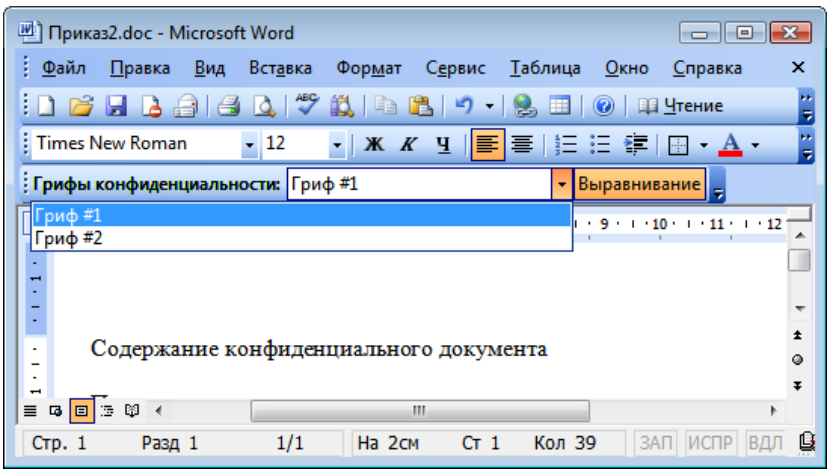
Для печати документа с грифом конфиденциальности:

1. Откройте в MS Word конфиденциальный документ (см. стр. 26).
2. Если в системе имеется несколько грифов конфиденциальности, выберите нужный гриф. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — в основном окне программы перейдите на вкладку "Secret Net" и в группе "Выбор грифа" выберите нужный гриф из раскрывающегося списка "Грифы конфиденциальности";



- в MS Word 2003 и более ранних версиях — выберите нужный гриф из раскрывающегося списка "Грифы конфиденциальности" на панели инструментов "Secret Net".

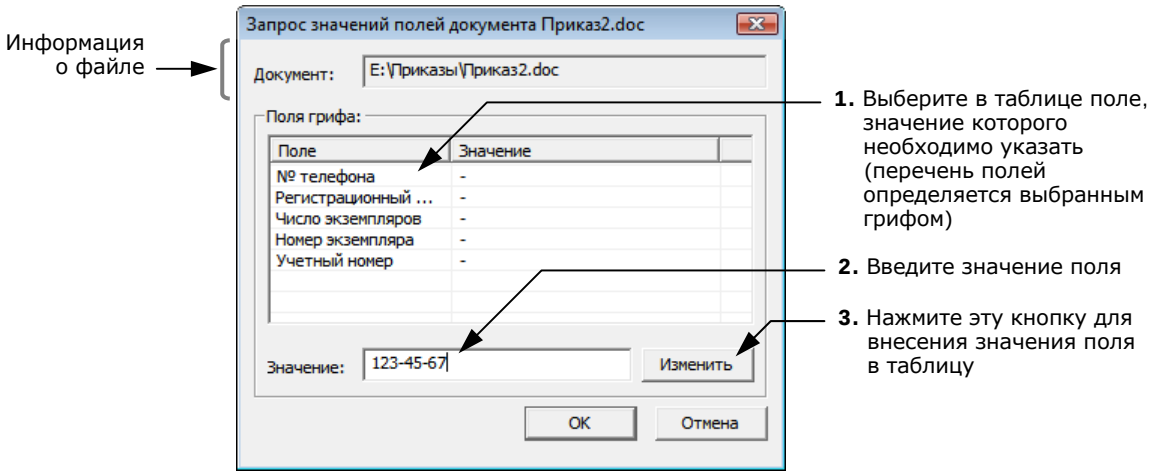
Если панель инструментов "Secret Net" не отображается, включить отображение панели можно в меню "Вид | Панели инструментов".



3. Активируйте в программе команду печати документа. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — в верхнем левом углу окна программы нажмите кнопку "Office" и в открывшемся меню активируйте команду "Печать | Печать";
   - в MS Word 2003 и более ранних версиях — в главном меню программы активируйте команду "Файл | Печать".

Если перед печатью требуется просмотреть вид документа с грифом конфиденциальности, используйте функцию предварительного просмотра редактора MS Word. Примеры документов с грифами "Гриф #1" и "Гриф #2" см. ниже.

На экране появится диалог для настройки полей грифа конфиденциальности:

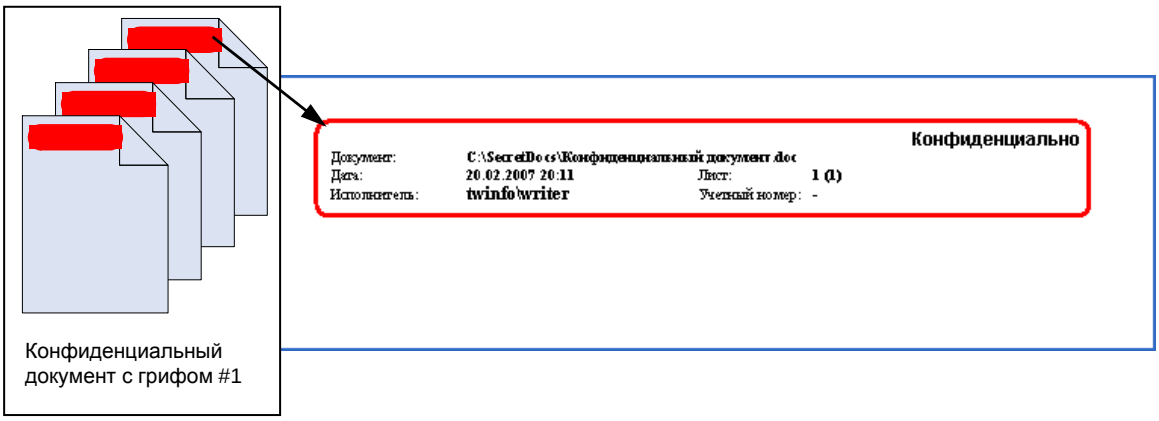


4. Задайте значения полей таблицы (см. выноски к рисунку).
5. Нажмите кнопку "OK".

   На экране появится стандартный диалог для определения параметров печати.
6. Укажите параметры печати и, если необходимо, настройте свойства принтера.
7. Нажмите кнопку "OK" в диалоге параметров печати.

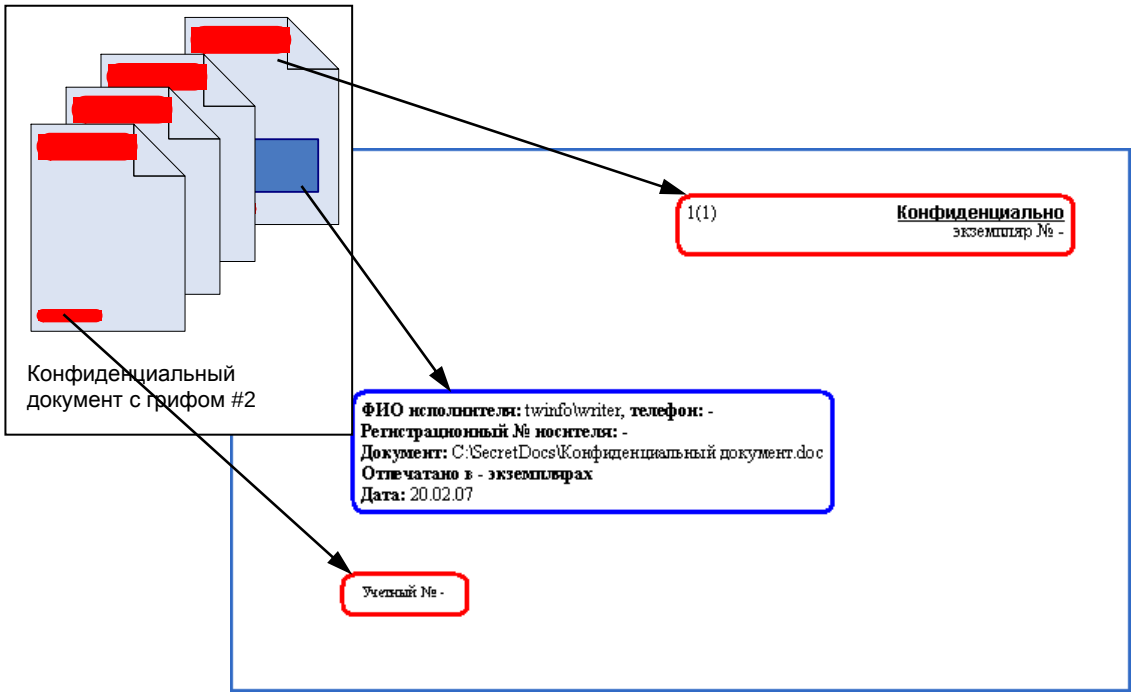
В итоге документ будет распечатан вместе с грифом конфиденциальности.

Ниже приведен пример вида документа с грифом конфиденциальности "Гриф # 1".



В верхнюю часть каждой страницы конфиденциального документа с грифом "Гриф # 1" добавляется группа полей, отмеченная на рисунке красной рамкой.

Ниже приведен пример вида документа с грифом конфиденциальности "Гриф # 2".



Каждая страница конфиденциального документа с грифом "Гриф #2" маркируется сверху и снизу полями, отмеченными на рисунке красной рамкой. Кроме того, в конце всего документа печатаются поля, выделенные на рисунке синей рамкой.

Если вы работаете не в режиме контроля потоков, то прежде чем вернуться к работе с неконфиденциальными документами, сохраните изменения и закройте все конфиденциальные документы, после чего закройте и повторно запустите MS Word.

Печать конфиденциального документа из MS Excel

Если в Secret Net 6 включен режим контроля печати конфиденциальных документов, то при печати из MS Excel конфиденциальный документ маркируется грифом конфиденциальности. В документах MS Excel элементы грифа конфиденциальности могут располагаться в верхнем и нижнем колонтитуле (с правой и левой стороны), а также в конце текстовой части всего документа.

Гриф конфиденциальности вставляется на место колонтитула. Исходный колонтитул самого документа при этом затирается.

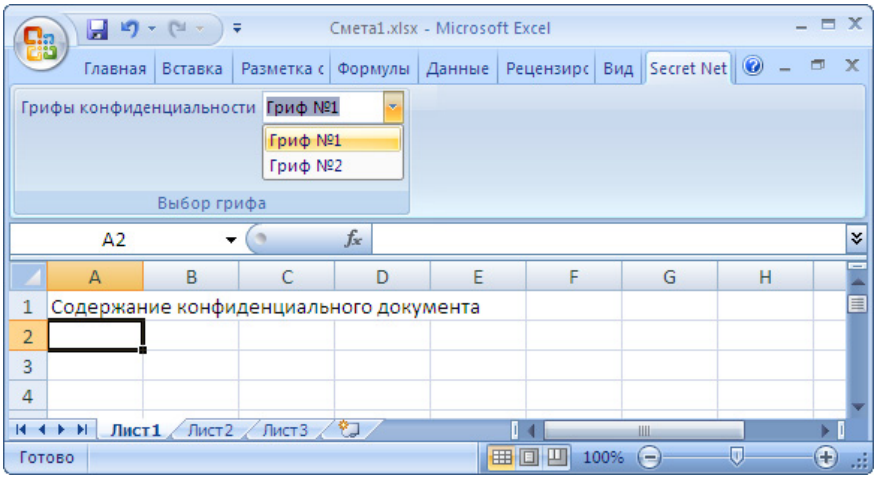
Элементы грифа конфиденциальности состоят из отдельных параметров (свойств) документа. Параметры документа могут быть двух типов:

- стандартные (например, "Исполнитель", "Дата", "Документ"), которые пользователю указывать не требуется — эти параметры автоматически заполняются из свойств документа;
- настраиваемые (например, "Учетный номер", "Номер экземпляра"), значения которых пользователь вводит непосредственно перед печатью.

Для печати конфиденциального документа из MS Excel:

1. Откройте в MS Excel конфиденциальный документ (см. стр. 26).
2. Если в системе имеется несколько грифов конфиденциальности, выберите нужный гриф. Для этого в зависимости от версии установленной программы MS Excel выполните соответствующее действие:
   - в MS Excel 2007 — в основном окне программы перейдите на вкладку "Secret Net" и в группе "Выбор грифа" выберите нужный гриф из раскрывающегося списка "Грифы конфиденциальности";

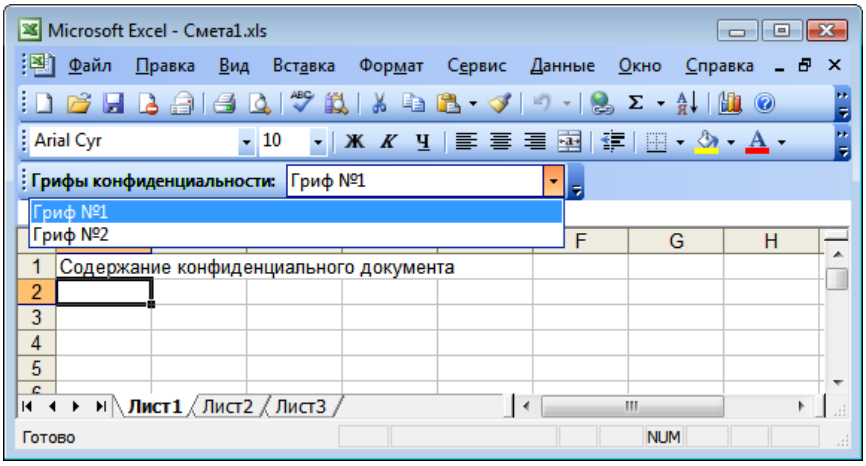
Группа "Выбор грифа" со списком грифов Secret Net



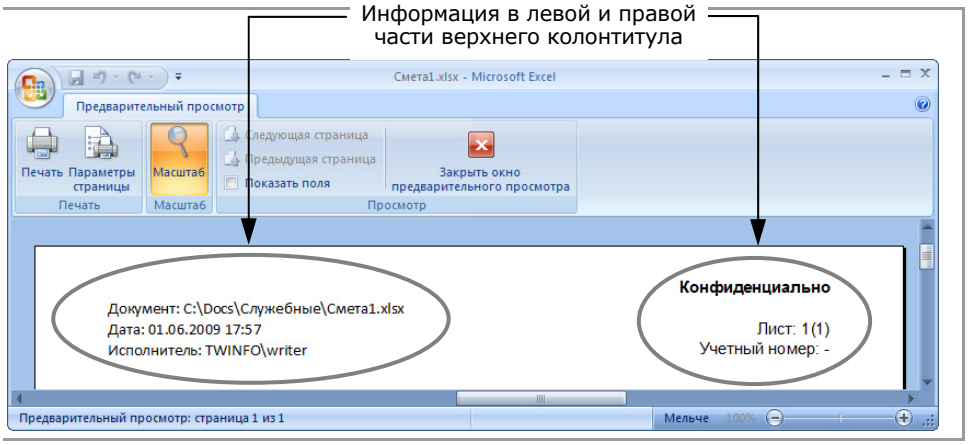
   - в MS Excel 2003 и более ранних версиях — выберите нужный гриф из раскрывающегося списка "Грифы конфиденциальности" на панели инструментов "Secret Net Bar".

Если панель инструментов "Secret Net Bar" не отображается, включить отображение панели можно в меню "Вид | Панели инструментов".

Панель инструментов со списком грифов Secret Net



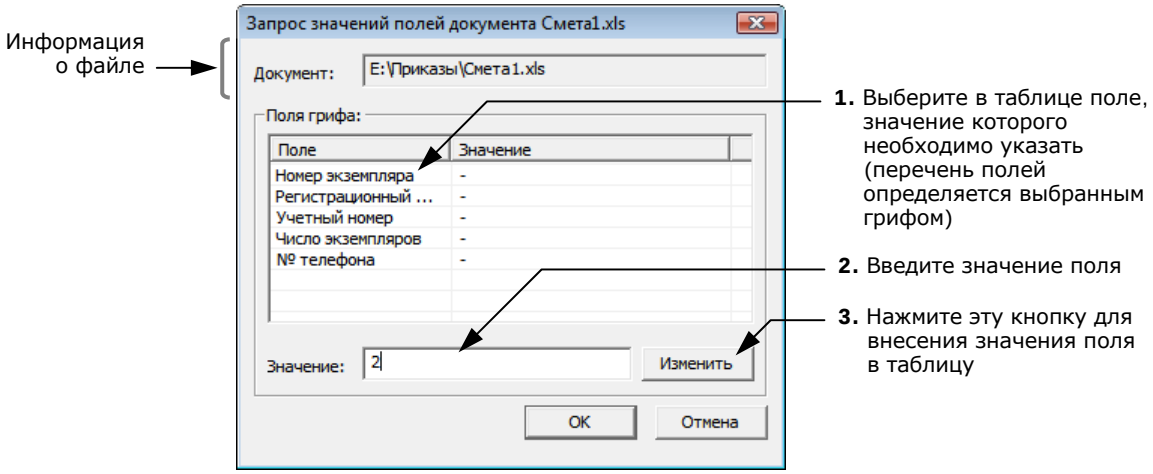
Если перед печатью требуется просмотреть вид документа с грифом конфиденциальности, используйте функцию предварительного просмотра редактора MS Excel. Пример оформления грифа конфиденциальности:



3. Активируйте в программе команду печати документа. Для этого в зависимости от версии установленной программы MS Excel выполните соответствующее действие:
   - в MS Excel 2007 — в верхнем левом углу окна программы нажмите кнопку "Office" и в открывшемся меню активируйте команду "Печать | Печать";
   - в MS Excel 2003 и более ранних версиях — в главном меню программы активируйте команду "Файл | Печать".

   На экране появится стандартный диалог для определения параметров печати.
4. Укажите параметры печати и, если необходимо, настройте свойства принтера.
5. Нажмите кнопку "Печать" в диалоге параметров печати.

   Если в колонтитул входят не только основные, но и настраиваемые параметры документа, то на экране появится диалог для ввода значений настраиваемых параметров:



6. Задайте значения полей таблицы (см. выноски к рисунку).
7. Нажмите кнопку "OK".

В итоге документ будет распечатан вместе с грифом конфиденциальности.

Если вы работаете не в режиме контроля потоков, то прежде чем вернуться к работе с неконфиденциальными документами, сохраните изменения и закройте все конфиденциальные документы, после чего закройте и повторно запустите MS Excel.

Предметный указатель