КОД безопасности

Средство защиты информации

Secret Net Studio

Руководство пользователя

RU.88338853.501400.001 92

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для пользователей компьютеров с установленным программным обеспечением изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые для работы с Secret Net Studio.

Условные обозначения

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

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

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. Вы можете посетить сайт компании "Код Безопасности" (https://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 в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training- courses/ . Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения

Что нужно знать

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. Он определяет, какие возможности доступны пользователям и какие ограничения с точки зрения безопасности должны действовать в системе.

Пользователи работают с ресурсами информационной системы и выполняют действия в рамках своих полномочий. Несанкционированные действия контролируются системой, и в зависимости от заданной реакции могут быть ограничены возможности доступа. Поэтому на начальном этапе следует выяснить у администратора, какими правами и привилегиями вы сможете пользоваться при работе в системе.

Что необходимо иметь

Для начала работы необходимо получить у администратора:

1. Учетные данные для входа в систему: имя пользователя и пароль.
2. Если для идентификации пользователей предусмотрено использование аппаратных средств, потребуется персональный идентификатор (например, Rutoken), присвоенный пользователю средствами системы Secret Net Studio.
3. Если применяется механизм шифрования данных в криптоконтейнерах, для доступа к криптоконтейнерам потребуется носитель, содержащий ключевую информацию (ключевой носитель). Ключевым носителем может являться присвоенный пользователю персональный идентификатор (тот же, который используется для идентификации, или другой), флеш-карта или USB-флеш-накопитель.
4. Если функционирует доверенная среда, для загрузки операционной системы компьютера потребуется загрузочный носитель — специализированный USB-флеш-накопитель.
5. Кроме того, в зависимости от конфигурации используемых защитных подсистем, для работы в системе Secret Net Studio могут использоваться дополнительные средства и данные, предоставляемые администратором.

Что важно помнить

Во избежание нежелательных последствий будьте внимательны при выполнении действий и следуйте общим рекомендациям:

1. Запомните свое имя пользователя и пароль. Не допускайте компрометации пароля и регулярно выполняйте процедуру его смены.
2. Никому не давайте персональный идентификатор или ключевой носитель.
3. Во всех сложных ситуациях, которые вы сами не в состоянии разрешить, обращайтесь к администратору безопасности. В том числе если нужны дополнительные права доступа к ресурсам для эффективного выполнения должностных обязанностей.

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 Studio, 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.**14**)	В системах, не оснащенных аппаратными средствами контроля входа
Только по идентификатору	Только с предъявлением персонального идентификатора (см. стр.**15**)	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

Для всех пользователей компьютера устанавливается единый режим входа.

В режимах входа "По имени" и "Смешанный" допускается идентификация посредством ввода имени пользователя вручную или с использованием средств идентификации, активированных средствами ОС Windows (например, Smart Card, eToken и пр.). Сведения об использовании средств идентификации в ОС Windows см. в документации на операционную систему. В режиме "Только по идентификатору" могут использоваться только персональные идентификаторы, активированные средствами Secret Net Studio, но не ОС Windows.

Если идентификатор содержит сертификат Microsoft, то в режиме "Смешанный" при предъявлении идентификатора вход выполняется по сертификату.

Если применяются средства аппаратной поддержки системы защиты, администратор выдает каждому пользователю персональный идентификатор (в зависимости от типа применяемого средства — идентификаторы eToken, Rutoken, JaCarta, ESMART 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 Studio 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, без него невозможно дальнейшее использование идентификатора.

В персональном идентификаторе также может быть записан пароль пользователя и ключевая информация, необходимая для работы с зашифрованными данными в криптоконтейнерах.

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 Studio, 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.

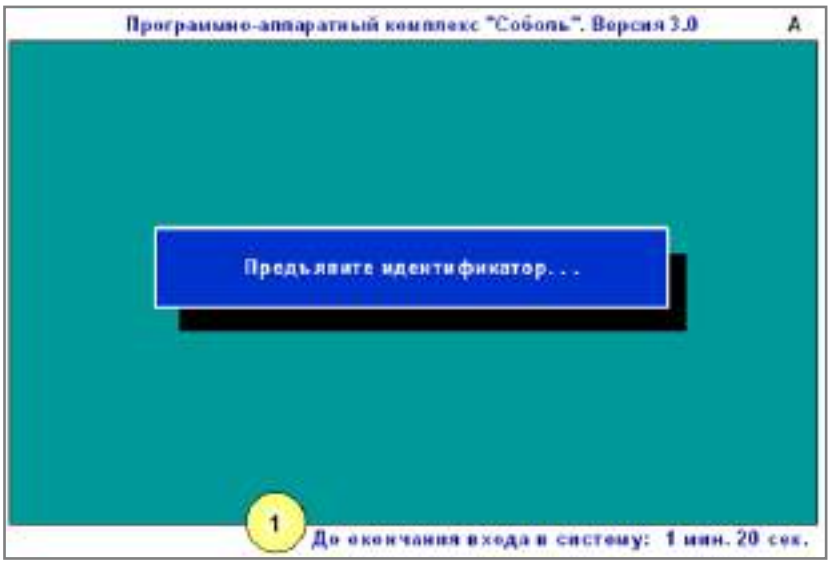
Система Secret Net Studio поддерживает интеграцию с комплексом "Соболь" версий 3.x и 4. Порядок загрузки компьютера и входа в систему в этих версиях разный. Используйте одну из следующих инструкций в зависимости от версии ПАК "Соболь", установленной на вашем компьютере:

- для версий 3.x — см. ниже;
- для версии 4 — см. стр.**9**.

Для загрузки компьютера и входа в систему при использовании комплекса "Соболь" версий 3.x:

1. Включите питание компьютера.

   На экране появится запрос персонального идентификатора.



Пояснение. На рисунке обозначены: 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 ОС.
- 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). При вводе пароля различаются строчные и заглавные буквы.

- 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).

Примечание.
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.

Начнется загрузка операционной системы.

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 этом случае после успешной проверки прав пользователя выполнится вход в систему без запроса пароля.
- В идентификаторе не записан пароль или идентификатор содержит другой пароль, который не является актуальным для ОС Windows.

В этом случае появится диалог для ввода учетных данных пользователя, где будет отображаться имя пользователя — владельца предъявленного идентификатора.

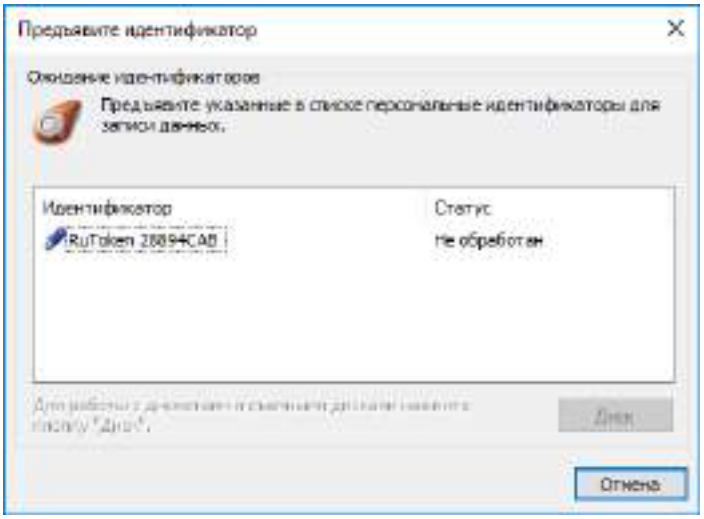
Введите актуальный пароль в поле "Пароль" и нажмите кнопку "→" или "OK".

Если введенный вами пароль правильный и хранение пароля в идентификаторе **не** предусмотрено, выполнится 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.

Для загрузки компьютера и входа в систему при использовании комплекса "Соболь" версии 4:

1. Включите питание компьютера.

   На экране пояится сообщение "Тестирование датчика случайных чисел..." или "Подготовка к работе...".

   Пояснение. При возникновении ошибки на данном этапе обратитесь к администратору.

   При успешной загрузке комплекса "Соболь" на экране появится запрос персонального идентификатора.

В центре окна может располагаться счетчик времени:

- оставшегося до автоматической загрузки ОС (в секундах) или
- оставшегося для предъявления идентификатора и ввода пароля (в минутах и секундах).

Пояснение.

- Счетчик времени, оставшегося до автоматической загрузки операционной системы, отображается, если в комплексе "Соболь" настроена автоматическая загрузка. В этом случае предъявление учетных данных не требуется. По истечении заданного времени выполнится загрузка операционной системы.
- Счетчик времени, оставшегося для предъявления идентификатора и ввода пароля, отображается, если администратор активировал режим ограничения времени на вход в информационную систему. Если вы не успели за отведенное время предъявить идентификатор и ввести пароль, компьютер будет заблокирован. Перезагрузите компьютер и повторите вход.

2. Предъявите выданный вам персональный идентификатор.

Пояснение.

- Если идентификатор уже предъявлен, комплекс автоматически считывает его.
- Если одновременно предъявлено несколько идентификаторов, считывается первый найденный комплексом идентификатор. Для смены идентификатора нажмите клавишу <Esc>.
- Если идентификатор предъявлен неправильно, запрос останется на экране. Повторно предъявите идентификатор.
- При появлении сообщения "Вход в систему запрещен администратором" нажмите кнопку "ОК" в окне с сообщением и обратитесь к администратору.

Если в идентификаторе не сохранен пароль, на экране появится диалог для его ввода.

- Введите пароль для входа в комплекс "Соболь".

Примечание.
На экране каждый символ пароля отображается как "*" (звездочка). При вводе пароля различаются строчные и заглавные буквы.

- Нажмите кнопку "Войти" или клавишу <Enter>.

Внимание!
- Если введенный пароль не соответствует предъявленному идентификатору, на экране появится сообщение "Неверный идентификатор или пароль". Нажмите кнопку "ОК" в окне с сообщением и снова предъявите идентификатор. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.
- Число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение, то при следующей попытке входа на экране появится сообщение о блокировке компьютера. В этом случае обратитесь к администратору.

После успешного предъявления учетных данных появится окно "Загрузка ОС" или окно с кнопкой "Загрузка ОС".

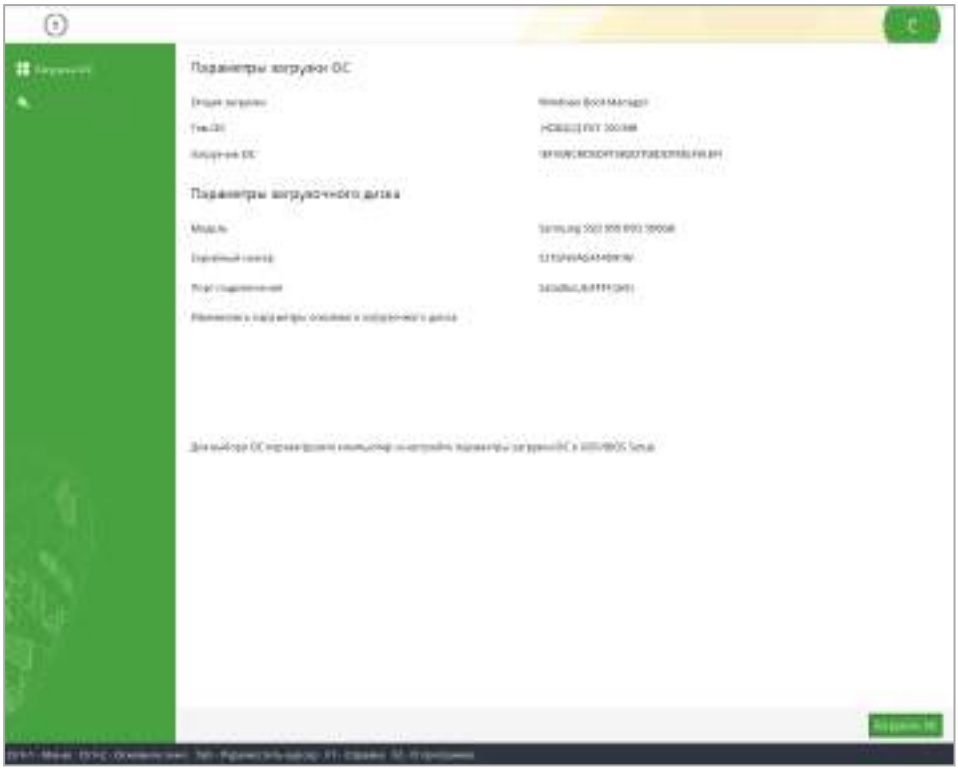


Рис.1 Окно "Загрузка ОС"

Рис.2 Окно с кнопкой "Загрузка ОС"

3. Нажмите кнопку "Загрузить ОС", "Загрузка ОС" или клавишу <Enter>. Выполнится проверка целостности объектов (если это предусмотрено).

Примечание.
- При обнаружении ошибок на экране появятся сообщения об ошибках. Нажмимайте кнопку "ОК" в окне с сообщением.
- Если уведомления комплекса в процессе проверки целостности не нужны, поставьте отметку "Больше не спрашивать" в окне с сообщением об ошибке.
- По окончании проверки нажмите кнопку "Готово" в окне проверки.
- Если на экране появилось сообщение "Компьютер заблокирован", выключите компьютер и обратитесь за помощью к администратору.

Начнется загрузка операционной системы.

4. 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 этом случае после успешной проверки прав пользователя выполнится вход в систему без запроса пароля.
   - В идентификаторе не записан пароль или идентификатор содержит другой пароль, который не является актуальным для ОС Windows.

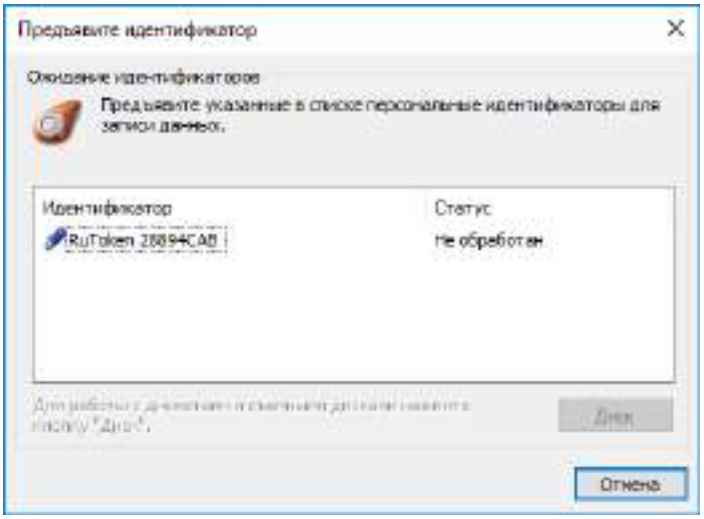
     В этом случае появится диалог для ввода учетных данных пользователя, где будет отображаться имя пользователя — владельца предъявленного идентификатора.

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

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

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 инструкциями, представленными в подразделах ниже.

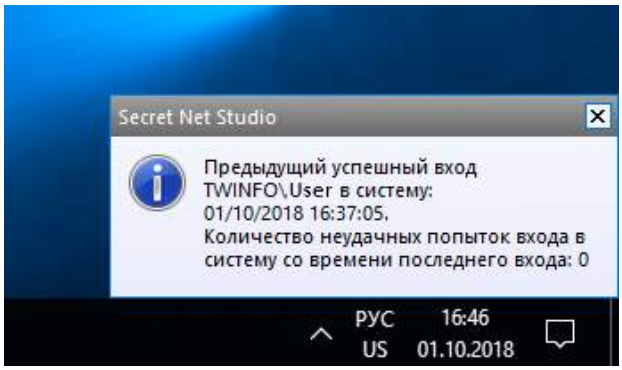
Процедура входа начинается при появлении на экране приглашения для входа в систему. Если администратор включил механизм оповещения, на экране приглашения отобразится информационное сообщение о реализованных в системе мерах защиты информации.

Внимание!

При наличии на экране приглашения сообщения о реализованных в системе мерах защиты информации вход в систему означает согласие с необходимостью соблюдения правил и ограничений на работу с информацией.

В зависимости от действующих механизмов защиты и ограничений, установленных администратором, действия пользователя для входа в систему могут различаться (см. инструкции в подразделах ниже).

Если администратор включил механизм оповещения, то после входа в систему над системной областью панели задач Windows отобразится сообщение с информацией о вашем последнем успешном входе в систему и количестве неудачных попыток входа с момента последнего успешного входа. Сообщение имеет вид, подобный показанному на следующем рисунке.



Пояснение.

- Если включен механизм оповещения, при первом входе в систему на экране отобразится сообщение "Данные о предыдущем входе пользователя отсутствуют".
- Сообщение с информацией о последнем успешном входе может не отобразиться в случае появления двух и более других информационных сообщений.

Стандартный способ входа в систему

Для входа стандартным способом:

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 10, Windows Server 2016, Windows Server 2019 — 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, в левом нижнем углу выберите нужное имя или элемент "Другой пользователь". На экране появятся поля для ввода учетных данных пользователя;
- на компьютере с ОС Windows 8.1 или Windows Server 2012 R2 — 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 или Windows Server 2008 R2 — выберите нужное имя учетной записи или элемент "Другой пользователь". На экране появятся поля 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 ваш пароль в поле "Пароль".

> **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 "→".

Если учетные данные введены правильно, выполняется вход в систему.

Вход по идентификатору

При использовании для входа в систему персонального идентификатора, активированного средствами Secret Net Studio, 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, содержащейся в персональном идентификаторе. Возможны следующие варианты:

- идентификатор содержит актуальный пароль пользователя;
- в идентификаторе не записан пароль/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)/идентификатор содержит сертификат Microsoft.

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
Ситуация 3	**Если в идентификаторе содержится сертификат Microsoft,** вход выполняется по сертификату без запроса пароля

В ситуациях 1 и 2 введите актуальный пароль в поле "Пароль" и нажмите кнопку "→" или "ОК".

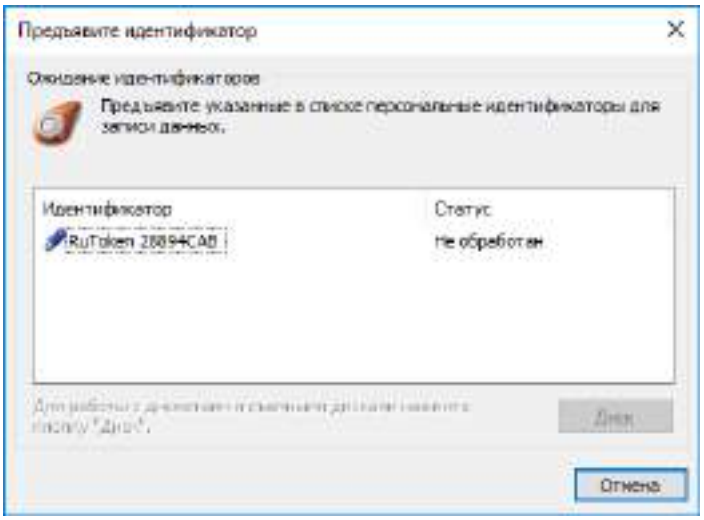
Примечание.
В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница.

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.

Особенности входа при усиленной аутентификации

В системе Secret Net Studio предусмотрены следующие режимы аутентификации пользователей:

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

Режим	Описание
Усиленная аутентификация по паролю	Помимо стандартной аутентификации ОС Windows, дополнительно выполняется аутентификация по паролю пользователя средствами системы Secret Net Studio

При усиленной аутентификации по паролю для выполнения проверки пароль должен быть сохранен в базе данных системы Secret Net Studio. Сохранение может выполняться 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.

Вход в систему при полномочном разграничении доступа

Если действует механизм полномочного управления доступом (см. стр.**29**), 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 вашего уровня допуска, система Secret Net Studio выдаст требование отключить данное устройство. Вход в систему будет запрещен до тех пор, пока устройство не будет отключено.

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 или ниже, чем уровень конфиденциальности сессии;
- обнаружены устройства с различными категориями 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.

Более подробную информацию о работе в системе в условиях полномочного разграничения доступа см. на стр.**30**.

Как действовать в проблемных ситуациях

При нарушении 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 Studio. 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 Studio. 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 Studio 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. 22) 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.

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.

Введен неверный PIN персонального идентификатора.

Причина. При входе в систему введен неправильный PIN персонального идентификатора.

Действия пользователя. Повторите ввод PIN.

Если вы забыли PIN персонального идентификатора, 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.**22**).

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 Studio, могут привести следующие причины: нарушения, связанные с контролем целостности защищаемых объектов, изменение аппаратной конфигурации, ошибки функционального контроля и пр.

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

Глава 3
Использование средств базовой защиты

Временная блокировка компьютера

Если вам необходимо временно прервать работу на компьютере, то для защиты от несанкционированного использования совсем не обязательно 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. Интервал неактивности может быть задан в ОС или настроен администратором в Secret Net Studio.

Для включения блокировки стандартным способом:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>.
2. В появившемся стандартном диалоге нажмите кнопку "Заблокировать" ("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 Studio 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.

Для разблокирования компьютера стандартным способом:

1. В зависимости от операционной системы компьютера выполните соответствующее действие:
   - На компьютере с ОС Windows 10/8.1 или Windows Server 2019/2016/2012 R2 — 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 или Windows Server 2008 R2 — выберите учетную запись пользователя заблокированного сеанса. На экране появится поле для ввода пароля.
2. Введите пароль и нажмите кнопку "→".

Для разблокирования компьютера с помощью 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 "→".

Смена пароля

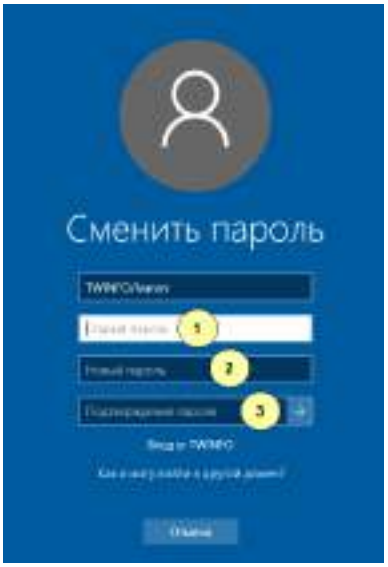
Для смены пароля:

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

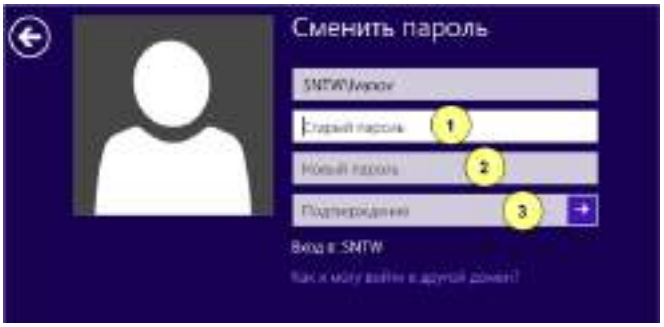
   Появится экран с оперативными командами ОС.
2. Нажмите кнопку "Сменить пароль"("Смена пароля" или "Изменить пароль").

   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 10 или Windows Server 2019/2016:

   - на компьютере с ОС Windows 8.1 или Windows Server 2012 R2:

- на компьютере с ОС Windows 7 или Windows Server 2008 R2:

Пояснение.
На рисунках обозначены: 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".

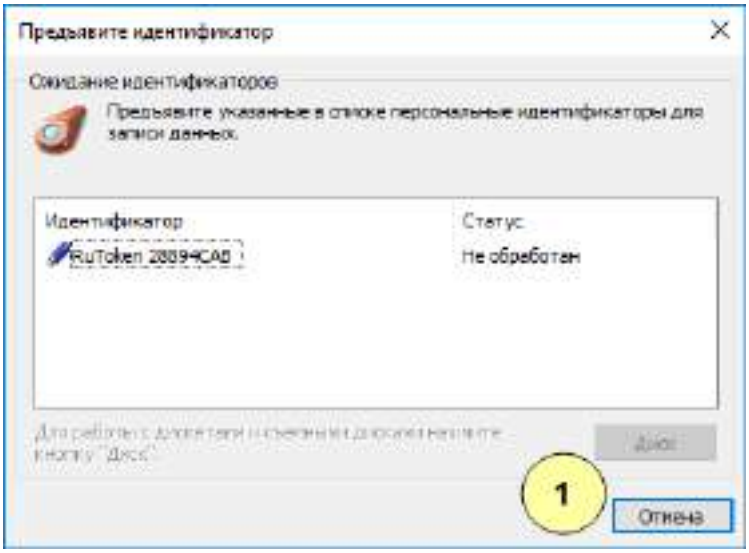
4. Нажмите кнопку "→".

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 рисунке обозначены: 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".

Локальные уведомления о событиях тревоги

Система Secret Net Studio может оповещать пользователя компьютера о возникновении событий, имеющих признаки несанкционированного доступа (к компьютеру, ресурсам и пр.). Эти события классифицируются как события тревоги с соответствующим уровнем. В качестве локального оповещения в системной области панели задач Windows меняется цвет пиктограммы Secret Net Studio и на экран выводится предупреждающее сообщение.

Администратор по своему усмотрению может сам включить/отключить режим локального оповещения и сбросить состояние тревоги или предоставить возможность управления режимом пользователям.

Для управления локальным оповещением:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Команды "Уведомления о тревогах" и "Сбросить состояние тревоги" предназначены для управления локальным оповещением.

   Если слева от команды "Уведомления о тревогах" отображается отметка, это означает, что оповещение о событиях тревоги включено.

Пояснение.

- Если команды "Уведомления о тревогах" и "Сбросить состояние тревоги" недоступны, значит, администратор не предоставил пользователям возможность управления локальным оповещением.
- Если администратор включил или отключил режим локального оповещения для всех пользователей компьютера, возможность изменения состояния режима недоступна для пользователя.

2. Для отключения оповещения нажмите на команду "Уведомления о тревогах" одним щелчком мыши, если команда доступна.
3. Для сброса состояния тревоги выберите команду "Сбросить состояние тревоги", если она доступна.

Глава 4
Работа с действующими средствами локальной защиты

Дискреционное управление доступом к файловым ресурсам

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. Он позволяет администраторам установить разрешения и запреты на выполнение операций с определенными ресурсами файловой системы.

Возможности по разграничению доступа зависят от типов ресурсов. Так, ограничены возможности по управлению доступом к ресурсам, необходимым для функционирования компьютера. Например, нельзя изменять разрешающие права доступа для корневого каталога системного диска и всего системного каталога.

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 Studio. 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.
При перемещении ресурса в другой логический раздел принудительно включается режим наследования прав доступа для этого ресурса. В этом случае независимо от ранее заданных прав, в новом размещении для ресурса будут действовать наследуемые права от вышестоящего каталога. При копировании ресурса (в тот же или другой логический раздел) режим наследования прав доступа включается для созданной копии ресурса.

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:

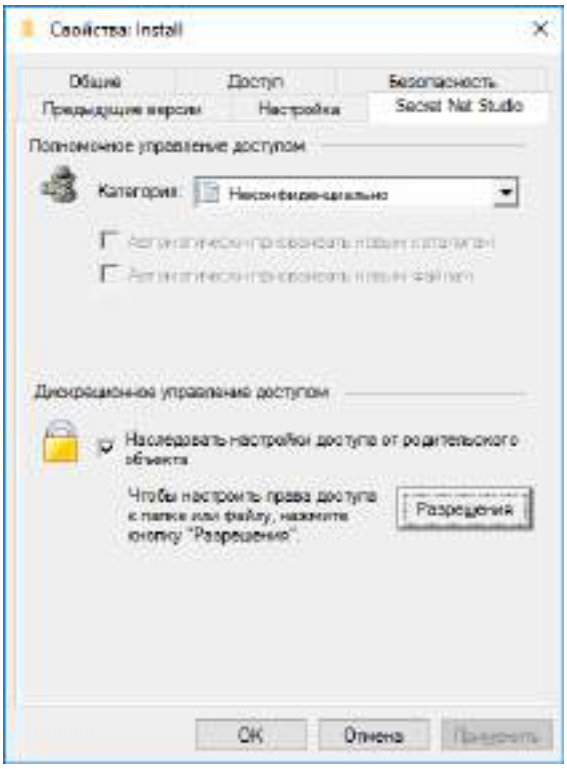
- администраторы безопасности или уполномоченные сотрудники, которым предоставлена привилегия "Управление правами доступа" — привилегия дает возможность изменять права доступа для всех ресурсов (независимо от установленных прав доступа к самим ресурсам);
- администраторы ресурса — пользователи, для которых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

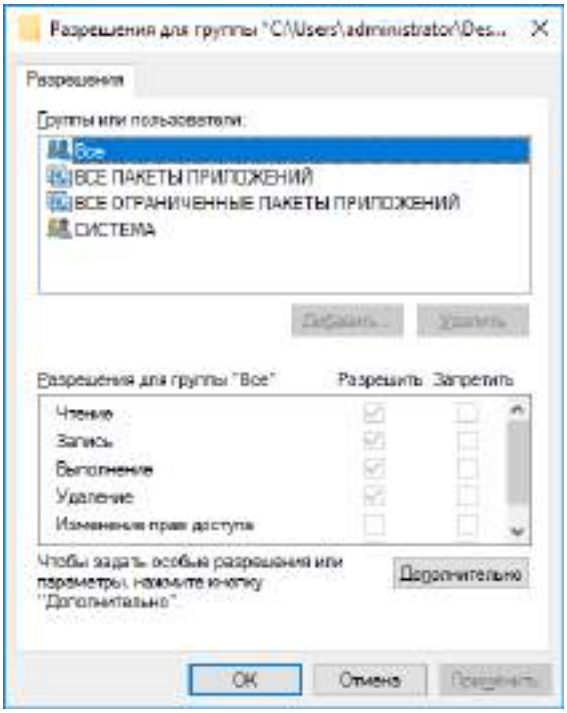
Для изменения прав доступа к ресурсу:

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 Studio".



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 нужно 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".

Удаление файлов с затиранием данных

При удалении файлов могут оставаться данные на устройствах хранения в областях памяти, которые были заняты этими файлами. В системе Secret Net Studio реализован механизм затирания удаляемой информации. Данный механизм обеспечивает невозможность восстановления и повторного использования данных после удаления.

Администратор безопасности может включить автоматическое затирание данных для файлов, удаляемых на локальных и/или сменных дисках. Автоматическое затирание происходит при выполнении стандартных команд удаления файлов в операционной системе. В частности, при очистке содержимого "Корзины" (файлы, находящиеся в папке "Корзина", еще не считаются удаленными) или при безвозвратном удалении выбранных объектов с помощью комбинации клавиш <Shift>+<Delete>.

Также пользователю может быть предоставлена возможность выборочного удаления файлов с затиранием данных.

Для выборочного удаления файлов с затиранием данных:

1. В программе "Проводник" выберите файловые объекты для удаления (файлы и/или каталоги), вызовите контекстное меню одного из выбранных объектов и выберите команду "Удалить безвозвратно".

Примечание.
Команда доступна, если администратором безопасности установлено ненулевое количество циклов затирания данных при удалении файловых объектов по выбору пользователя.

На экране появится запрос на продолжение операции.

2. Нажмите кнопку "Да" в диалоге запроса.

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 тревоги. 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 Studio с целью сбора информации о программах, которые используют пользователи.

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 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, 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.**17**).

Правила работы с конфиденциальными ресурсами

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

- каталогам и файлам, 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	
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"
Доступ к каталогам	

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></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>
<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 конфиденциальности</td></tr>
<tr><td colspan="2">Работа в приложениях</td></tr>
</table>

Без контроля потоков	**При контроле потоков**
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

<table>
<tr><th colspan="2">Печать конфиденциальных документов</th></tr>
<tr><td>Если включен механизм 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 механизм контроля печати:
пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (при условии, что 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 механизм 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</td></tr>
<tr><th colspan="2">Вывод на внешние носители</th></tr>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></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</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 учитывается.

Категория конфиденциальности локального физического диска имеет более высокий приоритет, чем категории файлов (каталогов), расположенных на этом устройстве. Если категория файла (каталога) ниже категории конфиденциальности устройства, система считает категорию файла (каталога) равной категории устройства. Если же категория файла (каталога) превышает категорию конфиденциальности устройства, доступ к файлу (каталогу) запрещается.

На всех устройствах USB, PCMCIA, IEEE1394, Secure Digital (сменные носители), подключенных к компьютеру, самим файлам и каталогам категория конфиденциальности не назначается. Для всех этих файлов и каталогов всегда действует категория, назначенная устройству.

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

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).

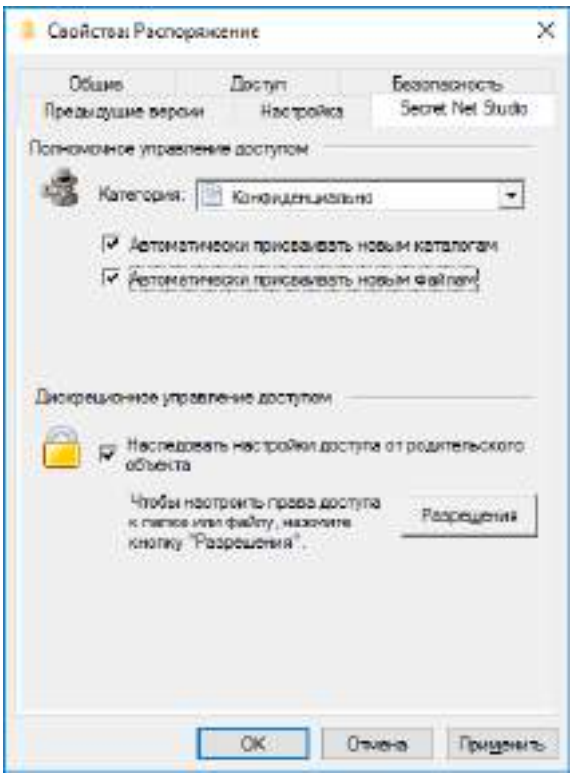
Внимание! Учитывайте следующие общие рекомендации:

- 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 локального физического диска, на котором располагаются эти объекты, так как категория такого устройства имеет более высокий приоритет;
- каталогам и файлам, находящимся на устройствах USB, PCMCIA, IEEE1394, Secure Digital (сменные носители), нельзя непосредственно назначить категорию конфиденциальности. Для них действует категория устройства.

Процедура выполняется с использованием программы "Проводник" ОС Windows.

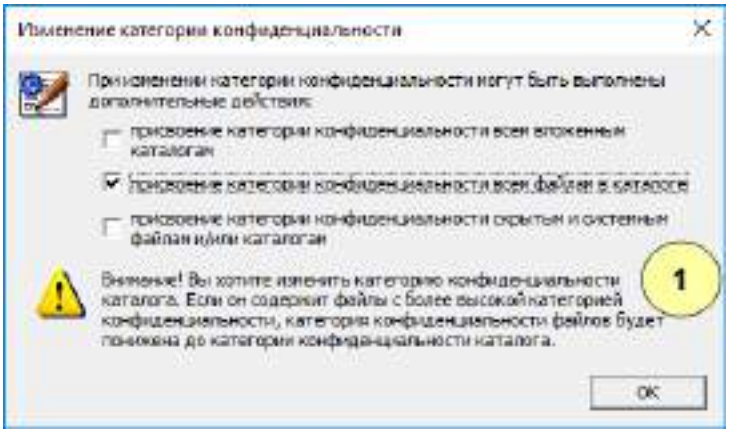
Для изменения категории конфиденциальности каталогов:

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 Studio".



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 обозначены: 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 и каталогам, отметьте поле "присвоение категории конфиденциальности скрытым и системным файлам и/или каталогам".

Внимание!

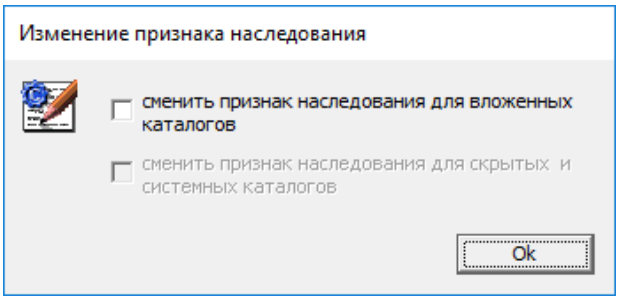
Во избежание нарушений в работе системы без особой необходимости не рекомендуется присваивать скрытым и системным файлам и каталогам категории конфиденциальности, отличающиеся от самой низшей категории (по умолчанию — "Неконфиденциально").

- 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.

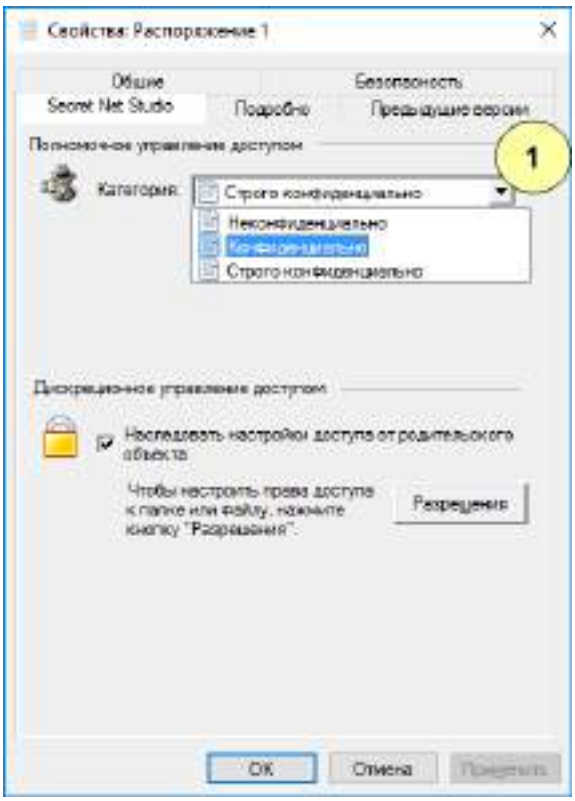
Если для каталога, содержащего подкаталоги, изменено значение параметра "Автоматически присваивать новым каталогам" или "Автоматически присваивать новым файлам", а категория конфиденциальности каталога осталась прежней, на экране появится диалог.



- 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 "ОК".

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 Studio".



Пояснение.
На рисунке обозначены: 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 "ОК".

Работа с конфиденциальным документом

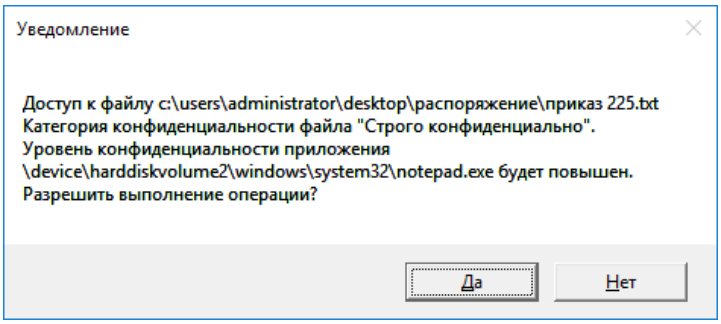
Прежде чем начать работу с конфиденциальными документами в программе редактирования (например MS Word), рекомендуется сохранить и закрыть все ранее открытые неконфиденциальные документы.

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".

Контроль печати

Печать документа с маркером системы Secret Net Studio

Если в Secret Net Studio 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:

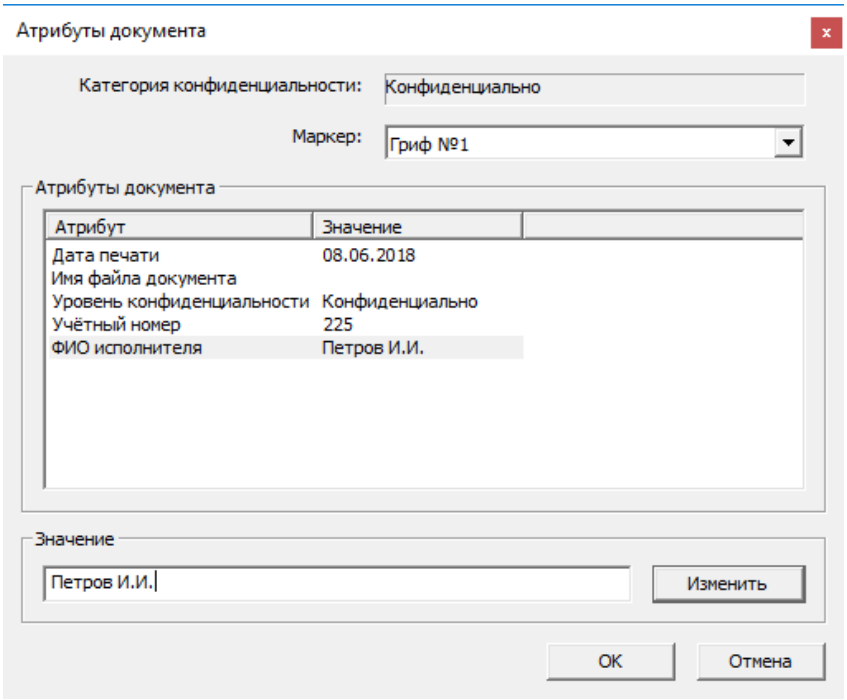
- обязательные поля, которые заполняются системой автоматически (например, "Дата", "Файл");
- настраиваемые поля, которые заполняются пользователем перед отправкой документа на печать (например, "Учетный номер").

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, подобный представленному на следующем рисунке.



4. При необходимости измените используемый маркер, выбрав нужное имя в поле "Маркер", и затем задайте значения для настраиваемых полей маркера. Для изменения значения выберите нужный атрибут в списке, в появившемся поле "Значение" введите данные и нажмите кнопку "Изменить".
5. Нажмите кнопку "OK".

   Документ будет распечатан вместе с маркером.

Работа с ключевой информацией

Ключевая информация пользователя размещается на ключевом носителе — в персональном идентификаторе или другом съемном носителе (например, USB-флеш-накопитель). Она необходима для работы с зашифрованными данными в криптоконтейнерах.

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. Смену ключевой информации можно выполнить самостоятельно либо обратиться для этого к администратору.

Загрузка и выгрузка криптографических ключей

Загрузка криптографических ключей пользователя происходит либо автоматически, либо принудительно по команде пользователя. Автоматическая загрузка выполняется во время процедуры входа пользователя в систему, если используется идентификатор, на котором также хранятся и криптографические ключи. Принудительная загрузка выполняется командой контекстного меню пиктограммы Secret Net Studio в системной области панели задач ОС Windows.

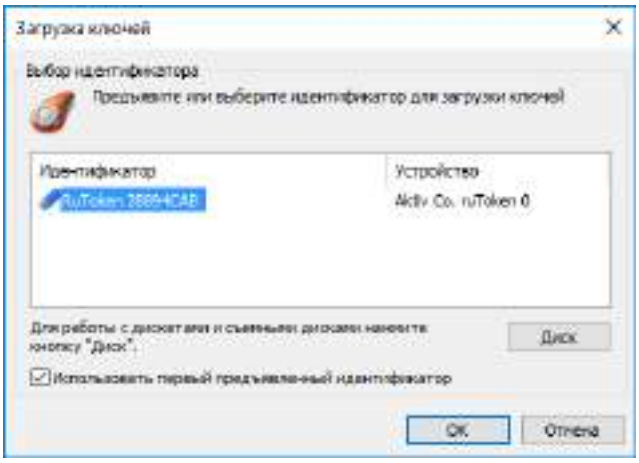
Выгрузка ключей может выполняться специальной командой или автоматически при завершении сеанса работы в системе.

Для принудительной загрузки криптографических ключей:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows и выберите команду "Загрузить ключи".

Примечание.
Команда доступна, если ключи не загружены в текущий момент.

На экране появится диалог.



2. Предъявите ключевой носитель. В зависимости от вида ключевого носителя (персональный идентификатор или съемный диск) выполните соответствующее действие:
   - если вы используете персональный идентификатор, предъявите его;
   - если вы используете в качестве ключевого носителя съемный диск, подключите его и нажмите кнопку "Диск".

     Совет.
     Если подключено несколько дисков, выберите в списке строку с названием нужного носителя и нажмите кнопку "ОК".

   Не прерывайте контакт ключевого носителя со считывателем до окончания чтения ключевой информации.

Для принудительной выгрузки криптографических ключей:

- Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows и выберите команду "Выгрузить ключи".

Примечание.
Команда доступна, если ключи загружены.

Смена ключевой информации

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

Процедура смены ключевой информации проводится в 2 этапа:

1. Смена ключевой информации на ключевом носителе.

   На ключевом носителе ключевая информация записана в двух экземплярах: действующий закрытый ключ пользователя и старый закрытый ключ (появляется после первой смены ключей). При загрузке ключевой информации система считывает как действующий, так и старый закрытый ключ.

   На первом этапе сначала генерируется новый закрытый ключ, который затем записывается на ключевой носитель на место действующего ключа. Предыдущий действующий ключ сохраняется в идентификаторе как старый ключ. А прежний старый ключ удаляется.

2. Обновление (перешифрование) управляющей информации в криптоконтейнерах — расшифрование на старом ключе и зашифрование на новом.

Для сохранения доступа к зашифрованной информации необходимо перешифровать управляющую информацию во всех доступных вам криптоконтейнерах. Процесс перешифрования управляющей информации запускается автоматически после смены ключей.

Внимание!

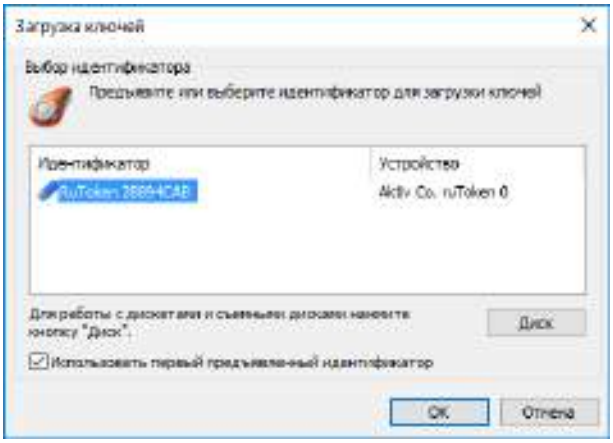
Автоматическое перешифрование управляющей информации возможно при условии доступности криптоконтейнера. Например, если криптоконтейнер недоступен по сети или находится на сменном носителе, который не подключен в данный момент, — перешифрование не происходит. В этом случае после смены ключей для перешифрования управляющей информации необходимо выполнить какую-либо операцию с таким криптоконтейнером (например, подключить криптоконтейнер) до следующей смены ключей. Иначе во время следующей смены ключей будет заменена предыдущая ключевая пара, и доступ к криптоконтейнеру будет невозможен из-за несовпадения ключей. Для возобновления доступа потребуется заново добавить пользователя в список имеющих доступ к криптоконтейнеру.

Для смены ключевой информации:

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

Примечание. Команда доступна, если ключи не загружены в текущий момент.

На экране появится диалог.

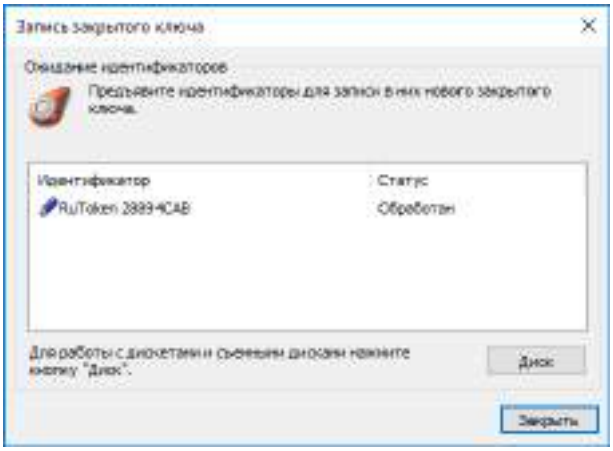


2. Предъявите один из ключевых носителей с текущей ключевой информацией. В зависимости от вида ключевого носителя (персональный идентификатор или съемный диск) выполните соответствующее действие:
   - если вы используете персональный идентификатор, предъявите его;
   - если вы используете в качестве ключевого носителя съемный диск, подключите его и нажмите кнопку "Диск".

Совет.

Если подключено несколько дисков, выберите в списке строку с названием нужного носителя 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, подключите его 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 или отключен съемный диск до окончания чтения.

Действия пользователя. Восстановите контакт между считывающим устройством и персональным идентификатором или подключите съемный диск. Нажмите кнопку "ОК".

Предъявленный персональный идентификатор не принадлежит текущему пользователю.
Предъявленный ключ пользователя не прошел проверку подлинности.
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 работы с зашифрованными данными в криптоконтейнерах.

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.

Операции с шифрованными ресурсами

Система Secret Net Studio предоставляет возможность шифрования содержимого объектов файловой системы (файлов и папок). Для операций зашифрования и расшифрования используются специальные хранилища — криптографические контейнеры или криптоконтейнеры. Криптоконтейнеры можно подключать к системе с локальных дисков, сменных носителей или с сетевых ресурсов.

Физически криптоконтейнер представляет собой файл, который можно подключить к системе в качестве дополнительного диска. Криптоконтейнер является образом диска, но все действия с ним выполняются через драйвер механизма шифрования. Драйвер обеспечивает работу с пользовательскими данными в контейнере в режиме "прозрачного шифрования". То есть пользователь, после подключения криптоконтейнера в качестве диска, выполняет операции с файлами на этом диске так же, как и на любом другом носителе. Дополнительных действий для зашифрования или расшифрования файлов не требуется, все криптографические операции с файлами выполняются автоматически.

После установки ПО Secret Net Studio в список системных ресурсов для хранения данных добавляется специальная папка "Криптоконтейнеры Secret Net Studio". Папка предназначена для выполнения действий со списком криптоконтейнеров. Для перехода к папке используйте ее ярлык в списке элементов управления объекта "Компьютер" в программе "Проводник".

Создание криптоконтейнера

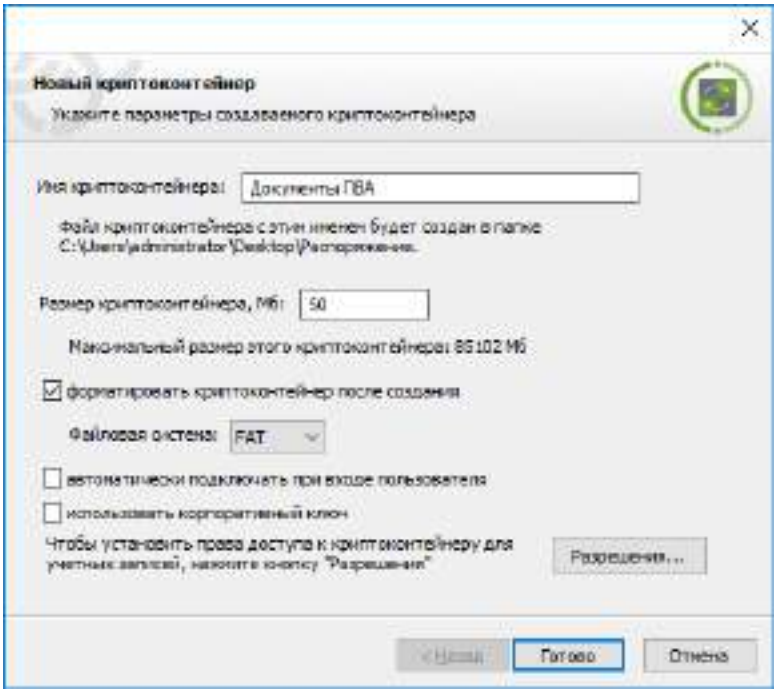
Создание криптоконтейнеров доступно пользователям с соответствующей привилегией. По умолчанию эта привилегия предоставлена всем учетным записям, которые входят в локальные группы администраторов или пользователей. Пользователь, создавший криптоконтейнер, получает право на управление им и в дальнейшем может делегировать (предоставить) это право доступа другому пользователю.

Запуск процедуры создания можно выполнить в каталоге, где будет размещен файл криптоконтейнера, или в списке криптоконтейнеров папки "Криптоконтейнеры Secret Net Studio".

Для создания криптоконтейнера в выбранном каталоге:

1. В программе "Проводник" выберите нужный каталог (папку), где будет размещен файл криптоконтейнера.
2. Вызовите контекстное меню и в подменю "Создать" выберите команду "Криптоконтейнер Secret Net Studio".

   На экране появится диалог мастера создания криптоконтейнера.

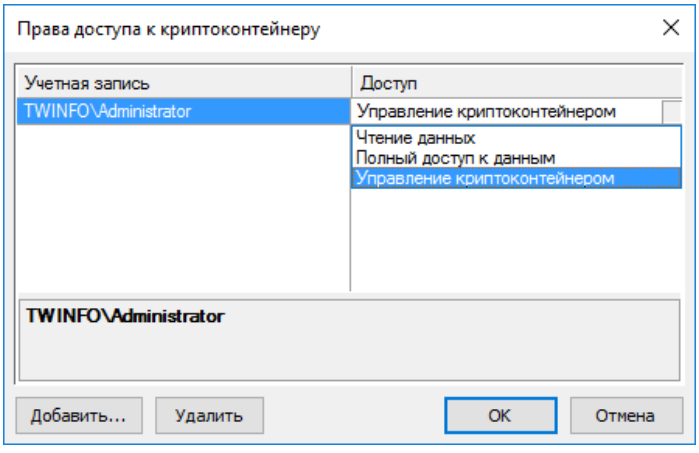


3. Введите имя и размер создаваемого криптоконтейнера в соответствующих полях.
4. Чтобы подготовить файловую систему криптоконтейнера сразу после его создания, установите отметку в поле "форматировать криптоконтейнер после создания" и выберите тип файловой системы.
5. При необходимости включите режим автоматического подключения криптоконтейнера при каждом входе пользователя в систему. Для этого установите отметку в поле "автоматически подключать при входе пользователя".
6. Чтобы усилить защиту криптоконтейнера, установите отметку в поле "использовать корпоративный ключ". В этом случае будет создан специальный ключ, обеспечивающий доступ к криптоконтейнеру только на этом компьютере (для работы с криптоконтейнером на других компьютерах потребуется скопировать ключ на эти компьютеры). При отсутствии отметки для криптоконтейнера не создается корпоративный ключ.

Примечание.
Корпоративный ключ сохраняется в системном реестре компьютера. Поэтому для создания ключа необходимы права на запись в реестр. По умолчанию такие права предоставлены пользователям локальной группы администраторов.

7. Сформируйте список учетных записей, которым будет предоставлен доступ к криптоконтейнеру. Для этого нажмите кнопку "Разрешения".

   На экране появится диалог для настройки прав доступа.



8. Отредактируйте список учетных записей с помощью кнопок "Добавить" и "Удалить". В список можно добавить только тех пользователей, для которых сгенерированы криптографические ключи. Для изменения прав доступа учетной записи выберите ее в списке и укажите нужное значение в ячейке колонки "Доступ" (чтобы раскрыть список возможных значений, нажмите кнопку в правой части ячейки).
9. Нажмите кнопку "OK" в диалоге настройки прав доступа.
10. В диалоге мастера создания криптоконтейнера нажмите кнопку "Готово".

    В выбранном каталоге будет добавлен файл криптоконтейнера, имеющий расширение .SnDisk.

Для создания криптоконтейнера при работе со списком криптоконтейнеров:

1. В папке "Криптоконтейнеры Secret Net Studio" вызовите контекстное меню в любом месте списка и выберите команду "Создать".

   На экране появится диалог мастера создания криптоконтейнера. Диалог отличается от приведенного в вышеописанной процедуре наличием поля для указания размещения файла криптоконтейнера.
2. В поле "Расположение криптоконтейнера" укажите каталог размещения файла и далее выполните действия вышеописанной процедуры, начиная с шага **3**.

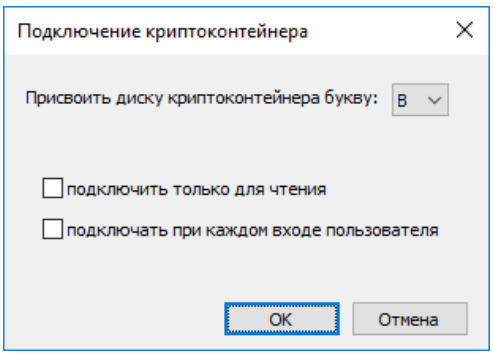
Подключение криптоконтейнера

При подключении криптоконтейнера в системе появляется дополнительный диск, образом которого является файл криптоконтейнера. После подключения можно выполнять операции с файлами на этом диске так же, как и на любом другом носителе (предварительно выполнив процедуру форматирования диска, если это не было сделано при создании криптоконтейнера).

Для подключения криптоконтейнера:

1. Загрузите криптографические ключи (см. стр.**38**).
2. Вызовите контекстное меню криптоконтейнера и выберите команду "Подключить".

   На экране появится диалог настройки параметров подключения.



3. Выберите букву диска в поле "Присвоить диску криптоконтейнера букву".
4. При необходимости настройте дополнительные параметры подключения:
   - чтобы защитить содержимое криптоконтейнера от записи — установите отметку в поле "подключить только для чтения";
   - чтобы включить режим автоматического подключения криптоконтейнера при входе в систему — установите отметку в поле "подключать при каждом входе пользователя".
5. Нажмите кнопку "OK".

   В списке дисков компьютера в программе "Проводник" появится новый элемент. В папке "Криптоконтейнеры Secret Net Studio" криптоконтейнер будет перемещен в раздел "Подключенные".

Отключение криптоконтейнера

При отключении криптоконтейнера из системы удаляется соответствующий дополнительный диск. После отключения будут невозможны любые действия с содержимым криптоконтейнера.

Подключенные криптоконтейнеры автоматически отключаются при завершении сеанса работы пользователя. Также предусмотрено принудительное отключение с использованием специальной команды.

Для принудительного отключения криптоконтейнера:

1. Закройте все открытые файлы, размещенные в криптоконтейнере.
2. В списке дисков компьютера в программе "Проводник" или в папке "Криптоконтейнеры Secret Net Studio" вызовите контекстное меню подключенного криптоконтейнера и выберите команду "Отключить".
3. При появлении диалога запроса подтвердите решение для продолжения операции.

   Логический диск криптоконтейнера будет удален из списка дисков компьютера в программе "Проводник". В папке "Криптоконтейнеры Secret Net Studio" он будет перемещен в раздел "Отключенные".

Просмотр и настройка параметров криптоконтейнера

При работе в папке "Криптоконтейнеры Secret Net Studio" предоставляется возможность открыть диалоговое окно для просмотра и настройки параметров криптоконтейнера. Изменение параметров доступно пользователям с правами на управление криптоконтейнером.

Чтобы открыть диалоговое окно, выберите криптоконтейнер в списке папки "Криптоконтейнеры Secret Net Studio", вызовите его контекстное меню и выберите команду "Свойства".

В диалоге представлены основные сведения о криптоконтейнере (состояние, размер и др.), а также средства для включения режима автоматического подключения и редактирования списка учетных записей с правами доступа. Настройка выполняется аналогично, как при создании криптоконтейнера (см. стр.**42**).

Перешифрование криптоконтейнера

При создании криптоконтейнера генерируется так называемый базовый ключ шифрования, на основе которого зашифрованы все остальные данные. Перешифрование всего содержимого криптоконтейнера происходит при смене базового ключа (в отличие от смены ключей пользователей, когда перешифруется только часть управляющей информации). В процессе эксплуатации системы следует регулярно выполнять смену как ключей пользователей, так и базовых ключей шифрования криптоконтейнеров.

Для перешифрования криптоконтейнеров:

1. В папке "Криптоконтейнеры Secret Net Studio" вызовите контекстное меню в любом месте списка и выберите команду "Смена ключа шифрования".

   На экране появится диалог со списком криптоконтейнеров.
2. Выберите в списке нужные криптоконтейнеры и нажмите кнопку "Сменить ключи".

Удаление криптоконтейнера

Подключенные криптоконтейнеры эксклюзивно управляются драйвером механизма шифрования. До отключения криптоконтейнера к нему не могут применяться операции удаления.

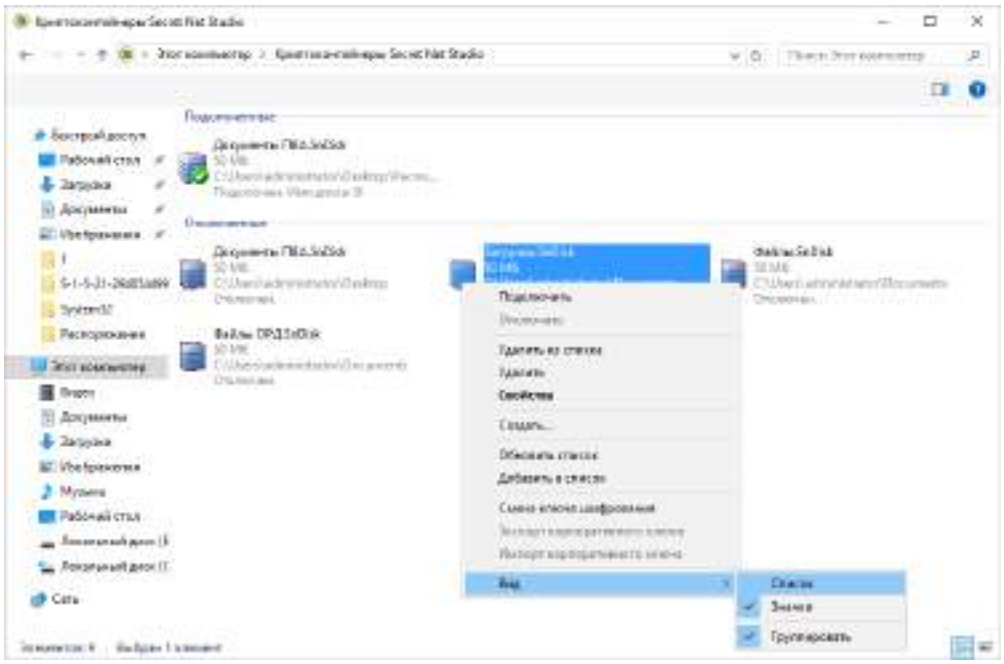
При работе со списком криптоконтейнеров в папке "Криптоконтейнеры Secret Net Studio" удалить отключенный криптоконтейнер можно в следующих вариантах:

- удаление только из списка криптоконтейнеров с оставлением самого файла криптоконтейнера в текущем размещении — для этого вызовите контекстное меню криптоконтейнера и выберите команду "Удалить из списка";
- удаление файла криптоконтейнера и записи о нем в списке криптоконтейнеров — для этого вызовите контекстное меню криптоконтейнера и выберите команду "Удалить".

Примечание.
Если файл криптоконтейнера был перенесен или удален из каталога размещения другими средствами (например, при работе с каталогом в программе "Проводник"), запись об этом контейнере остается в списке папки "Криптоконтейнеры Secret Net Studio" в разделе "Недоступные". Для удаления таких элементов также используется команда контекстного меню "Удалить из списка".

Управление списком криптоконтейнеров

Пример списка криптоконтейнеров в папке "Криптоконтейнеры Secret Net Studio" представлен на следующем рисунке.



Для управления списком могут использоваться команды контекстного меню.

Команда	Описание
Добавить в список	Запускает процедуру добавления криптоконтейнера из файла. Выбор криптоконтейнера осуществляется в стандартном диалоге открытия файла
Обновить список	Выполняет повторное чтение данных о наличии криптоконтейнеров в системе
Вид	Содержит команды переключения режимов отображения и группировки элементов

Глава 5
Работа с действующей доверенной средой

При функционирующей доверенной среде для включения компьютера необходим загрузочный носитель — специализированный USB-флеш-накопитель, содержащий служебную информацию.

Вход в систему, работа на компьютере и завершение работы осуществляются в обычном режиме.

Включение компьютера

Для включения компьютера при функционирующей доверенной среде:

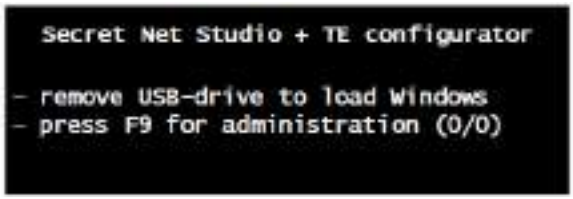
1. Подключите к компьютеру загрузочный носитель.

Внимание! При включении компьютера без загрузочного носителя выполнится загрузка операционной системы компьютера. На экране блокировки появится сообщение "Ошибка выполнения функционального контроля. Причины: доверенная среда не функционирует". Вход в систему будет невозможен.

2. Включите компьютер.

   Начнется процесс загрузки данных с загрузочного носителя.

   При успешной загрузке на экране появится меню доверенной среды.



Пояснение. При возникновении ошибок выключите компьютер, удерживая кнопку включения на системном блоке. Повторите попытку включения. Если ошибки все равно возникают, обратитесь к администратору.

3. Извлеките загрузочный носитель.

   Выполнится загрузка ОС компьютера.

4. Выполните вход в систему (см. стр.**14**) и работайте на компьютере в обычном режиме.

Глава 6
Работа с действующими средствами сетевой защиты

Персональный межсетевой экран

Для защиты компьютера от несанкционированного доступа, а также для разграничения сетевого доступа используется межсетевой экран Secret Net Studio.

Фильтрация сетевого трафика производится на основе формируемых для приложений правил, обладающих широким диапазоном настроек. Сетевые соединения могут быть ограничены на уровне пользователей, компьютеров, групп пользователей (компьютеров) и параметров соединения — служебных и прикладных протоколов, портов, сетевых интерфейсов, приложений, дня недели, времени суток.

Настройка межсетевого экрана осуществляется администратором в программе управления Secret Net Studio.

Глава 7
Работа с действующим антивирусом и средствами обнаружения вторжений

Принципы антивирусной защиты

Secret Net Studio осуществляет автоматическую проверку на наличие вредоносных программ на компьютере. При проверке осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств, сообщений электронной почты и др., позволяющее обнаружить и блокировать внешние и внутренние сетевые атаки, направленные на компьютер.

Примечание. Проверка файлов проводится только при наличии доступа на чтение файлов, папок. При отсутствии доступа на экране появится уведомление об ошибке, сканирование выполнено не будет.

Также возможен запуск проверки выбранных файлов, папок и дисков из контекстного меню Windows (см. стр.**49**).

При обнаружении зараженных объектов на экране появится соответствующее уведомление (кроме проверки по расписанию или сканирования подключаемых устройств). При автоматической проверке в соответствии с настроенными правилами будет выполнено одно из следующих действий: удаление зараженных файлов, изолирование файлов (перемещение в карантин), блокировка доступа к файлам, лечение. Восстановить файлы из карантина может только администратор в программе управления Secret Net Studio.

Внимание! Не рекомендуется запускать контекстное сканирование для сетевых папок. Зараженные файлы будут помещены в локальный карантин, поэтому восстановить их будет сложнее.

Примечание. Чтобы сбросить состояние тревоги после обнаружения вредоносной программы, вызовите контекстное меню пиктограммы Secret Net Studio, находящейся в системной области панели задач ОС Windows, и выберите команду "Сбросить состояние тревоги" (или дважды щелкните значок пиктограммы Secret Net Studio).

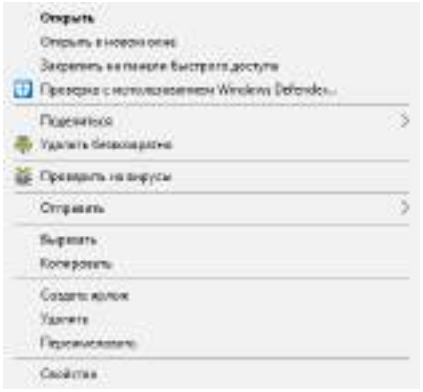
Настройка работы антивируса, выбор реакции на обнаруженные вредоносные программы и просмотр зараженных объектов осуществляются администратором централизованно в программе управления Secret Net Studio (см. документ "Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Контекстное сканирование

На защищаемом Secret Net Studio компьютере можно запустить проверку выбранных файлов, каталогов и дисков на наличие вирусов.

Для проверки файлов:

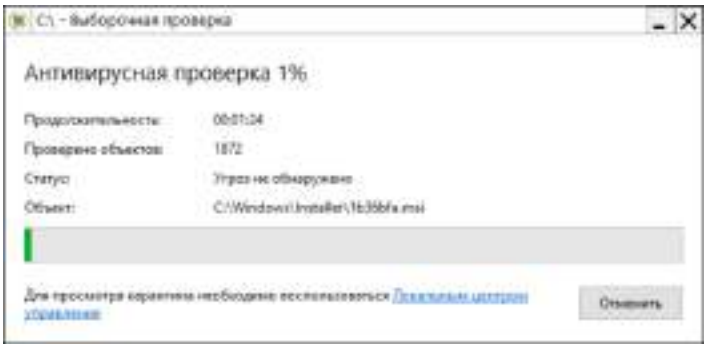
1. В программе "Проводник" вызовите контекстное меню для файла, каталога, диска или группы выбранных объектов.



2. Выберите команду "Проверить на вирусы".

Совет.
- Возможен одновременный запуск нескольких процедур сканирования.
- Если также требуется проверить и объекты из списка исключений, вызовите контекстное меню при нажатой клавише "Shift" и выберите команду "Проверить на вирусы (игнорировать белый список)".

Антивирус Secret Net Studio выполнит проверку файлов. Во время сканирования на экране появится следующее окно.



Совет. Чтобы прекратить сканирование, нажмите кнопку "Отменить" или закройте окно проверки.

3. По окончании проверки ознакомьтесь с полученным результатом и нажмите кнопку "Закрыть".

Чтобы просмотреть подробные результаты сканирования и список файлов в карантине, нажмите ссылку "Локальным центром управления" или в локальном центре управления Secret Net Studio на вкладке "Состояние" выберите объект "Антивирус" и в правой части окна перейдите на вкладку "Карантин".

Обнаружение вторжений

Secret Net Studio реализует обнаружение и блокирование внешних и внутренних вторжений, направленных на компьютер. Также осуществляется проверка сетевого трафика на предмет сетевых атак и блокировка атакующих компьютеров на заданный администратором промежуток времени.

При обнаружении атаки или при блокировке доступа к приложению на экране появится соответствующее уведомление.

Примечание. Чтобы сбросить состояние тревоги после обнаружения внешних или внутренних вторжений, вызовите контекстное меню пиктограммы Secret Net Studio, находящейся в системной области панели задач ОС Windows, и выберите команду "Сбросить состояние тревоги".

Настройка параметров механизма осуществляется администратором безопасности в программе управления Secret Net Studio.