КОД безопасности

Средство защиты информации

Secret Net Studio – C

Начало работы



© Компания "Код Безопасности", 2022. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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 ... **4**

Установка ... **5**

Подготовка к установке ... 5

Выбор компьютеров ... 5

Создание групп пользователей ... 6

Установка SQL-сервера ... 6

Установка сервера безопасности ... 8

Установка Центра управления ... 11

Централизованная установка клиента ... 11

Запуск Центра управления ... 11

Формирование списка устанавливаемого ПО ... 12

Формирование задания развертывания ... 12

Управление работой Secret Net Studio ... **15**

Интерфейс Центра управления ... 15

Мониторинг и оперативное управление ... 16

Настройка параметров безопасности ... 17

Работа с централизованными журналами ... 18

Документация ... **20**

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio – C" RU.88338853.501400.002 (далее — Secret Net Studio). В нем содержатся сведения, позволяющие администраторам быстро установить, ознакомиться и приступить к работе с Secret Net Studio.

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio – C" RU.88338853.501400.002 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения об использовании вспомогательных утилит и файлов настройки (далее — вспомогательные средства), необходимых 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.

Другие источники информации

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или 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
Установка

В качестве базового сценария развертывания Secret Net Studio для быстрого ознакомления выбран вариант установки в рамках одного домена Active Directory с одним сервером безопасности, одним рабочим местом администратора и несколькими защищаемыми компьютерами.

Установка выполняется в следующем порядке:

1. Подготовка к установке (см. ниже).
2. Установка сервера безопасности (см. стр.**8**).
3. Установка Центра управления (см. стр.**11**) на рабочем месте администратора.
4. Установка клиентов Secret Net Studio (см. стр.**11**) на всех защищаемых компьютерах централизованно с помощью Центра управления.

Примечание. В Secret Net Studio также поддерживается работа с аппаратными средствами защиты (например, с устройством ПАК "Соболь"). Однако в данном сценарии развертывания их установка не рассматривается. Подробные сведения об этом содержатся в разделе "Требования к аппаратному и программному обеспечению" документа [**1**].

Подготовка к установке

Прежде чем приступить к установке компонентов Secret Net Studio, необходимо выполнить ряд подготовительных действий.

Выбор компьютеров

В рамках одного домена Active Directory или организационного подразделения выберите компьютеры для размещения сервера безопасности, рабочего места администратора и нескольких клиентов Secret Net Studio. При выборе руководствуйтесь следующими рекомендуемыми требованиями к конфигурации компьютеров.

Совет. Подробные сведения об этом содержатся в разделе "Требования к аппаратному и программному обеспечению" документа [**1**].

Сервер безопасности

Требования к аппаратной конфигурации компьютера, на который устанавливается сервер безопасности:

Элемент	Требуется
Процессор	Intel Core i5/Xeon E3 и выше
Оперативная память	16 ГБ
Жесткий диск (свободное пространство)	150 ГБ. Рекомендуется использовать высокоскоростной жесткий диск
Операционная система	Windows Server 2022/2019/2016/2012 R2 Rollup Update KB2919355/2008 R2 SP1 KB3033929 (при наличии купленной поддержки производителя)

Дополнительно к компьютеру предъявляются следующие требования:

- на компьютере должны быть свободны и открыты TCP-порты 50000–50003. Если указанные порты заняты другими приложениями, при установке сервера безопасности будет предложено назначить другие порты для использования службами каталогов. Кроме того, должны быть открыты все TCP, UDP-порты, необходимые для функционирования компонентов ОС Windows в домене AD;

- в качестве языка программ, не поддерживающих стандарт кодирования Юникод, должен быть указан русский язык;
- для компьютера должна быть включена роль Веб-сервера (IIS).

Клиенты и Центр управления

Требования к аппаратной конфигурации компьютеров, предназначенных для рабочего места администратора и клиентов Secret Net Studio:

Элемент	Требуется
Процессор	В соответствии с требованиями ОС
Оперативная память	2 ГБ
Жесткий диск (свободное пространство)	4 ГБ
Операционная система и другое ПО	Windows 11/10/8.1 Rollup Update KB2919355/7 SP1 KB3033929 (при наличии купленной поддержки производителя) Windows Server 2022/2019/2016/2012 R2 Rollup Update KB2919355/2008 R2 SP1 KB3033929 (при наличии купленной поддержки производителя) Internet Explorer версии 8 или выше

В данном сценарии установка клиента выполняется централизованно под управлением сервера безопасности, поэтому в брандмауэре, если он включен, необходимо разрешить использование портов для доступа к общим ресурсам: UDP – 137, 138; TCP – 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа. Кроме того, должны быть открыты все TCP, UDP- порты, необходимые для функционирования компонентов ОС Windows в домене AD.

Создание групп пользователей

В рамках выбранного домена Active Directory создайте стандартными средствами администрирования ОС Windows две глобальные группы пользователей:

- группа администраторов домена безопасности;
- группа администраторов леса доменов безопасности (пользователи данной группы получат права на создание новых доменов безопасности в этом лесу).

Нужные права будут предоставлены данным группам в ходе установки сервера безопасности.

Включите в эти группы доменного пользователя, под именем которого будет выполняться установка компонентов и работа с Secret Net Studio.

Включите обе эти группы в локальную группу администраторов на компьютере, на котором будет установлен сервер безопасности. Группу администраторов домена безопасности также включите в локальную группу администраторов на всех компьютерах, выбранных для установки клиента Secret Net Studio.

Установка SQL-сервера

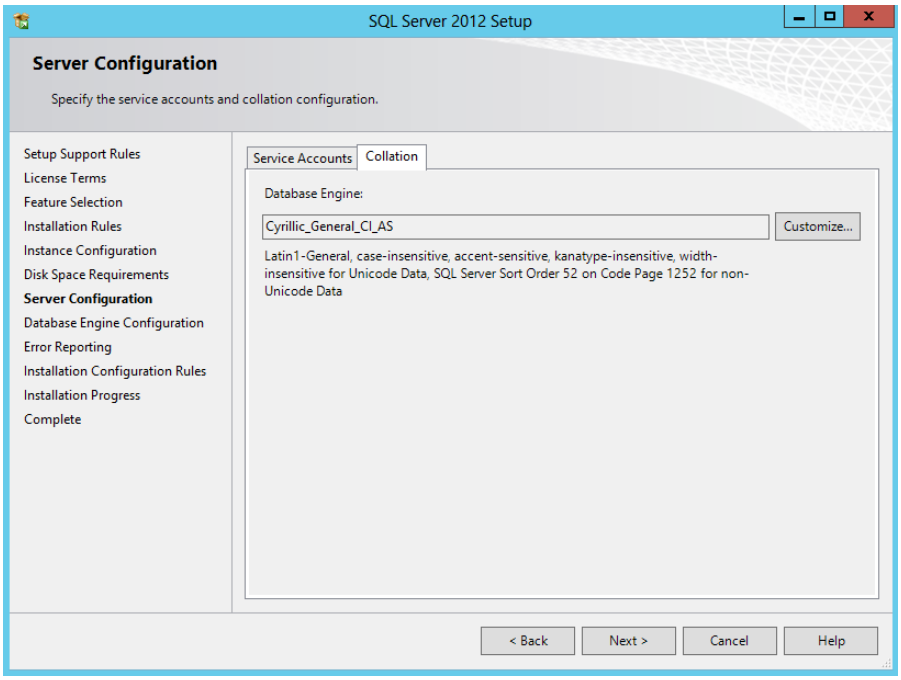
Для функционирования сервера безопасности требуется СУБД MS SQL. В том числе может быть использована бесплатно распространяемая версия MS SQL Server 2012 SP1 Express. В данном сценарии развертывания сервер безопасности и SQL-сервер устанавливаются на одном компьютере.

Совет. Если в организации уже есть установленный SQL-сервер, его также можно использовать. Сведения об этом см. в разделе "Сведения об установке и настройке СУБД MS SQL" документа [**1**].

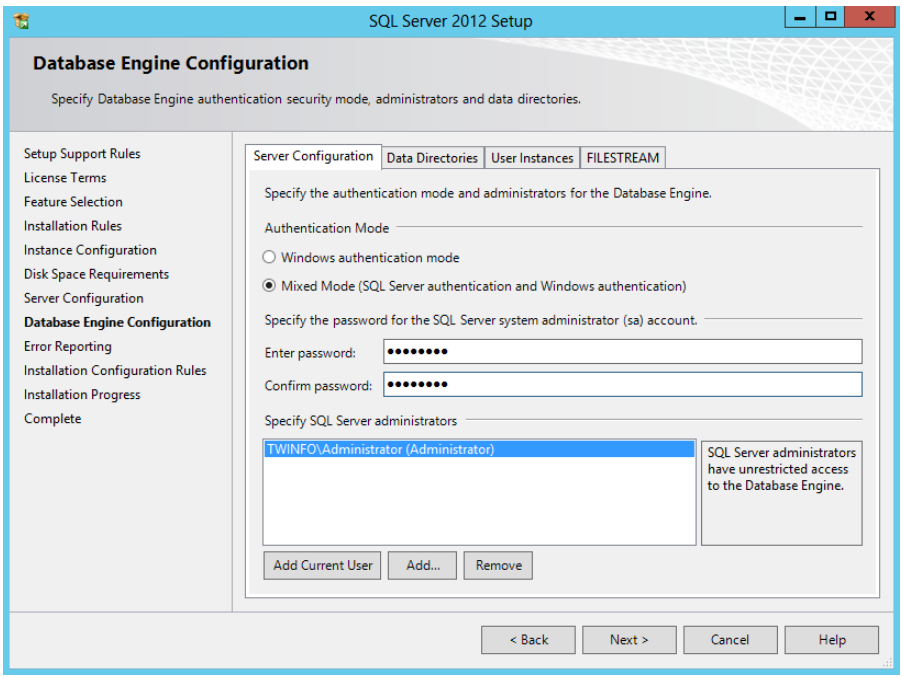
Перед установкой SQL-сервера необходимо включить в ОС Windows компонент .NET Framework 3.5. На компьютере с ОС Windows Server 2008 R2 также нужно установить .NET Framework 4.5 с языковым пакетом (файлы для установки dotNetFx45_Full_x86_x64.exe и dotNetFx45LP_Full_x86_x64ru.exe находятся в каталоге \Tools\Microsoft\Prerequisites на установочном диске).

Установку SQL-сервера следует выполнять с параметрами, заданными по умолчанию, за исключением значений следующих параметров, обеспечивающих корректное взаимодействие сервера безопасности и SQL-сервера.

- В разделе "Server Configuration" на вкладке "Collation" укажите в параметрах сортировки для компонента Database Engine значение Cyrillic_General_CI_AS, чтобы включить режим поддержки сортировки кириллицы для экземпляра базы данных.



- В разделе "Database Engine Configuration" на вкладке "Server Configuration" включите для SQL-сервера смешанный режим аутентификации (Mixed mode), обеспечивающий проверку подлинности и SQL Server, и Windows.



Совет. Более подробные сведения об установке и настройке СУБД MS SQL содержатся в разделе "Сведения об установке и настройке СУБД MS SQL" документа [1].

Установка сервера безопасности

На компьютере, который будет использоваться в качестве сервера безопасности, войдите в систему под именем доменного пользователя, входящего в локальную группу администраторов компьютера.

Для установки сервера:

1. Вставьте в привод установочный диск Secret Net Studio. При появлении окна программы автозапуска нажмите в нем кнопку "Сервер безопасности".

   Примечание. Если окно программы автозапуска не появилось, запуск установки нужно выполнить вручную. Для этого запустите с установочного диска файл \Setup\Server\x64\setup.ru-RU.exe.

   После запуска программы установки выполняется анализ системы на соответствие программным и аппаратным требованиям для установки компонента. При этом проверяется текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC).

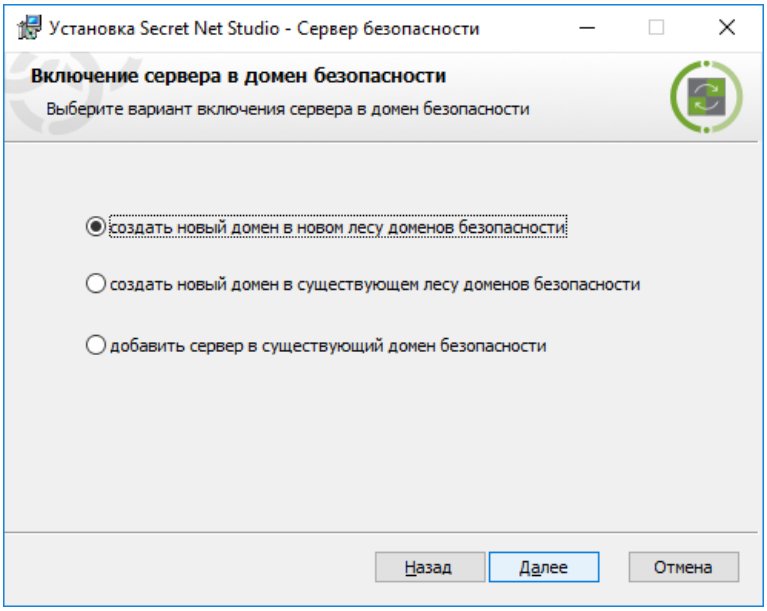
   Внимание! Если механизм UAC включен — на экране появится запрос на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и только после этого снова запустите процедуру установки сервера безопасности.

   По окончании проверки системы на экран будет выведен диалог с перечнем устанавливаемых компонентов.
2. Нажмите кнопку "Установить", оставив перечень без изменения.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
3. Для продолжения установки нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   На экране появится диалог "Включение сервера в домен безопасности".



5. Установите отметку в поле "создать новый домен в новом лесу доменов безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации".
6. Не меняйте значения параметров и нажмите кнопку "Далее".

   На экране появится диалог "Настройка домена безопасности".

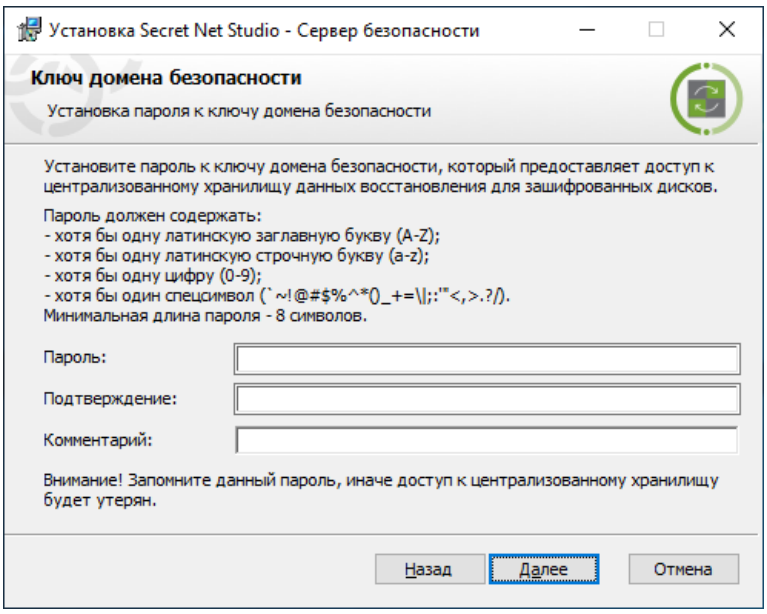
7. Выберите в раскрывающемся списке контейнер для формирования нового домена безопасности. Используйте организационное подразделение, в которое входят компьютеры, выбранные вами ранее для установки компонентов системы, или любое вышестоящее организационное подразделение (включая весь домен AD). После выбора контейнера при необходимости отредактируйте имя создаваемого домена безопасности.
8. Нажмите кнопку "Далее".

   На экране появится диалог "Группы администраторов безопасности".
9. Укажите созданные вами ранее на этапе подготовки группы пользователей, которым будут предоставлены права администрирования домена безопасности и леса доменов безопасности. Нажмите кнопку "Далее".

   Совет. В качестве группы администраторов домена безопасности не рекомендуется использовать стандартную доменную группу администраторов (Domain Admins). Иначе при подключении к серверу Центра управления, установленного на этом же компьютере, может возникать ошибка из-за недостаточных привилегий пользователя.

   На экране появится диалог "Настройка каталогов".
10. Оставьте заданные по умолчанию каталоги установки сервера безопасности и размещения служебных файлов и нажмите кнопку "Далее".

    На экране появится диалог "Ключ домена безопасности".

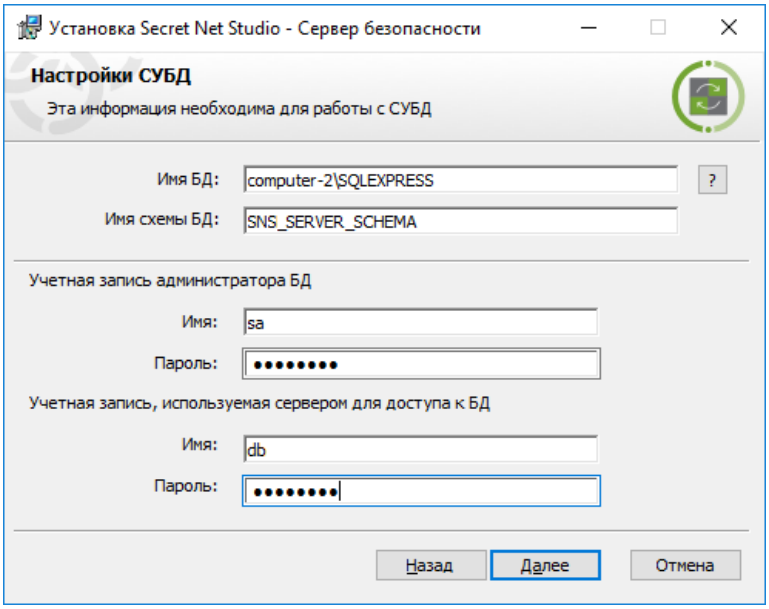


11. Установите пароль к ключу домена безопасности. Ключ и пароль предназначены для предоставления доступа к централизованному хранилищу данных восстановления для зашифрованных дисков. Пароль должен удовлетворять требованиям, указанным в диалоге.

    Внимание! Запомните пароль к ключу домена безопасности, иначе доступ к централизованному хранилищу данных восстановления будет утерян.

    Введите подтверждение пароля. При необходимости укажите комментарий к паролю. Нажмите кнопку "Далее".

    На экране появится диалог "Настройки СУБД". Пример содержимого диалога представлен на следующем рисунке.



12. Выполните следующие действия:

- Укажите параметры соединения с тем экземпляром БД, который предназначен для работы с устанавливаемым сервером безопасности:
  - в поле "Имя БД" укажите строку соединения с экземпляром БД: <имя данного компьютера>\SQLEXPRESS

    Пояснение. В нашем сценарии развертывания SQL-сервер устанавливается с параметрами по умолчанию на компьютере с сервером безопасности. Подробно формат строки соединения рассматривается в разделе "Создание леса и домена безопасности" документа [1].
  - в поле "Имя схемы БД" укажите наименование схемы БД;
  - в группе полей "Учетная запись администратора БД" укажите учетные данные администратора базы данных на SQL-сервере, заданные ранее при его установке;
  - в группе полей "Учетная запись, используемая сервером для доступа к БД" укажите учетные данные, с которыми сервер безопасности будет выполнять подключение к базе данных (будет создана учетная запись для подключения).
- Нажмите кнопку "Далее".

На экране появится диалог "Название организации".

13. Укажите названия организации и подразделения, которое будет обслуживать устанавливаемый сервер, и нажмите кнопку "Далее".

На экране появится диалог, сообщающий о готовности к установке.

14. Нажмите кнопку "Установить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

После успешной установки и настройки на экране появится сообщение, содержащее перечень выполненных операций установки и предупреждение о необходимости перезагрузки компьютера.

15. Нажмите кнопку "Перезагрузить".

Совет. Подробные сведения о различных вариантах установки сервера безопасности см. в разделе "Установка сервера безопасности" документа [1]. Если данный сервер безопасности предполагается использовать не только в ознакомительных целях, но и для построения системы защиты, рекомендуется в дальнейшем в созданном домене безопасности Secret Net Studio установить второй (резервный) сервер безопасности.

Установка Центра управления

Перейдите на компьютер, выбранный для организации рабочего места администратора безопасности, и войдите в систему под именем доменного пользователя, включенного в группу администраторов домена безопасности при выполнении подготовительных действий.

Для установки Центра управления:

1. Вставьте в привод установочный диск Secret Net Studio. При появлении окна программы автозапуска нажмите в нем кнопку "Центр управления".

   Совет. Если окно программы автозапуска не появилось, запуск установки нужно выполнить вручную. Для этого:
   - на компьютере с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\x64\setup.ru-RU.exe;
   - на компьютере с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\Win32\setup.ru-RU.exe.

   Программа установки выполнит подготовительные действия, по окончании которых на экране появится диалог приветствия.
2. Для продолжения установки нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее".

   На экране появится диалог "Конечная папка".
4. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее".

   На экране появится диалог, сообщающий о готовности к установке.
5. Нажмите кнопку "Установить".

   Начнется процесс установки, ход которого отображается в информационном окне в виде полосы прогресса. После успешной установки на экране появится диалог "Установка завершена".
6. Нажмите кнопку "Готово", а затем нажмите кнопку "Закрыть" в еще одном появившемся на экране диалоге.

Теперь можно приступить к установке клиентов на рабочие станции.

Централизованная установка клиента

Централизованная установка ПО клиента выполняется под управлением сервера безопасности. Для этого в Центре управления формируется список устанавливаемого ПО и создаются задания развертывания.

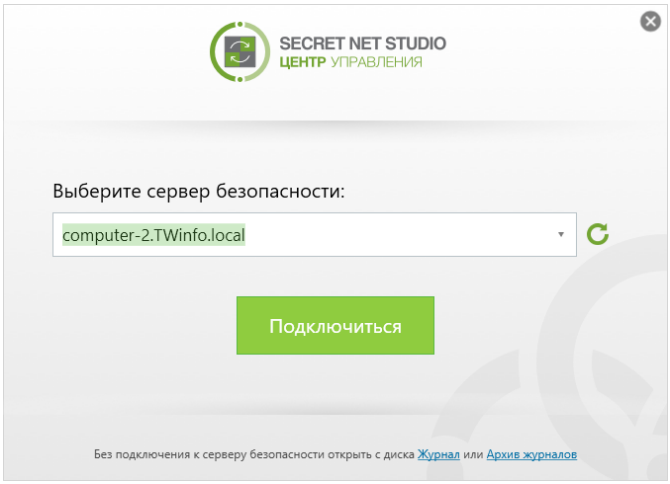
Внимание! Для успешного выполнения всех описанных ниже действий работающий на компьютере пользователь должен входить в группу администраторов домена безопасности.

Запуск Центра управления

Для запуска программы:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Центр управления".

   На экране появится стартовый диалог программы.



2. В поле "Выберите сервер безопасности" укажите имя установленного ранее сервера безопасности. Для обновления списка серверов нажмите кнопку справа от поля.
3. Нажмите кнопку "Подключиться".

После этого на экране появится основное окно программы.

Формирование списка устанавливаемого ПО

По умолчанию список централизованно устанавливаемого ПО пуст. Необходимо добавить в него комплект установочных файлов.

При первом запуске Центра управления в главном окне появится сообщение, предлагающее начать работу с системой и перейти к установке клиентов Secret Net Studio на компьютеры.

Для добавления комплекта установочных файлов:

1. Нажмите кнопку "Перейти на Развертывание".

   В главном окне Центра управления появится панель "Развертывание" и сообщение, предлагающее добавить дистрибутив Secret Net Studio.
2. Нажмите кнопку "Добавить".

   На экране появится диалог "Добавить дистрибутивы".
3. Вставьте в привод установочный диск Secret Net Studio, нажмите кнопку "Добавить", в появившемся диалоге выберите корневой каталог установочного диска и нажмите кнопку "Выбор папки".

   После считывания содержимого указанного каталога в диалоге "Добавить дистрибутивы" появится информация о выбранном установочном комплекте.
4. Нажмите кнопку "Применить".

   На экране появится диалог, отображающий процесс добавления файлов. Дождитесь окончания этого процесса.
5. Нажмите кнопку "Закрыть".

   В списке на вкладке "Репозиторий" появится новый элемент, содержащий сведения о загруженном комплекте установочных файлов.

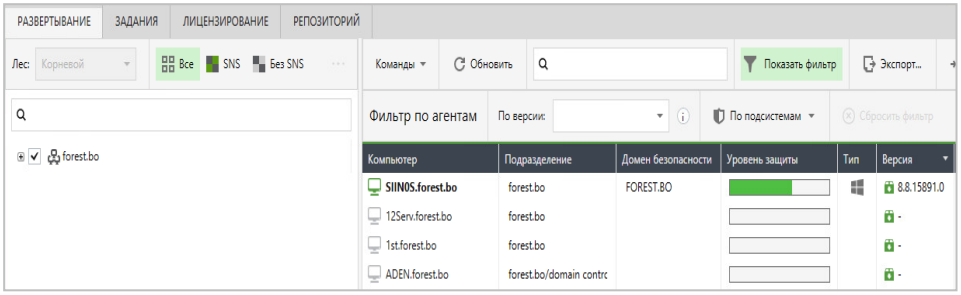
Формирование задания развертывания

После формирования списка централизованно устанавливаемого ПО необходимо добавить задание развертывания. Задание определяет список компьютеров, на которых в автоматическом режиме будут выполняться нужные действия.

Внимание! Для централизованной установки ПО на компьютеры пользователь, от имени которого выполняется установка (см. п.**6** процедуры), должен обладать правами локального администратора этих компьютеров. Предполагается, что при выполнении подготовительных действий группа администраторов домена безопасности была включена в локальные группы администраторов на всех нужных компьютерах, и доменный пользователь, включенный в эту группу, уже обладает всеми нужными правами.

Для добавления задания развертывания:

1. В панели "Развертывание" перейдите на вкладку "Развертывание".

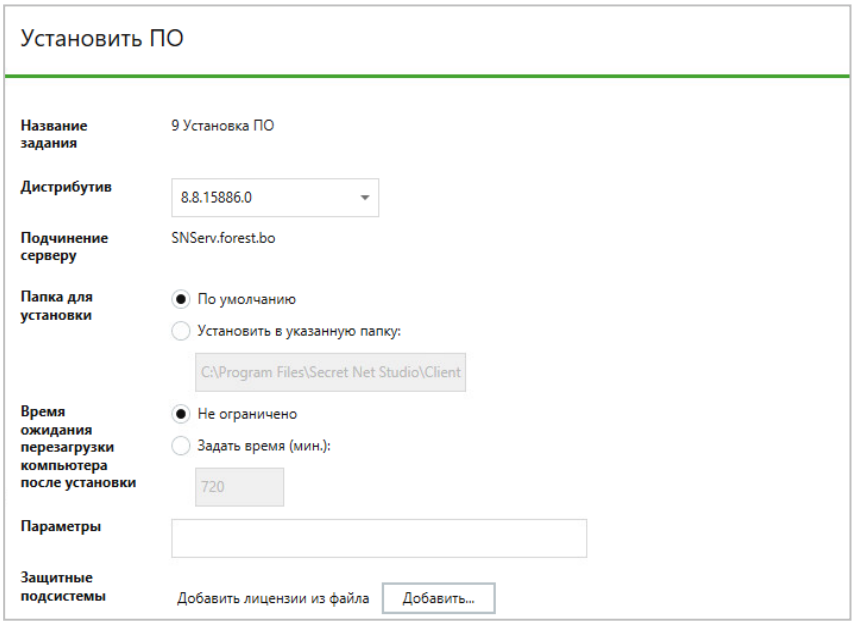


2. Слева в списке отметьте контейнеры AD с нужными компьютерами, а справа в списке выберите компьютеры, на которые нужно установить ПО клиента.

Совет. Выбор нескольких компьютеров выполняется, если нажата клавиша <Ctrl> или <Shift>.

3. Вызовите контекстное меню для одного из выбранных компьютеров и выберите команду "Установить ПО".

   В правой части окна появится панель настройки параметров задания.

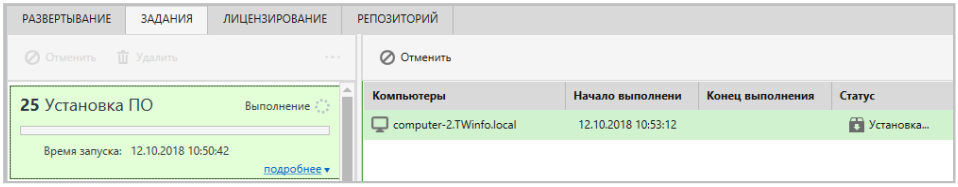


4. В группе полей "Время ожидания перезагрузки..." для включения режима автоматической перезагрузки выберите вариант "Задать время" и в поле ввода укажите, через сколько минут после завершения установки следует выполнить автоматическую перезагрузку компьютера.
5. В группе полей "Защитные подсистемы" добавьте лицензии на использование продукта. Для этого нажмите кнопку "Выбрать" и выберите в появившемся диалоге файл с лицензиями, предоставленный поставщиком.

   После загрузки данных в группе полей появятся сведения о лицензиях.
6. В полях "Имя" и "Пароль" введите учетные данные пользователя, имеющего права локального администратора на всех выбранных компьютерах.

Совет. Используйте учетные данные доменного пользователя, включенного в группу администраторов домена безопасности при выполнении подготовительных действий.

7. Нажмите кнопку "Установить" в нижней части панели.
8. Перейдите на вкладку "Задания" для наблюдения за ходом выполнения созданного задания.



На этой вкладке для заданий и компьютеров отображаются сведения о времени и статусе выполнения процесса установки.

Совет. Чтобы увидеть дополнительные сведения о задании, нажмите кнопку "Подробнее" в нижней части информационного блока. Для просмотра подробных сведений о каждом компьютере нажмите кнопку со стрелкой, которая расположена в правом нижнем углу списка компьютеров.

На защищаемых компьютерах установка ПО выполняется автоматически в фоновом режиме. Пользователь оповещается о начале и завершении установки.

После успешной установки клиента Secret Net Studio и перезагрузки компьютеров они через некоторое время появятся в структуре управления в качестве подчиненных объектов сервера безопасности.

Глава 2
Управление работой Secret Net Studio

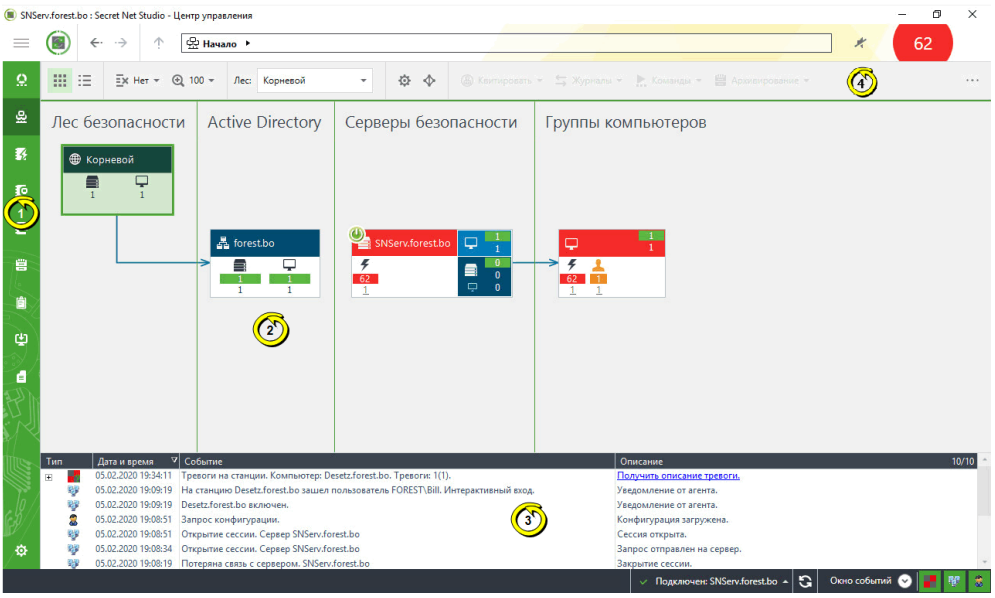
Центр управления Secret Net Studio используется для централизованного управления защищаемыми компьютерами (сведения о запуске программы см. на стр.**11**). Он позволяет выполнять следующие основные действия:

- настройка параметров защиты и управление компьютерами;
- мониторинг состояния системы;
- конфигурирование сетевой структуры Secret Net Studio;
- работа с централизованными журналами.

Примечание. В составе клиента Secret Net Studio устанавливается вариант Центра управления для работы в локальном режиме. Режим предназначен для локальной настройки параметров защиты, управления механизмами и просмотра локальных журналов данного компьютера. Возможности централизованного управления в этом режиме недоступны.

Интерфейс Центра управления

Пример внешнего вида основного окна программы представлен на рисунке ниже.



Основное окно программы состоит из следующих частей:

- панель навигации (1) — отображается в левой части основного окна и содержит ярлыки вызова панелей управления программы;
- панель "Компьютеры" (2) — предназначена для отображения сетевой структуры и выполнения действий с объектами;
- панель "События системы" (3) — содержит перечень событий, регистрируемых Secret Net Studio;
- средства навигации по сетевой структуре (4) — содержит кнопки для настройки режима отображения сетевой структуры и выполнения ряда других команд.

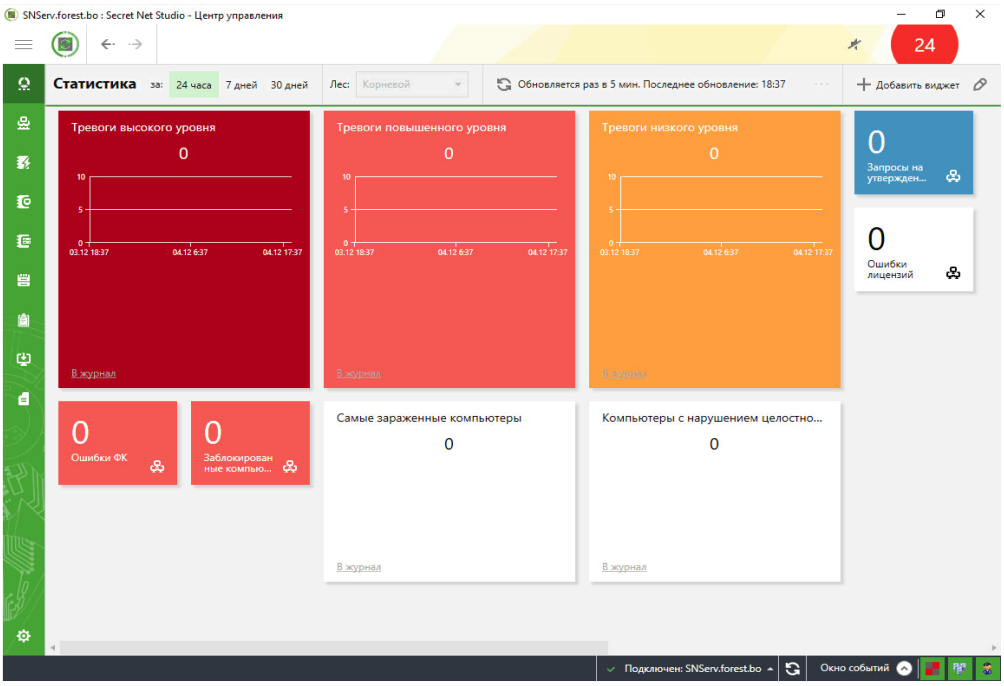
В программе имеются следующие панели управления:

Панель управления	Описание
Статистика	Содержит виджеты. Виджетом является визуальный элемент интерфейса программы, наглядно характеризующий один системный параметр
Компьютеры	Содержит средства управления компьютерами. Представляет собой схему элементов, соответствующих доменам, организационным подразделениям, серверам безопасности и защищаемым компьютерам
Журналы тревог	Содержит информацию о событиях тревоги, произошедших на защищаемых компьютерах. Формируется из уведомлений о событиях тревоги, направляемых серверу безопасности
Журналы станций	Содержит информацию о событиях, зарегистрированных в локальных журналах защищаемых компьютеров
Журналы сервера	Содержит информацию о сессиях доступа к серверу безопасности, открываемых компонентами и программами Secret Net Studio, включая внутренние сессии самого сервера
Архивы	Содержит средства работы с архивами журналов
Отчеты	Содержит средства для работы с отчетами
Развертывание	Содержит средства настройки автоматической установки и обновления ПО на компьютерах
Паспорт ПО	Содержит средства настройки механизма защиты "Паспорт ПО"
События системы	Содержит сведения об изменении состояния объектов системы

Совет. Подробные сведения о работе с панелями управления содержатся в документе [1].

Мониторинг и оперативное управление

Сведения об общем состоянии защищенности системы содержатся в информационной панели "Статистика", пример которой представлен на следующем рисунке. Для просмотра этих сведений нажмите кнопку "Статистика" вверху панели навигации (слева в основном окне).

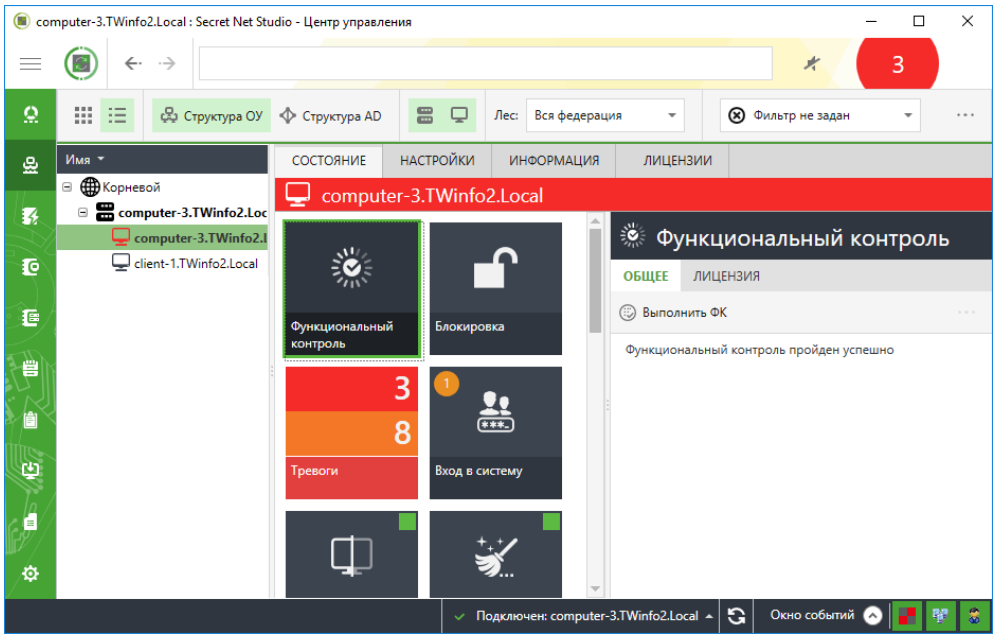


Информационная панель "Статистика" состоит из виджетов. Виджетом является визуальный элемент интерфейса программы, наглядно характеризующий один системный параметр. Панель по умолчанию содержит фиксированный набор виджетов с настроенными параметрами отображения.

Набор показанных на панели виджетов, параметры их отображения и их расположение на панели можно менять.

Совет. Подробные сведения о работе с панелью "Статистика" см. в разделе "Общее состояние системы" документа [1].

Сведения о состоянии компьютеров можно посмотреть в панели "Компьютеры" на вкладке "Состояние", имеющей вид, подобный представленному на рисунке.



Чтобы включить или отключить панель свойств, вызовите контекстное меню для объекта на диаграмме панели "Компьютеры" и выберите команду "Свойства".

Оперативное управление защищаемыми компьютерами можно осуществлять командами контекстного меню объекта на панели "Компьютеры" (подменю "Команды"). Команды оперативного управления могут применяться только к включенным компьютерам.

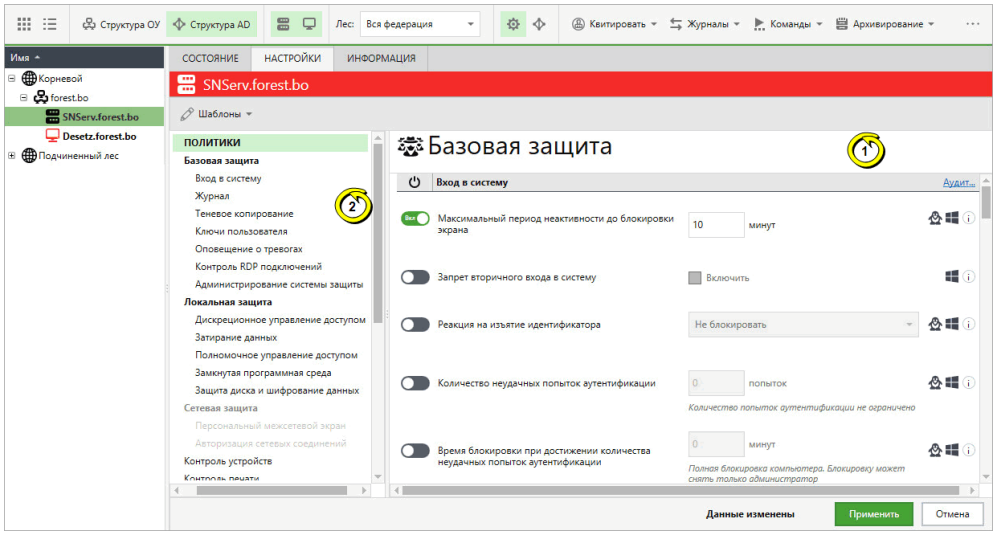
Совет. Подробные сведения о мониторинге и оперативном управлении см. в разделе "Мониторинг и оперативное управление" документа [1].

Настройка параметров безопасности

Управление параметрами безопасности осуществляется в панели "Компьютеры" на вкладке "Настройки", которая содержится в панели свойств объектов. Чтобы включить или отключить отображение панели свойств, вызовите контекстное меню для объекта на диаграмме и выберите команду "Свойства".

Для управления параметрами безопасности выбранного объекта необходимо загрузить параметры с сервера безопасности. Для этого перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки". Набор доступных параметров зависит от типа выбранного объекта. После загрузки параметров для их обновления используйте кнопку "Обновить" в верхней части вкладки.

Пример содержимого вкладки "Настройки" представлен на рисунке ниже.



Область отображения параметров (1) и область оглавления (2) разделены между собой передвигаемыми границами. При необходимости можно скрыть какую-либо область, передвинув ее границу.

Сделанные изменения вступают в силу после сохранения. Для сохранения изменений используйте кнопку "Применить" внизу вкладки.

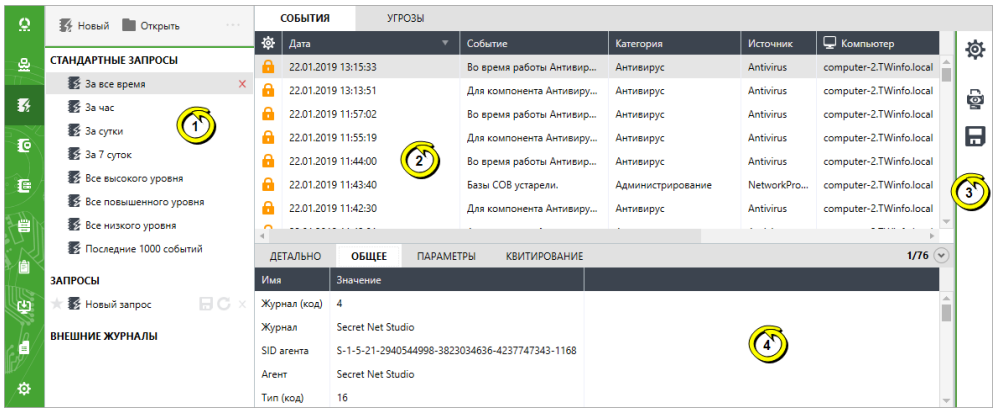
Совет. Подробные сведения о настройке параметров безопасности содержатся в разделе "Настройка параметров безопасности" документа [1].

Работа с централизованными журналами

В базе данных сервера безопасности накапливаются следующие журналы:

- журнал событий тревоги;
- журнал событий;
- журнал сервера безопасности.

К примеру, панель журнала событий тревоги имеет вид, подобный представленному на рисунке ниже.



На рисунке обозначены:

- 1 — панель управления запросами;
- 2 — область отображения сведений;
- 3 — панель настройки вывода сведений;
- 4 — область описания событий.

Просмотр и управление записями журналов, хранящихся в БД сервера безопасности, осуществляются только в Центре управления. Для загрузки записей в панели создается вкладка, называемая запросом.

Загруженная информация о событиях выводится в области отображения сведений соответствующей панели (см. рисунок выше). Для анализа содержимого журналов предусмотрены различные режимы отображения сведений.

В режиме "События" выводится список загруженных записей журналов в табличной форме. Это основной режим для просмотра и управления записями.

В режиме "Угрозы" выводится список событий угроз, полученных в результате анализа загруженных записей. События угроз представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях. Режим предназначен для представления администратору или аудитору наиболее важной для них информации из журналов.

Совет. Подробные сведения о работе с централизованными журналами содержатся в разделе "Работа с централизованными журналами" документа [**1**].

Документация

1. Средство защиты информации Secret Net Studio – C. Руководство администратора. Установка, управление, мониторинг и аудит	RU.88338853.501400.002 91 1
2. Средство защиты информации Secret Net Studio – C. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.002 91 2
3. Средство защиты информации Secret Net Studio – C. Руководство пользователя	RU.88338853.501400.002 92