КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

Континент-АП
Версия 3.7

Руководство администратора
Windows

RU.88338853.501430.007 91

© 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:	**http://www.securitycode.ru**

Оглавление

Введение

Данный документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент- АП". Версия 3.7" (далее — комплекс). В нем содержатся сведения, необходимые администратору для установки и настройки компонентов комплекса на платформе Windows.

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

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 http://www.securitycode.ru/company/education/training- courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Назначение и основные функции

С внедрением в повседневную работу различных средств обмена информацией в электронном виде актуальной становится проблема обеспечения ее конфиденциальности, целостности и авторства.

Изделие "Аппаратно-программный комплекс шифрования (АПКШ) "Континент" предназначено для безопасной передачи данных через общедоступные (незащищенные) сети. Эта технология называется "виртуальная частная сеть" (VPN). Защита данных обеспечивается криптографическими методами, вследствие чего через общедоступную сеть данные передаются в зашифрованном виде.

АПКШ "Континент" включает в свой состав компоненты, обеспечивающие удаленный доступ пользователей к ресурсам защищенной корпоративной сети с компьютеров, не входящих в защищаемые сегменты сети. На этих компьютерах устанавливается абонентский пункт, являющийся составной частью АПКШ. Абонентский пункт для передачи данных соединяется с сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к ресурсам защищенной сети.

В состав программного обеспечения комплекса входит межсетевой экран (далее — МСЭ), предназначенный для фильтрации IP-пакетов сетевого трафика компьютера, на котором установлен абонентский пункт.

МСЭ обеспечивает фильтрацию входящих и исходящих IP-пакетов по следующим признакам:

- IP-адреса отправителя и получателя;
- тип прикладного протокола (POP3, HTTP, SMTP и т. д.);
- сетевой интерфейс, через который пакет был получен или будет отправлен;
- поля заголовков и содержимомое IP-пакетов.

Кроме того, IP-пакеты фильтруются:

- по типу транспортного протокола (TCP/UDP/ICMP/…);
- по портам TCP/UDP;
- по типам и кодам протокола ICMP.

Проверка входящих и исходящих IP-пакетов осуществляется по правилам фильтрации и в соответствии с заданным расписанием.

События, происходящие при фильтрации сетевого трафика, регистрируются и сохраняются в журнале Terminal Station.

Ролевая аутентификация

В соответствии с требованиями безопасности пользователи комплекса разделяются по ролям на администраторов АП и пользователей АП.

Администратор АП — участник группы администраторов Windows (локальной или доменной).

Пользователь АП — участник любой группы "не администраторов" Windows.

Для высокого уровня безопасности (об уровнях безопасности см. стр. **9**) доступные пользователю комплекса функции и элементы интерфейса ограничиваются назначенной ему ролью. Роль пользователя в АП определяется по результатам аутентификации при входе в систему. Назначение ролей пользователям выполняют средствами СЗИ Secret Net/Secret Net Studio.

Примечание. Программное обеспечение СЗИ Secret Net устанавливается в составе ПО абонентского пункта. ПО СЗИ Secret Net Studio устанавливается отдельно.

Перечень функций и элементов интерфейса, доступных каждой из ролей, приведен в Приложении (см. стр.**40**).

Принципы функционирования МСЭ

Списки правил фильтрации

Межсетевой экран обрабатывает все входящие и исходящие IP-пакеты сетевого трафика. Порядок действий над IP-пакетами с заданными характеристиками определяется правилами фильтрации.

Предусмотрены два режима работы МСЭ: режим ожидания и режим работы пользователя.

В режиме ожидания МСЭ использует список правил сетевой фильтрации "Правила фильтрации до авторизации". Эти правила разрешают минимальное количество технических соединений, обеспечивающих работу компьютера в сети. Правила фильтрации до авторизации, действующие по умолчанию, устанавливаются совместно с программным обеспечением МСЭ (см. стр.**51**).

Для перехода к режиму работы необходимо предъявить пароль пользователя. В этом режиме МСЭ использует следующие списки правил фильтрации:

- "Правила фильтрации" — применяются для фильтрации IP-пакетов по полям заголовков протокола TCP/IP;
- "Правила прикладной фильтрации" — применяются для фильтрации IP-пакетов по полям заголовков и по содержимому пакетов.

В правилах прикладной фильтрации используется механизм регулярных выражений. С помощью этого механизма задают дополнительный признак: наличие в поле данных IP-пакета определенной последовательности символов.

Например, для протокола TFTP атрибутами могут быть коды выполняемых операций (запрос на запись или на чтение). Чтобы предотвратить несанкционированную передачу данных по протоколу TFTP, необходимо составить правило фильтрации, запрещающее передачу пакетов (на udp-порт #69), и задать дополнительный признак — наличие в передаваемых пакетах запросов на запись или на чтение.

Другим примером атрибута или информационного объекта является наличие команд сервера в поле данных IP-пакета для протоколов HTTP (GET, POST и т. д.). В этом случае для запрета передачи или отправки данных к правилу фильтрации необходимо добавить регулярное выражение, содержащее в явном виде наименование команды. Также в качестве информационного объекта может быть указан фрагмент текста, на основании которого можно сделать вывод о передаче той или иной информации.

В списках правил, используемых в режиме работы пользователя, по умолчанию содержится единственное правило, разрешающее прохождение через МСЭ любых IP-пакетов.

Списки правил фильтрации состоят из последовательных записей правил, по одному правилу в каждой строке. Описание языка правил фильтрации приведено в Приложении (см. стр.**41**). Примеры правил фильтрации см. стр.**48**.

Период работы правила фильтрации определяется расписанием. Для этого правило должно иметь флаг sched с указанием идентификатора расписания.

Управление правилами фильтрации возможно только после предъявления пароля администратора МСЭ.

Порядок обработки IP-пакетов

Входящие и исходящие IP-пакеты проверяются на соответствие правилам фильтрации. Проверка начинается с первого правила в списке и производится до тех пор, пока не будет найдено правило, удовлетворяющее данному пакету. При совпадении характеристик IP-пакета с их описанием в правиле фильтрации осуществляется предусмотренное правилом действие и дальнейшая проверка этого пакета на соответствие оставшимся правилам не выполняется.

При пустом списке правил фильтрации IP-пакеты не пропускаются.

Контроль целостности установленного ПО

Функция контроля целостности (КЦ) предназначена для слежения за неизменностью содержимого установленного программного обеспечения абонентского пункта. Действие функции основано на сравнении текущих значений содержимого контролируемых файлов и значений, принятых за эталон.

Эталонные значения рассчитываются при установке или обновлении программного обеспечения абонентского пункта. Контролю подлежат все служебные файлы абонентского пункта (см.стр.**55**), размещенные в каталоге установки и системных папках ОС Windows.

Рассчитанные при установке программного обеспечения контрольные суммы для контролируемых файлов и полные пути к ним содержатся в файле integrity.xml каталога установки.

Проверка контрольных сумм выполняется в следующих случаях:

- автоматически при запуске операционной системы;
- автоматически при попытке соединения с сервером доступа;
- вручную по команде оператора.

Результаты проверки заносятся в журнал приложений ОС Windows. При отрицательном результате автоматической проверки на экран выводится сообщение "Нарушена целостность файлов абонентского пункта. Обратитесь к системному администратору" или "Тест контроля целостности не пройден. Продолжение работы невозможно, обратитесь к системному администратору".

При отрицательном результате проверки соединение абонентского пункта с сервером доступа установлено не будет.

Порядок действий при отрицательном результате проверки контроля целостности приведен в документе "Средство криптографической защиты информации "Континент-АП". Версия 3.7. Правила пользования" RU.88338853.501430.007 93 (см. п. 7.13.7).

Если комплекс устанавливается с высоким уровнем безопасности (см. стр.**9**), контроль целостности выполняется средствами СЗИ Secret Net. В этом случае эталонные значения рассчитываются при выполнении задания на КЦ в Secret Net. Кроме того, средствами Secret Net предусмотрена реализация режима замкнутой программной среды, которая представляет собой перечень ресурсов, разрешенных для запуска программ, библиотек и сценариев.

Описание настройки и управления защитными механизмами контроля целостности и замкнутой программной среды приведено в эксплуатационной документации СЗИ Secret Net.

Установка, изменение и удаление

Программное обеспечение комплекса поставляется на компакт-дисках.

Перед установкой комплекса убедитесь, что компьютер удовлетворяет всем требованиям, предъявляемым к аппаратному и программному обеспечению.

Программное обеспечение комплекса устанавливается в соответствии с одним из трех вариантов, обеспечивающим необходимый уровень безопасности:

- низкий — соответствует классу КС1;
- средний — соответствует классу КС2;
- высокий — соответствует классу КС3.

Предусмотрены два варианта программы установки ПО комплекса:

- обычная установка — используется для низкого и среднего уровня безопасности;
- расширенная установка, включающая в себя установку ПО Secret Net, — используется для высокого уровня безопасности.

В зависимости от выбираемого варианта установка имеет следующие особенности:

Низкий	Устанавливаются: • ПО абонентского пункта и межсетевого экрана; • биологический датчик случайных чисел; • ПО "Код Безопасности CSP"
Средний	Требуется наличие следующих компонентов: • плата и ПО ПАК "Соболь"; • ПО "КриптоПро CSP" (при необходимости использования данного ПО). Устанавливаются: • ПО абонентского пункта и межсетевого экрана; • физический датчик случайных чисел; • ПО "Код Безопасности CSP"
Высокий	Требуется наличие следующих компонентов: Устанавливаются: • ПО абонентского пункта и межсетевого экрана; • ПО Secret Net (если используется); • ПО "Код Безопасности CSP"

Требования к аппаратному и программному обеспечению

Абонентский пункт

Комплекс предназначен для использования на компьютерах, оснащенных процессорами семейства Intel X86 или совместимыми с ними. Требования к конфигурации компьютеров приведены в таблице ниже.

Элемент	Минимально	Рекомендуется
Жесткий диск (свободное пространство)	512 МБ	512 МБ
Процессор **Оперативная память**	В соответствии с требованиями ОС, установленной на компьютер	

Элемент	Минимально	Рекомендуется
Операционная система	Windows Server 2008 R2 SP1 x64 (только Standard и Enterprise Edition); Windows 7 SP1 (кроме всех выпусков Starter и Home Edition); Windows 8.1; Windows Server 2012 R2 Standard; Windows 10 (кроме всех выпусков Home Edition), начиная с версии 1703. Только для низкого и среднего уровня безопасности	
Установленное ПО	**Низкий уровень безопасности** MS Internet Explorer версии 6.0 и выше	
	Средний уровень безопасности ПАК "Соболь" 3.0, 3.1, 3.2; ПО "КриптоПро CSP" версии 4.0 (при необходимости); MS Internet Explorer версии 6.0 и выше	
	Высокий уровень безопасности ПАК "Соболь" 3.0, 3.1, 3.2;; ПО "КриптоПро CSP" версии 4.0; Secret Net 7.4 (не поддерживается работа с ОС Windows 10); MS Internet Explorer версии 6.0 и выше	
Ключевое устройство	Дискета 3,5"; USB-флеш-накопитель; USB-ключ eToken PRO (Java); Смарт-карта eToken Pro (Java) с USB-считывателем Athena ASEDrive IIIe USB V2; Рутокен S/ ЭЦП; iButton DS1994/ DS1995/ DS1996; Secret Net Card/ Secret Net Touch Memory Card; JaCarta PKI, JaCarta ГОСТ	

На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевыми протоколами TCP/IP.

Внимание!

- Все службы, реализующие штатные механизмы удаленного управления операционной системой, должны быть отключены.
- Если на компьютере используется UEFI с возможностью включения и отключения опции безопасной загрузки (Secure Boot), перед установкой АП данную опцию необходимо отключить. В противном случае установка АП завершится с ошибкой.
- Пропускная способность сетевого канала, по которому устанавливается соединение абонентского пункта с сервером доступа, должна быть не менее 9,6 Кбит/с.
- Компьютер, на который устанавливают абонентский пункт, при необходимости соответствия определенному уровню безопасности должен содержать средства, обеспечивающие контроль целостности программного обеспечения (например ПАК "Соболь").
- При использовании абонентского пункта совместно с ПАК "Соболь", а также с криптопровайдером "КриптоПро CSP" необходимо перед установкой абонентского пункта установить эти аппаратные и программные продукты согласно эксплуатационной документации на них. В зависимости от требований устанавливаемого уровня безопасности, настроить "КриптоПро CSP" на использование аппаратного датчика случайных чисел ПАК "Соболь". В случае если ПАК "Соболь" не используется, требуется настроить любой другой датчик случайных чисел, например биологический.
- Потери в канале связи должны быть не более 80%.

Установка абонентского пункта и межсетевого экрана

Пакет установки комплекса содержит следующие компоненты:

- абонентский пункт;
- программа установки ПО Secret Net;
- межсетевой экран.

В состав абонентского пункта входит криптопровайдер "Код Безопасности CSP".

Установка МСЭ без абонентского пункта невозможна.

Внимание! В процессе установки абонентского пункта все работающие сетевые подключения будут автоматически разорваны. Для их восстановления необходима перезагрузка компьютера. Работа установленных компонентов комплекса возможна также только после перезагрузки компьютера.

Примечание. Имеется возможность установки программного обеспечения комплекса из командной строки (см. стр. 15).

Установка программного обеспечения низкого и среднего уровня безопасности

Для установки программного обеспечения:

1. Войдите в систему с правами администратора компьютера.

   Примечание. Правами администратора компьютера обладает пользователь, входящий в локальную группу администраторов.

2. Завершите работу всех приложений, выполняющихся на компьютере.
3. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл ts_ setup.exe, находящийся в каталоге с дистрибутивом комплекса.

   Примечание. Для установки с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог и запустите на исполнение файл ts_setup.exe.

   Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера установки.

   Совет. Для управления процессом установки используйте кнопки:
   - "Назад" — для возврата к предыдущему диалогу;
   - "Далее" — для перехода к следующему диалогу;
   - "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

4. Нажмите кнопку "Далее >" для продолжения установки.

   На экране появится диалог "Лицензионное соглашение".

5. Прочтите лицензионное соглашение, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее >".

   На экране появится диалог "Компоненты устанавливаемой программы".

6. Если установка межсетевого экрана не требуется, удалите отметку у компонента "Брэндмауэр".

   Нажмите кнопку "Далее >".

   На экране появится диалог "Выбор папки установки". По умолчанию программа установки копирует файлы на системный диск в каталог \Program Files\Security Code\Terminal Station.

   Примечание. Для установки программы в другую папку нажмите кнопку "Обзор..." и укажите нужную папку в диалоге, появившемся на экране.

7. Нажмите кнопку "Далее >".

На экране появится диалог "Конфигурация АП".

8. Укажите нужные значения параметров, выберите требуемый уровень безопасности (низкий или средний) и нажмите кнопку "Установить".

Имя RAS-соединения	Наименование подключения к RAS-серверу (по умолчанию "Континент-АП")
Адрес сервера доступа	IP-адрес или сетевое имя сервера доступа (по умолчанию 0.0.0.0)

Если в состав устанавливаемых компонентов межсетевой экран не входит, начнется установка. Дождитесь завершения установки и перейдите к **п. 10**.

Если должен быть установлен межсетевой экран, на экране появится окно с вопросом о вхождении данного компьютера в домен.

Укажите — входит ли данный компьютер в домен и нажмите кнопку "Далее >".

На экране появится окно настроек межсетевого экрана.

Логин администратора	Логин и пароль для перехода МСЭ к режиму настройки (по умолчанию логин "Администратор", пароль "111111")
Пароль администратора	
Пароль пользователя	Пароль для перехода МСЭ к режиму работы пользователя (по умолчанию "111111")

9. Укажите нужные значения и нажмите кнопку "Установить".

Программа установки приступит к копированию файлов в указанную папку. Полоса прогресса и сообщения, появляющиеся в диалоге, отображают ход процесса установки.

Примечание. В процессе установки на экране могут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".

Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику комплекса.

По окончании процесса копирования в верхней части диалога появится сообщение "Установка завершена", а кнопка "Далее >" станет активной.

10. Нажмите кнопку "Далее >".

На экране появится заключительное окно мастера установки с запросом на перезагрузку компьютера.

Внимание! Работа установленных компонентов возможна только после перезагрузки компьютера.

11. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

Внимание! Для уровня безопасности "Низкий" после перезагрузки и автоматического запуска абонентского пункта появится диалоговое окно встроенного криптопровайдера "Код Безопасности CSP". В этом диалоге выполняют набор энтропии, необходимой для дальнейшей работы криптопровайдера. Следуйте указаниям, отображаемым в данном диалоге.

После установки абонентского пункта и перезагрузки компьютера:

- в элементе управления Windows "Панель управления \ Сетевые подключения" появится новое сетевое подключение "Континент-АП";
- в меню "Все программы" главного меню Windows появится подменю "Код Безопасности \ Континент АП 3.7", которое содержит пункты "VPN клиент", "Код Безопасности CSP", "Контроль целостности", "Брэндмауэр", "Удаление Континент АП";
- на панели задач Windows появится пиктограмма абонентского пункта (в случае полной установки дополнительно появятся пиктограмма межсетевого экрана и сообщение об ограничении доступа к сети).

Установка программного обеспечения высокого уровня безопасности

Процедура установки программного обеспечения абонентского пункта включает в себя установку ПО Secret Net.

Внимание! Работа Secret Net с ОС Windows 10 не поддерживается.

Для установки с ПО Secret Net:

1. Войдите в систему с правами администратора компьютера.

   Примечание. Правами администратора компьютера обладает пользователь, входящий в локальную группу администраторов.

2. Завершите работу всех приложений, выполняющихся на компьютере.
3. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл ts_sn_setup.exe, находящийся в каталоге с дистрибутивом комплекса.

   Примечание. Для установки с жесткого диска скопируйте файлы с установочного диска в любой рабочий каталог и запустите на исполнение файл ts_setup.exe.

   Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экран будет выведен стартовый диалог мастера установки.

   Совет. Для управления процессом установки используйте кнопки:
   - "Назад" — для возврата к предыдущему диалогу;
   - "Далее" — для перехода к следующему диалогу;
   - "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

4. Нажмите кнопку "Далее >" для продолжения установки.

   На экране появится диалог "Лицензионное соглашение".

5. Прочтите лицензионное соглашение, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее >".

   На экране появится диалог "Компоненты устанавливаемой программы".

6. Если установка межсетевого экрана не требуется, удалите отметку у компонента "Брэндмауэр".

   Нажмите кнопку "Далее >".

   На экране появится диалог "Выбор папки установки". По умолчанию программа установки копирует файлы на системный диск в каталог \Program Files\Security Code\Terminal Station.

   Примечание. Для установки программы в другую папку нажмите кнопку "Обзор..." и укажите нужную папку в диалоге, появившемся на экране.

7. Нажмите кнопку "Далее >".

   На экране появится диалог "Конфигурация АП".

8. Укажите нужные значения параметров и нажмите кнопку "Установить" (если установка выполняется без межсетевого экрана) или "Далее>" (если установка выполняется с межсетевым экраном).

Имя RAS-соединения	Наименование подключения к RAS-серверу (по умолчанию "Континент-АП")
Адрес сервера доступа	IP-адрес или сетевое имя сервера доступа (по умолчанию 0.0.0.0)

Если в состав устанавливаемых компонентов межсетевой экран не входит, начнется установка и программа установки приступит к копированию файлов в указанную папку. Полоса прогресса и сообщения, появляющиеся в диалоге, отображают ход процесса установки. Дождитесь появления окна выбора режима работы Secret Net (сетевой или автономный) и перейдите к **п. 11**.

Если должен быть установлен межсетевой экран, на экране появится окно с вопросом о вхождении данного компьютера в домен.

9. Укажите — входит ли данный компьютер в домен и нажмите кнопку "Далее >".

На экране появится окно настроек межсетевого экрана.

Логин администратора	Логин и пароль для перехода МСЭ к режиму настройки (по умолчанию логин "Администратор", пароль "111111")
Пароль администратора	
Пароль пользователя	Пароль для перехода МСЭ к режиму работы пользователя (по умолчанию "111111")

10. Укажите нужные значения и нажмите кнопку "Установить".

Программа установки приступит к копированию файлов в указанную папку. Полоса прогресса и сообщения, появляющиеся в диалоге, отображают ход процесса установки.

Примечание. В процессе установки на экране могут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".

Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику комплекса.

Дождитесь появления окна выбора режима работы Secret Net (сетевой или автономный).

11. Выберите автономный режим работы Secret Net "Автономный" и нажмите кнопку "Далее>".

На экране появится стартовое окно программы установки Secret Net.

12. Нажмите кнопку "Далее>" и выполните установку Secret Net в соответствии с прилагаемой на установочном диске документацией.

После завершения установки Secret Net продолжится установка программного обеспечения абонентского пункта.

Дождитесь завершения установки.

13. В окне с сообщением об успешном завершении нажмите кнопку "Далее>".

На экране появится заключительное окно мастера установки с запросом на перезагрузку компьютера.

Внимание! Работа установленных компонентов возможна только после перезагрузки компьютера.

14. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

После установки абонентского пункта и перезагрузки компьютера:

- в элементе управления Windows "Панель управления \ Сетевые подключения" появится новое сетевое подключение "Континент-АП";
- в меню "Все программы" главного меню Windows появится подменю "Код Безопасности \ Континент-АП 3.7", которое содержит пункты "VPN-клиент", "Код Безопасности CSP", "Контроль целостности", "Брэндмауэр" (если был установлен), "Удаление Континент-АП";
- на панели задач Windows появится пиктограмма абонентского пункта (в случае полной установки дополнительно появятся пиктограмма межсетевого экрана и сообщение об ограничении доступа к сети).

Установка из командной строки

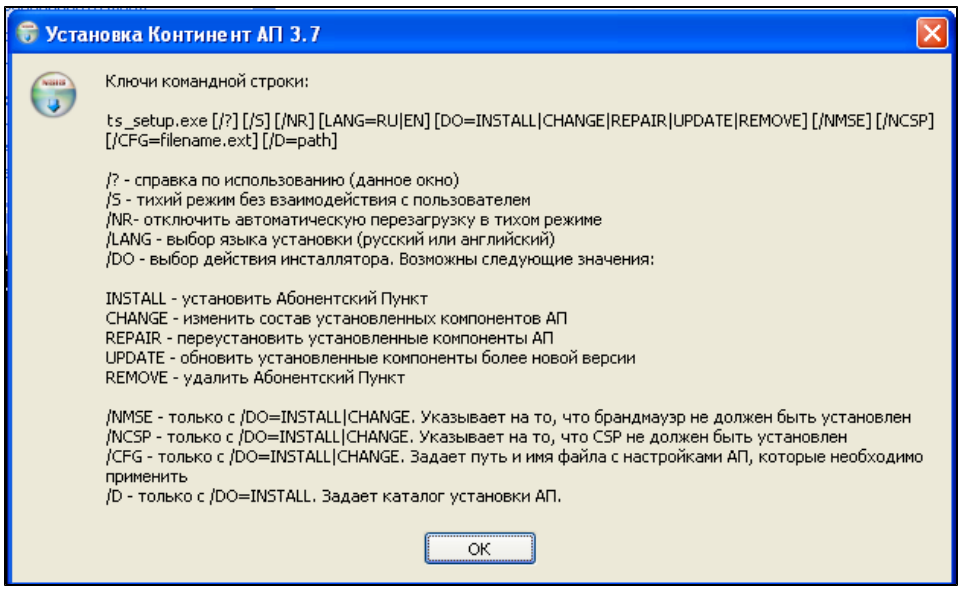
Внимание! Из командной строки можно установить программное обеспечение комплекса, соответствующее только низкому и среднему уровням безопасности.

Для установки программного обеспечения комплекса из командной строки используется команда **ts_setup.exe**. Формат команды и описание ключей представлены в справочной системе.

Для вызова справочного окна:

- Введите в командной строке "ts_setup.exe /?" (без кавычек).

  На экране появится окно справочной системы с описанием формата и ключей команды.



Предусмотрена возможность выполнить установку в фоновом режиме без взаимодействия с пользователем.

Для задания фонового режима установки:

1. В меню "Пуск" вызовите контекстное меню для пункта "Мой компьютер" и выберите команду "Свойства".

   На экране появится стандартный диалог "Свойства системы".
2. Перейдите на вкладку "Оборудование" и в разделе "Драйверы" нажмите кнопку "Подписывание драйверов".

   На экране появится диалог "Параметры подписывания драйвера".
3. Выберите пункт "Пропускать" и нажмите кнопку "ОК".

Для установки программного обеспечения из командной строки:

- Введите в командной строке:

  ts_setup.exe /S /LANG=RU /DO=INSTALL

  и нажмите клавишу <ENTER>.

Начнется установка программного обеспечения комплекса и после ее завершения будет выполнена перезагрузка компьютера.

Результаты установки приведены в разделе выше. При этом значения настраиваемых параметров устанавливаются по умолчанию.

Изменение и восстановление программного обеспечения

Вызов мастера установки

Управление программным обеспечением комплекса выполняют с помощью мастера установки программы.

Для вызова мастера установки программы:

- Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл ts_ setup.exe, находящийся в каталоге с дистрибутивом комплекса, путь к которому указан в документе Release Notes.

  Программа установки начнет выполнение подготовительных действий, и на экране появится сообщение об этом. После завершения подготовительных действий на экране появится диалог "Обслуживание".

Изменение установленного ПО

Изменение программного обеспечения выполняют, если необходимо установить или удалить МСЭ.

Для установки МСЭ:

1. Вызовите на экран мастер установки программы (см. стр.**16**).
2. Выберите действие "Изменить" и нажмите кнопку "Далее >".

   На экране появится диалог "Компоненты устанавливаемой программы".
3. Установите отметку в поле "Брэндмауэр" и нажмите кнопку "Далее >".

   На экране появится диалог с вопросом о вхождении данного компьютера в домен.
4. Выберите нужное значение и нажмите кнопку "Далее >".

   На экране появится диалог "Конфигурация АП" с параметрами межсетевого экрана.
5. Укажите нужные значения параметров и нажмите кнопку "Установить".

Логин администратора	Логин и пароль для перехода МСЭ к режиму настройки (по умолчанию логин "Администратор", пароль "111111")
Пароль администратора	
Пароль пользователя	Пароль для перехода МСЭ к режиму работы пользователя (по умолчанию "111111")

Программа установки приступит к копированию файлов в указанную папку. Полоса прогресса и сообщения, появляющиеся в диалоге, отображают ход процесса установки.

Внимание! В процессе установки на экране будут появляться сообщения о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой. В окне таких сообщений следует нажимать кнопку "Все равно продолжить".

Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику комплекса.

По окончании процесса копирования на экране появится сообщение об успешном завершении установки.

6. Нажмите кнопку "Далее>".

   На экране появится сообщение о завершении работы мастера установки.

7. Нажмите кнопку "Готово" в окне сообщения.

   Окно сообщения закроется.

   Для запуска программы управления МСЭ используйте меню "Пуск".

Для удаления МСЭ:

1. Нажмите кнопку "Пуск" и в главном меню Windows выберите команду "Все программы | Код Безопасности | Континент-АП 3.7 | Удаление Континент-АП".

   На экране появится стартовый диалог программы удаления.

2. Нажмите кнопку "Далее>".

   На экране появится диалог выбора компонентов для удаления.

3. Установите отметку в поле "Брэндмауэр" и нажмите кнопку "Удалить".

   Программа удаления приступит к удалению файлов. По завершении процесса удаления на экране появится заключительное окно мастера удаления с запросом на перезагрузку компьютера.

4. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

Восстановление установленного ПО

Восстановление программного обеспечения выявляет и исправляет поврежденные файлы, ошибки в реестре и т. д.

Примечание. Пользователь, выполняющий восстановление, должен входить в локальную группу администраторов.

Для восстановления ПО:

1. Вызовите на экран мастер установки программы (см. стр.**16**).

2. Выберите действие "Восстановить" и нажмите кнопку "Далее >".

   Мастер приступит к удалению старой версии продукта, и на экране появится запрос на перезагрузку системы.

3. Нажмите кнопку "Да".

   Мастер перезагрузит компьютер и приступит к установке исходной версии продукта.

   Сообщения, появляющиеся на экране, отображают этапы процесса установки.

   Примечание. Если по какой-то причине отсутствует какой-либо из файлов, входящих в комплект поставки, на экране появится предупреждающее сообщение с указанием имени отсутствующего файла. В этом случае проверьте компьютер на наличие вирусов и повторите установку. Если в дальнейшем данная ошибка будет повторяться, обратитесь к поставщику комплекса.

   По окончании процесса исправления на экране появится заключительное окно мастера установки с запросом на перезагрузку компьютера.

   Внимание! Работа установленных компонентов возможна только после перезагрузки компьютера.

4. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

Удаление программного обеспечения

Ниже приведена процедура удаления с использованием стандартной панели управления Windows. Предусмотрен также более быстрый способ запуска процедуры удаления из меню "Пуск": "Все программы | Код Безопасности | Континент-АП 3.7 | Удаление Континент-АП".

Примечание. Пользователь, выполняющий удаление, должен входить в локальную группу администраторов компьютера.

Для удаления программы:

1. Нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления".
2. В окне "Панель управления" активируйте элемент "Установка и удаление программ".
3. Выберите в списке установленных программ элемент "Континент-АП 3.7" и нажмите кнопку "Заменить/Удалить".

   На экране появится диалог для подтверждения удаления ПО из указанной папки.
4. Нажмите кнопку "Далее >".

   На экране появится диалог выбора компонентов программы.
5. Выберите удаляемые компоненты и нажмите кнопку "Удалить".

   Программа удаления приступит к удалению файлов. По завершении процесса удаления на экране появится заключительное окно мастера удаления с запросом на перезагрузку компьютера.
6. Выберите вариант перезагрузки компьютера и нажмите кнопку "Готово".

Обновление версии абонентского пункта

Предусмотрено обновление ПО комплекса с версии 3.7.5.

Файлы обновления поставляются в виде установочного файла ts_setup.exe. Обновление версии абонентского пункта выполняют в следующем порядке:

1. Загрузка файла обновления на компьютер (см. стр.**19**).
2. Установка обновления на компьютер (см. стр.**19**).

Примечания:

- Пользователь, выполняющий обновление, должен входить в локальную группу администраторов компьютера.
- В процессе обновления абонентского пункта МСЭ не устанавливается.
- После обновления абонентского пункта все работающие сетевые подключения будут автоматически разорваны.

Имеется режим автоматической проверки наличия обновлений. В этом режиме при каждом запуске абонентского пункта происходит обращение к адресу, указанному в настройках программы. Если по указанному адресу обнаруживаются файлы дистрибутива новой версии абонентского пункта, на экран выводится окно с уведомлением.

Настройка автоматической проверки обновления

Автоматическая проверка обновления программного обеспечения абонентского пункта предусматривает:

- поиск файлов обновления по адресу, заданному пользователем;
- оповещение пользователя о найденных файлах.

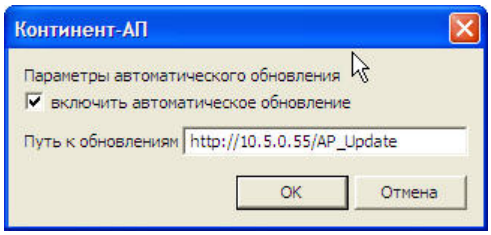
Проверка наличия новой версии программного обеспечения производится при каждом запуске абонентского пункта. По умолчанию режим автоматической проверки выключен.

Особенности настройки MS Explorer. Режим MS Explorer "Автоматическое определение параметров" должен быть отключен (Сервис> Настройки обозревателя> Подключение> Настройка LAN).

Для настройки автоматической проверки обновления:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Активируйте команду "Настройки автоматического обновления".

На экране появится диалог настройки автоматической проверки обновления.



3. Заполните поля диалога:
   - установите отметку в поле "Включить автоматическое обновление";
   - в поле "Путь к обновлениям" введите путь к папке с обновлениями, расположенной на удаленном сервере (допускается использование протоколов HTTP, FTP и SMB).
4. Нажмите кнопку "OK".

   Если при очередном запуске абонентского пункта по указанному адресу будет найдено обновление, то на экране появится сообщение об этом.

Загрузка обновления

Файл установки с обновлением можно получить у администратора комплекса или загрузить самостоятельно.

Для автоматической проверки наличия обновлений нужно включить и настроить одноименный режим (см. стр. **18**). Если по указанному адресу обнаруживаются файлы дистрибутива новой версии абонентского пункта, на экран выводится окно с уведомлением.

Для загрузки обновления на компьютер:

1. Нажмите кнопку "Обновить" в появившемся окне уведомления.

   На экране появится запрос на сохранение файла.
2. Нажмите кнопку "Сохранить".

   На экране появится стандартный диалог Windows для сохранения файла.
3. Укажите папку назначения и нажмите кнопку "Сохранить".

   Файл обновления будет сохранен в указанной папке.

Установка обновления на компьютер

Внимание! Пользователь, выполняющий установку обновления, должен входить в группу локальных администраторов компьютера.

Для установки обновления:

- Запустите на выполнение файл установки обновления, полученный от администратора комплекса или загруженный после автоматической проверки обновлений (см. выше).

  Начнется процедура обновления ПО абонентского пункта.

Настройка параметров абонентского пункта

Вызов меню управления абонентским пунктом

Управление абонентским пунктом выполняется с помощью специального меню.

Для вызова меню управления абонентским пунктом:

- Наведите указатель мыши на пиктограмму абонентского пункта, расположенную на панели задач Windows, и нажмите правую кнопку мыши.

  На экране появится меню управления абонентским пунктом.

  Внимание! Состав меню, отображаемого на экране, зависит от прав пользователя, вошедшего в систему, и от уровня безопасности, выбранного при установке абонентского пункта (см. стр.**40**).

  Цвет пиктограммы абонентского пункта указывает на наличие или отсутствие соединения с сервером доступа:

Пиктограмма	Цвет	Пояснение
	Серый	Соединение не установлено
	Зеленый	Соединение установлено

Табл.1 Команды меню управления абонентским пунктом

Команда	Описание
Подключить "<имя подключения>"	Запускает процедуру установки или разрыва подключения абонентского пункта с сервером доступа, определенного как подключение по умолчанию
Выбор соединения по умолчанию	Определяет выбранное в подменю подключение как подключение по умолчанию. В списке отображаются все доступные подключения, зарегистрированные на компьютере
Выбор криптопровайдера по умолчанию	Определяет выбранный в подменю криптопровайдер как криптопровайдер, используемый по умолчанию. В списке отображаются все доступные криптопровайдеры, установленные на компьютере
Установить/разорвать соединение	Запускает процедуру установки или разрыва выбранного в подменю подключения абонентского пункта с сервером доступа
Создать новое соединение	Запускает процедуру создания нового соединения. Параметры подключения могут быть настроены вручную или с применением конфигурационного файла
Удалить соединение	Запускает процедуру удаления выбранного соединения
Настройка соединения	Устанавливает способ подключения к СД (по HTTP-туннелю, через прокси или по UDP). Предоставляет возможность изменить адрес СД и в случае необходимости указать настройки прокси-сервера
Настройка аутентификации	Вызывает на экран диалог свойств протокола проверки подлинности для выбранного в подменю подключения абонентского пункта
Настройка зависимости между соединениями	Включает/выключает режим автоматического запуска процедуры подключения компьютера к сети провайдера
Журнал	Вызывает на экран стандартное приложение просмотра событий ОС Windows. Зарегистрированные события хранятся в разделе "Terminal Station"

Команда	Описание
Сертификаты > Создать запрос на пользовательский сертификат…	Запускает процедуру создания запроса на получение сертификата пользователя
Сертификаты > Установить сертификат пользователя	Вызывает на экран стандартный диалог Windows для выбора файла сертификата
Загружать автоматически	Включает/выключает режим автоматического запуска программы управления абонентским пунктом при запуске Windows
Поддержка модемного соединения	Включает/выключает режим работы МСЭ с внешними 3G/4G-модемами
Настройка автоматического обновления	Вызывает на экран диалог настройки автоматической проверки обновления программного обеспечения абонентского пункта
Справка	Вызывает на экран окно оперативной справочной системы
О программе…	Вызывает на экран диалог со сведениями о номере версии программы и авторских правах
Выход	Завершает работу программы управления абонентским пунктом

Выбор режима запуска программы управления абонентским пунктом

После установки абонентского пункта и перезагрузки компьютера программа управления абонентским пунктом запустится автоматически, и на панели задач Windows появится пиктограмма абонентского пункта. Пользователь может выбрать дальнейший режим запуска программы управления абонентским пунктом:

- автоматический режим — программа управления абонентским пунктом будет запускаться одновременно с запуском Windows (установлен по умолчанию);
- ручной режим — программа управления абонентским пунктом запускается пользователем вручную.

Для выбора режима запуска:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Выберите режим запуска абонентского пункта:
   - для включения автоматического режима установите отметку слева от параметра "Загружать автоматически";
   - для включения ручного режима удалите отметку слева от параметра "Загружать автоматически".

   Выбранный режим вступит в действие при следующем запуске программы.

Запуск программы управления абонентским пунктом вручную

Для запуска программы управления абонентским пунктом вручную:

- В главном меню Windows активируйте команду "Все Программы\Код Безопасности\Континент-АП 3.7\VPN клиент".

  Программа управления абонентским пунктом будет запущена. На панели задач Windows появится пиктограмма абонентского пункта.

Создание нового соединения

По умолчанию после установки абонентского пункта пользователям доступно соединение с сервером доступа под названием "Континент-АП".

Пользователь с административными правами может создавать новые соединения.

Новое соединение можно создать вручную или с использованием файла конфигурации пользователя, полученного от администратора сервера доступа.

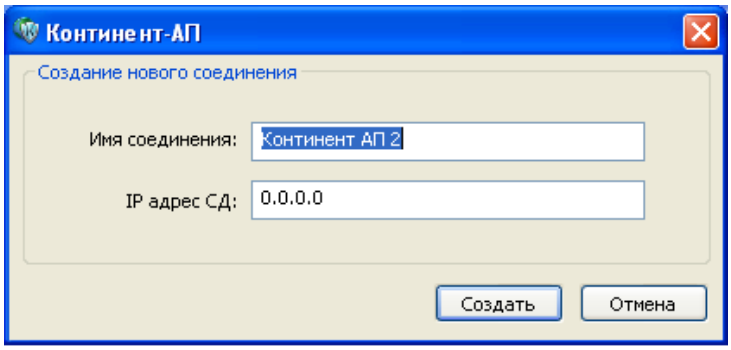
Примечание. Конфигурационный файл создается при регистрации нового пользователя на сервере доступа. При регистрации пользователя также создается ключевой контейнер. Если при формировании ключей используется криптопровайдер "Код Безопасности CSP", ключи пользователя сохраняются в конфигурационном файле; если в качестве криптопровайдера используется "КриптоПро CSP", ключи сохраняются на внешнем носителе.

Внимание! Если абонентский пункт работает в режиме высокого уровня безопасности, создание нового соединения с использованием конфигурационного файла недоступно.

Для создания нового соединения вручную:

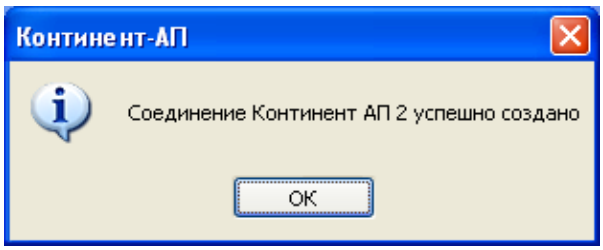
1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Выберите пункт "Создать соединение | Ручная настройка".

   Появится диалог создания нового соединения.



3. Введите имя создаваемого соединения, укажите IP-адрес или доменное имя сервера доступа и нажмите кнопку "Создать".

   На экране появится сообщение об успешном создании нового соединения.



4. Для завершения процедуры нажмите кнопку "ОК" в окне сообщения.

   Созданное соединение можно использовать для подключения к серверу доступа с указанным IP-адресом или доменным именем.

Для создания нового соединения с использованием конфигурационного файла:

1. Получите у администратора сервера доступа конфигурационный файл пользователя, включающий в себя настройки подключения, и файлы сертификатов с ключевым контейнером, а также пароль доступа к файлу конфигурации.
2. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows, и выберите пункт "Создать соединение | Применение настроек из файла конфигурации".

   Появится диалог выбора файла конфигурации.
3. Укажите файл, введите пароль доступа к файлу и нажмите кнопку "Далее".

   На экране появится диалог настройки соединения.
4. При необходимости измените имя соединения и удалите отметку в поле "Установить как соединение по умолчанию".

   Если соединение с таким именем уже существует, на экране появится соответствующее сообщение. Для продолжения измените имя соединения.
5. Если подключение к серверу доступа осуществляется через прокси-сервер, укажите имя пользователя и пароль.
6. Нажмите кнопку "Далее".

   На экране появится запрос на ввод пароля доступа к ключевому контейнеру пользователя.
7. Введите пароль и при необходимости установите отметку в поле "Запомнить пароль".

   Нажмите кнопку "ОК".

   На экране появится диалог смены пароля на доступ к ключевому контейнеру пользователя.
8. Введите и подтвердите новый пароль и нажмите кнопку "ОК".

   На экране появится окно выбора ключевого носителя.
9. Выберите ключевой носитель, на который будет помещен закрытый ключ пользовательского сертификата, и нажмите кнопку "ОК".
   - Если корневой сертификат на компьютер не устанавливался, на экране появится запрос на его установку.

     Нажмите кнопку "Да".

   На экране появится завершающее окно мастера создания нового соединения. В окне приводятся подробные сведения о настройках соединения, выполненных на основе конфигурационного файла.
10. Для завершения процедуры создания соединения нажмите кнопку "Готово".

Выбор режима подключения компьютера к сети провайдера

Чтобы установить соединение с сервером доступа, компьютер должен быть подключен к локальной корпоративной сети или сети провайдера. Подключение компьютера к локальной сети выполняется автоматически при запуске Windows. Автоматический режим подключения к сети провайдера устанавливают средствами абонентского пункта. В этом случае процедура подключения компьютера к сети провайдера запускается автоматически при установлении соединения абонентского пункта с сервером доступа.

Для включения автоматического режима:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Настройка зависимости между соединениями" активируйте команду с названием нужного подключения абонентского пункта (по умолчанию "Континент-АП"), а затем в появившемся списке выберите нужное подключение компьютера.

   Слева от выбранного подключения появится отметка.

Примечание. Для выключения автоматического режима выполните те же действия повторно.

Внимание! Если подключение компьютера к локальной сети или сети провайдера выполняется с помощью модема или каким-либо другим способом (например, средствами удаленного доступа), при создании такого подключения в настройках Windows необходимо включить параметр "Разрешить использовать это подключение другим пользователям".

Режим работы абонентского пункта

Режим работы абонентского пункта определяется на сервере доступа. Администратор сервера доступа может разрешить или запретить пользователю во время работы абонентского пункта незащищенные (без шифрования трафика) соединения с абонентами, не входящими в защищенную сеть.

Особенности режима работы абонентского пункта:

- режим запрета незащищенных соединений — в этом режиме на время сеанса связи абонентского пункта и сервера доступа будут запрещены любые соединения, кроме соединений, указанных в списке разрешенных, и соединения абонентского пункта с сервером доступа;
- режим разрешения незащищенных соединений — в этом режиме во время сеанса связи абонентского пункта и сервера доступа любые другие соединения разрешены.

Настройка соединения

Перед тем как устанавливать соединение с сервером доступа, рекомендуется проверить и при необходимости выполнить настройку параметров сетевого подключения, посредством которого устанавливается соединение.

Примечание. Значения параметров сетевого подключения задаются при установке программного обеспечения абонентского пункта автоматически. При необходимости значения параметров могут быть изменены в соответствии с приведенной ниже процедурой.

Для настройки соединения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. В меню "Настройка соединения" активируйте команду с названием нужного подключения (по умолчанию "Континент-АП").

   На экране появится диалог для настройки выбранного сетевого подключения.
3. Заполните поля диалога и нажмите кнопку "ОК".

Поле	Описание
Адрес СД	Сетевое имя или IP-адрес сервера доступа
Режим защищенного соединения	Способ подключения абонентского пункта к серверу доступа: • стандартное подключение (UDP); • подключение через прокси; • потоковое подключение (TCP). **Внимание!** Если на сервере доступа в настройках параметров подключения АП у параметра "Активные на СД каналы связи" установлено значение "стандартный VPN-канал", подключение через прокси и потоковое подключение будут недоступны
Сервер	Сетевое имя или IP-адрес прокси-сервера (только для "Подключение через прокси")
Порт	Порт прокси-сервера (только для "Подключение через прокси")
Тип	Тип аутентификации: • Без аутентификации • Basic • Kerberos • NTLM • Negotiate Поле доступно, если выбрано подключение через прокси
Пользователь	Имя пользователя для аутентификации на прокси-сервере. Поле доступно, если выбрано подключение через прокси
Пароль	Пароль пользователя для аутентификации на прокси-сервере. Поле доступно, если выбрано подключение через прокси

Настройка аутентификации

Настройку аутентификации выполняют в диалоге свойств протокола проверки подлинности. Имеется возможность выполнения следующих настроек:

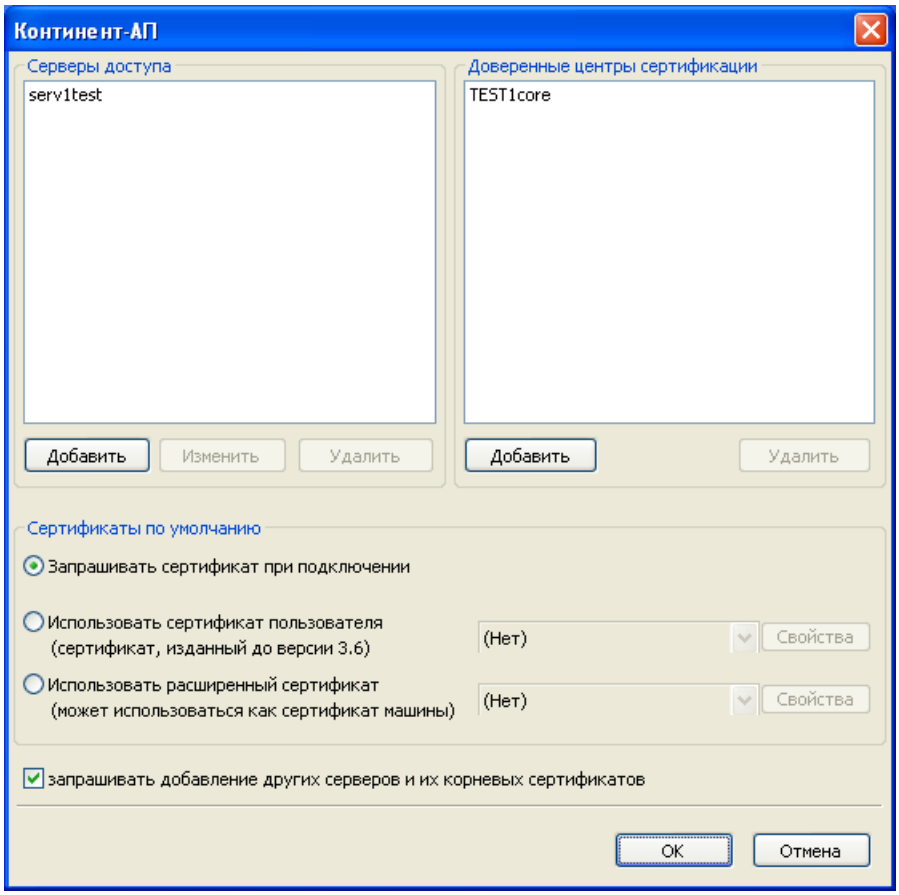
- просмотр и формирование списка разрешенных серверов доступа;
- просмотр и формирование списка сертификатов доверенных центров сертификации;
- выбор режима аутентификации;
- отображение/скрытие запроса на добавление сервера доступа и корневого сертификата в списки разрешенных.

Вызов диалога настроек аутентификации соединения

Для вызова диалога:

- Выберите команду "Настройка аутентификации" контекстного меню пиктограммы абонентского пункта и в ней активируйте сетевое подключение.

  Появится диалог настроек аутентификации соединения.



Формирование списка разрешенных серверов

Добавление имени сервера доступа в список осуществляется автоматически при наличии отметки в поле "Запрашивать добавление других серверов и их корневых сертификатов" при первом подключении абонентского пункта к данному серверу. Кроме того, список разрешенных серверов формируется при импорте настроек из файла конфигурации.

Внимание! Пользователю АП, работающего в режиме высокого уровня безопасности, формирование списка разрешенных серверов запрещено. При первом подключении к серверу доступа пользователь получит сообщение о невозможности соединения с сервером доступа и необходимости обращения к администратору для выполнения настройки аутентификации. В этом случае администратор должен вручную по сведениям от пользователя внести сервер доступа в список разрешенных.

Примечание. После получения от пользователя запроса на настройку аутентификации администратор может выполнить ее следующим образом: запустить ПУ АП от своего имени, выполнить подключение к СД с сертификатом пользователя и после появления диалога настроек аутентификации соединения внести сервер доступа в список разрешенных.

Для ручного формирования списка:

- Используйте кнопки, расположенные под списком. Имя сервера доступа вводят или корректируют с клавиатуры в текстовом поле. Корневой сертификат выбирают в стандартном диалоге Windows.

Выбор режима аутентификации

При подключении абонентского пункта к серверу доступа необходимо предъявить сертификат пользователя. Существуют следующие режимы аутентификации:

- ручной выбор сертификата пользователя при каждом подключении;
- автоматическое использование указанного сертификата пользователя (сертификат по умолчанию);
- автоматическое использование указанного сертификата пользователя (сертификат по умолчанию) в качестве сертификата компьютера.

В последнем случае появляется дополнительная возможность применения доменных политик к компьютеру, на котором установлен комплекс. Этот режим доступен только для сертификатов пользователя, изданных средствами программы управления сервером доступа версии 3.6 и выше.

Для выбора режима аутентификации:

- В группе полей "Сертификаты по умолчанию" диалога свойств протокола проверки подлинности выберите нужное значение:

Значение	Описание
Запрашивать сертификат при подключении	При каждом подключении абонентского пункта к СД на экране отображается диалог выбора сертификата
Использовать сертификат пользователя…	При подключении автоматически используется указанный сертификат пользователя
Использовать расширенный сертификат…	При подключении автоматически используется указанный сертификат пользователя. Этот сертификат используется и как сертификат пользователя, и как сертификат компьютера. Выберите нужный сертификат из раскрывающегося списка. Если сертификат на компьютере не установлен, выберите в списке значение "Импорт" и установите сертификат

Настройка запроса на добавление сервера доступа в список разрешенных

С помощью этой настройки устанавливают порядок первого подключения к серверу доступа: с запросом на добавление сервера доступа в списки разрешенных или без запроса.

Данный запрос содержит имена сервера доступа и его корневого сертификата. Необходимо убедиться в верности этих имен перед занесением в списки. Если отображение запроса отключено, то при отсутствии сервера доступа в списке разрешенных соединение не устанавливается.

Внимание! Настройку запроса для абонентского пункта, работающего в режиме высокого уровня безопасности, должен выполнять администратор.

Для отображения/скрытия запроса:

- Установите/удалите отметку в поле "Запрашивать добавление других серверов и их корневых сертификатов".

Индивидуальные соединения пользователей

Если необходимо, чтобы каждый из нескольких пользователей АП подключался к СД со своим сертификатом без возможности выбора его из списка, администратор должен выполнить следующее:

1. Создать для каждого пользователя новое соединение (см. стр.**22**).
2. Настроить соединение каждого пользователя (см. стр.**24**).
3. Настроить аутентификацию для каждого соединения, указав режим аутентификации – "Использовать сертификат пользователя..." и сертификат (см. стр.**25**).

Удаление соединения

Удаление соединения осуществляется средствами программы управления абонентским пунктом. Пользователям АП, работающего в режиме высокого уровня безопасности, удаление соединения недоступно.

Не рекомендуется удалять средствами ОС Windows соединения, созданные в программе управления абонентским пунктом.

Для удаления соединения:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Выберите пункт "Удалить соединение".

   Появится список соединений.
3. Выберите удаляемое соединение.

   На экране появится запрос на подтверждение удаления.
4. Нажмите кнопку "Да".

   Соединение будет удалено.

Внимание! Если соединение по каким-либо причинам было удалено средствами ОС Windows, оно по-прежнему будет отображаться в меню программы управления абонентским пунктом и будет доступно только для просмотра настроек. При этом подключение к серверу доступа для данного соединения будет невозможно. Для удаления соединения из меню программы управления необходимо выполнить процедуру, описанную выше. Перед началом процедуры можно просмотреть настройку соединения и настройку аутентификации.

Использование сертификата пользователя в качестве сертификата компьютера

Этот режим предоставляет возможность применения доменных политик к компьютеру, на котором установлен комплекс, до входа пользователя в систему (при условии вхождения компьютера в домен).

Режим доступен только для сертификатов пользователя, изданных средствами программы управления сервером доступа версии 3.6 и выше.

Внимание! Подключение абонентского пункта к серверу доступа возможно только с предъявлением ключевого контейнера с закрытым ключом пользователя при сохраненном пароле доступа к ключевому контейнеру и сохраненном PIN-коде (для ключевых носителей, защищенных PIN-кодом).

Для настройки режима:

1. Перейдите к диалогу свойств протокола проверки подлинности (см. стр.**26**).
2. Выберите значение "Использовать расширенный сертификат" и укажите нужный сертификат (см. стр.**27**).

   Внимание! Должно выполняться следующее условие: указанный сертификат должен был быть зарегистрирован тем же пользователем, от имени которого осуществляется переключение в режим использования

расширенного сертификата. В противном случае после выполнения данной процедуры подключение к серверу доступа станет невозможным и будет сопровождаться ошибкой подписи ключа. Об исправлении некорректного переключения в режим использования расширенного сертификата см. стр.**30**.

Примечание. Если в списке отсутствует необходимый сертификат, зарегистрируйте его (см. Регистрация сертификатов, [**2**]) с сохранением пароля доступа к ключевому контейнеру и PIN-кода (если используется).

3. Выполните контрольное подключение к серверу доступа (см. Установление соединения с сервером доступа, [**2**]). В запросах на ввод защитного PIN-кода и пароля доступа к ключевому контейнеру сохраните PIN-код и пароль.
4. Отключите абонентский пункт от сервера доступа и перезагрузите компьютер.

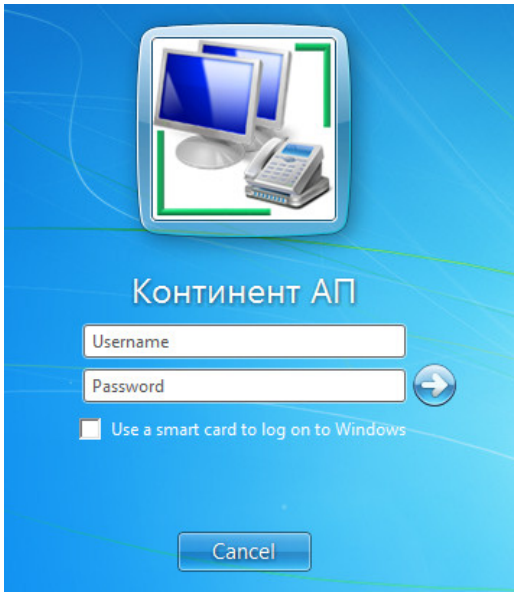
   Компьютер готов к работе в режиме использования сертификата пользователя в качестве сертификата компьютера.

Процедура подключения к серверу доступа зависит от ОС, установленной на компьютере. Ниже приведен пример процедуры подключения для Windows 7 (Windows Server 2008 R2).

Для Windows 7:

1. В окне "Вход в Windows" нажмите кнопку сетевого подключения  .

   Появится приглашение на ввод имени и пароля доменного пользователя для соединения с сервером доступа.



2. Введите доменное имя и пароль пользователя и нажмите кнопку "Войти".

   Начнется подключение абонентского пункта к серверу доступа и после успешного соединения будет выполнена идентификация и аутентификация пользователя на контроллере домена.

   После успешной идентификации и аутентификации будет выполнен вход пользователя в систему с применением к компьютеру доменных политик.

Некорректное переключение в режим использования расширенного сертификата

Для исправления некорректного переключения в режим использования расширенного сертификата необходимо выполнить следующее:

1. В диалоге свойств протокола проверки подлинности установить значение "Запрашивать сертификат при подключении" (см. стр.**26**).
2. Средствами ОС Windows из хранилищ всех пользователей и из хранилища компьютера удалить все экземпляры сертификата, который был указан при переключении в режим "Использовать расширенный сертификат" (см. стр.**28**).
3. Повторно зарегистрировать удаленный из хранилищ сертификат (см. [**2**]).
4. Выполнить процедуру настройки режима использования расширенного сертификата (см.стр.**28**).

Настройка времени ожидания ответа от сервера доступа

Пользователь может указать время, по истечении которого будет разорвано соединение абонентского пункта с сервером доступа в том случае, если сервер неактивен.

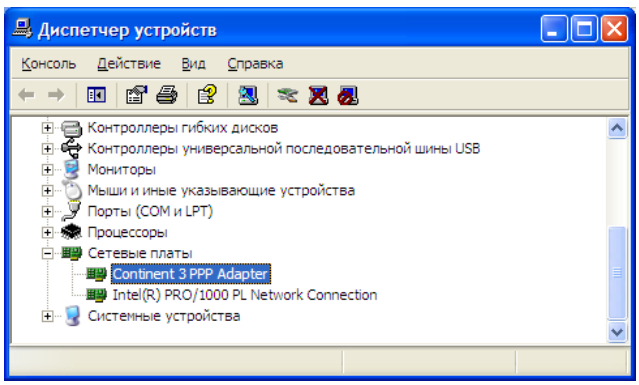
Примечание. Данная функция настраивается для эмулятора модема Continent 3 PPP Device, посредством которого устанавливается соединение с сервером доступа. По умолчанию это время составляет 1 минуту.

Этот параметр будет действовать для всех соединений, которые можно устанавливать из меню управления абонентским пунктом, т. е. соединений, указанных в пункте "Установить/разорвать соединение" в контекстном меню пиктограммы абонентского пункта.

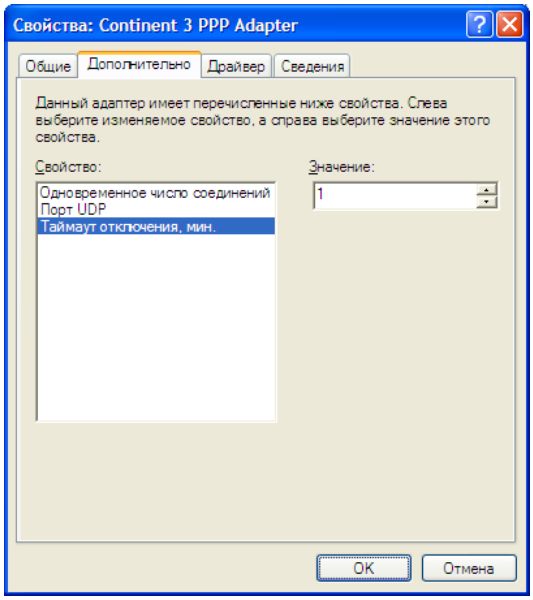
Для изменения времени ожидания ответа от сервера доступа:

1. Вызовите на экран стандартное окно Windows "Диспетчер устройств".

Совет. Для этого нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления". В окне "Панель управления" активируйте элемент "Система". В появившемся диалоге перейдите к вкладке "Оборудование" и нажмите кнопку "Диспетчер устройств".



2. Перейдите к группе устройств "Сетевые платы" и активируйте команду "Свойства" в контекстном меню эмулятора модема Continent 3 PPP Device.
3. В появившемся диалоге "Свойства: Continent 3 PPP Device" перейдите к вкладке "Дополнительно":



4. В списке "Свойство" выберите значение "Тайм-аут отключения, мин." и в поле "Значение" укажите время ожидания ответа от сервера доступа в минутах.
5. Нажмите кнопку "OK" для подтверждения изменений.

Выход из программы управления

При завершении работы программы управления абонентский пункт продолжает свою работу.

Для выхода из программы:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.
2. Активируйте команду "Выход".

   Работа программы управления абонентским пунктом будет завершена. Пиктограмма этой программы исчезнет с панели Windows.

Резервное копирование сертификатов

Резервное копирование сертификата пользователя и сертификата корневого центра сертификации выполняется обычными средствами копирования файлов. При необходимости вы сможете использовать копию корневого сертификата на другом компьютере или на том же компьютере после переустановки операционной системы и программного обеспечения. Для того чтобы использовать подобным образом копию сертификата пользователя, необходимо иметь в наличии ключевой носитель, содержащий ключевую информацию, соответствующую данному сертификату.

Внимание! Физический носитель информации, на котором будут храниться резервные копии файлов сертификатов, должен отличаться от физического носителя, на котором находятся рабочие экземпляры файлов. Иначе при отказе этого носителя будут потеряны и рабочие файлы, и их резервные копии.

Запуск МСЭ

МСЭ начинает свою работу автоматически, сразу же после перезагрузки компьютера, а в дальнейшем — при каждом входе в систему.

После запуска МСЭ в системной области панели задач Windows появится пиктограмма программы управления МСЭ. Цвет пиктограммы указывает на режим работы МСЭ:

	Зеленый	Режим работы пользователя
	Желтый	Режим ожидания или ошибка в работе

Внимание! После установки программного обеспечения и перезагрузки компьютера для МСЭ устанавливается режим ожидания (пиктограмма желтого цвета). При этом действуют ограничения на доступ к сети. Для снятия ограничений необходимо включить режим работы пользователя (см. далее).

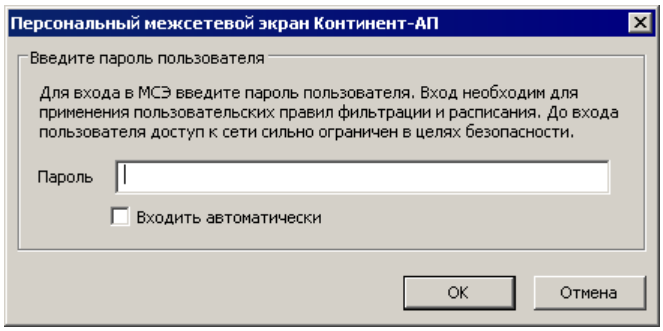
Включение режима работы пользователя

Для включения режима работы пользователя необходимо ввести пароль пользователя. По умолчанию пароль пользователя МСЭ имеет значение "111111", если не был изменен во время установки абонентского пункта.

Для включения режима работы:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Начать сеанс работы…".

   На экране появится диалог для ввода пароля.



2. Введите пароль и нажмите кнопку "OK".

Примечание. Для автоматического включения режима работы пользователя сразу после загрузки операционной системы установите отметку в поле "Входить автоматически".

Администрирование МСЭ

Внимание! Для администрирования программа управления МСЭ должна быть запущена от имени пользователя, наделенного правами локального администратора компьютера.

Ручной запуск программы управления МСЭ

Программа управления МСЭ запускается автоматически одновременно с запуском МСЭ. Ручной запуск предусмотрен для возобновления работы программы управления после ее ручного отключения.

Для запуска программы управления МСЭ:

- Выполните одно из следующих действий:
  - активируйте в меню Windows команду "Пуск > Программы > Код Безопасности > Континент-АП 3.7>Брэндмауэр";
  - запустите на исполнение файл mseGui.exe из каталога установки программного обеспечения МСЭ. Каталог установки по умолчанию: "C:\Program Files\Security Code\Continent Client".

Примечание. Для запуска программы управления от имени другого пользователя в контекстном меню команды "Программа управления" или файла mseGui.exe активируйте команду "Запуск от имени…".

Команды программы управления МСЭ

Контекстное меню пиктограммы МСЭ содержит следующие команды для управления пакетным фильтром:

Пункт меню	Описание
Начать сеанс работы…	Вызывает на экран окно для ввода пароля пользователя. После авторизации включается режим работы пользователя
Завершить сеанс работы	Выключает режим работы пользователя, и включает режим ожидания
Изменить пароль…	Вызывает на экран окно для изменения пароля пользователя
Входить автоматически	При наличии отметки режим работы пользователя включается автоматически сразу после загрузки операционной системы без запроса пароля
Войти в режим настройки…	Вызывает на экран окно для ввода пароля администратора. После ввода пароля становятся доступными команды управления правилами фильтрации
Выйти из режима настройки	Завершает сеанс работы администратора. Команды управления правилами фильтрации становятся недоступными
Изменить данные администратора…	Вызывает на экран окно для изменения логина и пароля администратора
Изменить расписание…	Открывает окно для формирования расписаний работы правил фильтрации
Изменить правила фильтрации…	Открывает окно для формирования списка правил сетевой фильтрации, действующих в режиме работы пользователя
Изменить правила прикладной фильтрации…	Открывает окно для формирования списка правил прикладной фильтрации. Эти правила действуют в режиме работы пользователя
Изменить правила фильтрации до авторизации…	Открывает окно для формирования списка правил фильтрации, действующих в режиме ожидания
Включить оповещение	При наличии отметки на экран выводятся сообщения о срабатывании правил фильтрации с флагом alert

Пункт меню	Описание
Журналы	Вызывает на экран выбранный в подменю регистрационный журнал
Журнал событий	Вызывает на экран стандартное приложение просмотра событий ОС Windows. Зарегистрированные события хранятся в разделе "Terminal Station"
Справка	Вызывает на экран окно справочной системы МСЭ
О программе…	Вызывает на экран окно с информацией об установленной на компьютере версии программного обеспечения МСЭ
Выход	Закрывает программу управления МСЭ. При этом сам МСЭ будет продолжать работать

Так как настройку параметров МСЭ может выполнить лишь пользователь, наделенный правами администратора, часть команд контекстного меню доступна для активации только после ввода пароля администратора (см. ниже).

Включение режима настройки

Для администрирования МСЭ необходимо ввести логин и пароль, подтверждающие полномочия пользователя на выполнение операций. По умолчанию логин администратора МСЭ имеет значение "администратор", пароль "111111", если эти значения не изменялись во время установки абонентского пункта.

Для включения режима настройки:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Войти в режим настройки…".

   На экране появится диалог для ввода логина и пароля.
2. Введите логин и пароль и нажмите кнопку "ОК".

Изменение аутентификационных параметров администратора

По умолчанию логин администратора МСЭ имеет значение "администратор", пароль "111111".

Для изменения пароля администратора:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Изменить данные администратора".

   На экране появится диалог для ввода логина и пароля.
2. Внесите нужные изменения и нажмите кнопку "ОК". При изменении пароля необходимо ввести новое значение и подтвердить его.

Выключение режима настройки

Для выключения режима настройки:

- Активируйте в контекстном меню пиктограммы МСЭ команду "Выйти из режима настройки".

  Сеанс работы администратора будет завершен и часть команд контекстного меню пиктограммы МСЭ станет недоступной для активации.

Завершение работы программы управления МСЭ

После завершения работы программы управления все сервисы МСЭ будут работать в штатном режиме, за исключением сервиса оповещения.

Внимание! После завершения работы программы управления оповещения о срабатывании правил фильтрации на экран не выводятся.

Для завершения работы программы управления МСЭ:

- Активируйте в контекстном меню пиктограммы МСЭ команду "Выход".

  Пиктограмма МСЭ будет удалена из системной области панели задач Windows.

Проверка контрольных сумм

Проверка контрольных сумм выполняется в следующих случаях:

- автоматически при запуске операционной системы;
- автоматически при попытке соединения с сервером доступа;
- вручную по команде оператора.

Для проверки контрольных сумм вручную:

- Активируйте в меню Windows команду "Пуск > Программы > Код Безопасности > Континент-АП 3.7 > Контроль целостности".

По окончании выполнения процедуры проверки на экране появится информационное окно, в котором будет представлен отчет о результатах проверки.

В отчете содержится информация о количестве проверенных файлов и сведения о каждом из них:

- наименование и полный путь к файлу;
- результат проверки:

Успешно	Результат проверки положительный
Ошибка! Файл не найден	Файл не найден
Ошибка! Значение хеш-функции не совпадает	Содержимое файла изменено

Управление параметрами фильтрации

Управление списками правил фильтрации

Для управления списком:

1. Активируйте в контекстном меню пиктограммы МСЭ нужную команду:

Изменить правила фильтрации до авторизации	Для редактирования списка правил фильтрации, действующих до авторизации
Изменить правила фильтрации	Для редактирования списка правил фильтрации, действующих после авторизации
Изменить правила прикладной фильтрации	Для редактирования списка правил прикладной фильтрации

   На экране появится указанный список правил.

2. Отредактируйте список правил, удалив ненужные правила или создав новые. Описание языка правил фильтрации представлено в приложении (см. стр.**41**).

   Примечание. Редактирование правила сопровождается автоматической проверкой его синтаксиса. При обнаружении ошибки на экране появится сообщение с указанием номера позиции, в которой была допущена ошибка, а в редактируемом списке правил фильтрации весь текст, начиная с указанной позиции, будет выделен подчеркиванием красного цвета.

3. При необходимости используйте кнопки:

Импорт...	Вызывает на экран типовой диалог для открытия файлов. Выберите файл с созданными ранее правилами. Содержимое файла отобразится в диалоге для редактирования правил фильтрации
По умолчанию	Возвращает список к состоянию после установки ПО. В окне "Правила фильтрации до авторизации" в открывшемся списке выберите нужное значение: • локальные правила фильтрации — для компьютера не в домене; • доменные правила фильтрации — для компьютера в домене

4. Для применения новых правил нажмите кнопку "ОК".

Настройка расписания

Для настройки расписания:

1. Активируйте в контекстном меню пиктограммы МСЭ команду "Изменить расписание".

   На экране появится диалоговое окно с расписанием.

   Примечание. Изначально после установки абонентского пункта расписание отсутствует.

2. Сформируйте или отредактируйте расписание, удалив ненужные строки или добавив новые. Структура файла с расписаниями представлена в Приложении (см. стр.**52**).

   Внимание! Заданные в расписании интервалы действия правил фильтрации могут сдвигаться в сторону задержки на одну (или меньше) минуту.

3. При необходимости используйте кнопки:

Импорт...	Вызывает на экран типовой диалог для открытия файлов. Выберите файл с созданными ранее правилами. Содержимое файла отобразится в диалоге для редактирования правил фильтрации
По умолчанию	Возвращает список к состоянию после установки ПО

4. Для применения расписания нажмите кнопку "ОК".

Настройка оповещений о срабатывании правил фильтрации

Средства МСЭ позволяют оповещать пользователя о срабатывании правил фильтрации. Оповещение представляет собой всплывающее сообщение, появляющееся над пиктограммой МСЭ в панели задач Windows.

Для настройки оповещений необходимо:

- в списке правил фильтрации установить флаг alert для тех правил фильтрации, о срабатывании которых требуется оповещать пользователя (см.стр.**41**);
- включить режим оповещения.

Для включения режима оповещения:

- Отметьте в контекстном меню пиктограммы МСЭ команду "Включить оповещение".

Примечание. Для отмены оповещений удалите отметку.

Регистрация событий

В зависимости от уровня безопасности установленного программного обеспечения комплекса события, относящиеся к соединениям абонентского пункта с сервером доступа, сохраняются в журнале Secret Net (для высокого уровня безопасности) или в собственном журнале "Terminal Station" (для низкого и среднего уровня безопасности).

Перечень регистрируемых событий, относящихся к соединениям абонентского пункта, приведен в Приложении (см. стр.**52**).

Сведения о событиях сохраняются в виде записей, содержащих подробную информацию о событии.

Для просмотра событий в журнале Secret Net:

- активируйте команду "Пуск | Все программы | Secret Net 7 | Журналы".

Примечание. О работе с журналом смотрите соответствующий раздел документации ПО Secret Net.

Для просмотра событий в журнале Terminal Station:

1. Откройте системный журнал Windows и выберите папку "Terminal Station".

   Примечание. Открыть журнал Terminal Station можно в ПУ АП, выбрав соответствующий пункт меню.

   Справа отобразится список зарегистрированных событий.
2. Выберите нужную запись.
3. В контекстном меню выбранной записи активируйте команду "Свойства".

   На экране появится окно, в котором содержится информация о событии.

Приложение

Пример конфигурационного файла

Ниже приведен пример файла конфигурационных настроек, используемого при установке ПО абонентского пункта.

```
[config]
version=3.7
vpn=1
firewall=1
upd_state=0
upd_path=
[vpn]
defcsp=90
kclevel=1
conns_num=1
[connection#0]
name=Континент АП
ip=172.17.7.101
addunksrv=1
depend=
idmode=0
lastid=W7_Aviales_06062015_1959.cer
calist=172.17.6.191_25032015_2059.cer,root_172.17.7.101_
06062015_1959.cer,root_172.17.7.101_31052015_1959.cer
sdlist=srv172.17.6.191,srv_172.17.7.101
userproxy=0
proxyaddress=0.0.0.0
proxyport=0
proxyauthtype=None
proxyuser=
proxypassword=
default=1
[firewall]
notify=0
log_user=log_user.txt
log_appl=log_appl.txt
adm_
login=hex:7849f6369eeae40cb31b9cadcaea7fb01bfa093305e02d32360-
b16d67aa46826
adm_
pass=hex:071a2f3162a5913613ac885c56e5883cf2506a292aed015ef16f-
a94bc84b135b
user_
pass=hex:071a2f3162a5913613ac885c56e5883cf2506a292aed015ef16f-
a94bc84b135b
rules_base=pass:udp port 67;pass:udp port 68;
rules_user=pass :tcp port 80;pass :tcp port 3389;pass :udp
port 445;sched=2 log :icmp;log :tcp dst host
192.168.170.100:; pass:;
rules_appl=pass::;
rules_sched=1 daily 11:30-12:45;2 daily 9:00-17:00;3 daily
8:45-18:00;
```

Разделение прав пользователей и администраторов АП

Ниже приведены функции и пункты меню управления АП, доступные пользователям в зависимости от их роли в комплексе, соответствующем высокому уровню безопасности.

Функция АП	Пользователь	Администратор
Создание, удаление, изменение соединения с СД	Нет	Да
Создание личного запроса на сертификат и ключевого контейнера	Да	Да
Установка личного пользовательского сертификата в локальное хранилище и связывание с ключевым контейнером	Да	Да
Установка корневого сертификата (цепочки корневых сертификатов) в локальное хранилище доверенных сертификатов	Да	Да
Выбор личного сертификата пользователя для установления соединения с СД	Да	Да
Выбор расширенного сертификата для установления соединения с СД	Нет	Да
Установление соединения АП с СД с личным сертифи-катом или расширенным сертификатом, используемым как сертификат локального компьютера (последнее настраивается администратором)	Да	Да
Регистрация сертификата СД и его корневого в локальной системе (диалог "Настройка аутентификации")	Нет	Да
Установка зависимостей подключений	Нет	Да
Закрытие приложения	Да	Да
Установка, удаление, изменение приложения	Нет	Да
Обновление приложения	Нет	Да
Просмотр журналов	Нет	Да
Архивирование журналов (выполняется средствами Secret Net)	Нет	Да
Восстановление модифицированных ресурсов по эталонам (выполняется средствами Secret Net)	Нет	Да
Проведение и просмотр отчета КЦ	Нет	Да
Настройка работы АП	Нет	Да

Пункт меню АП	Пользователь	Администратор
Подключить <Название соединения>	Да	Да
Выбор соединения по умолчанию	Да	Да
Выбор криптопровайдера по умолчанию	Да	Да
Установить/Разорвать соединение	Да	Да
Создать новое соединение	Нет	Да
Удалить соединение	Нет	Да
Настройка соединения	Нет	Да
Настройка аутентификации	Нет	Да
Настройка зависимости между соединениями	Нет	Да

Пункт меню АП	Пользователь	Администратор
Журнал	Нет	Да
Сертификаты/Создать запрос на пользовательский сертификат	Да	Да
Сертификаты/Установить сертификат пользователя	Да	Да
Загружать автоматически	Нет	Да
Поддержка модемного соединения	Да	Да
Настройка автоматического обновления	Нет	Да
Справка	Да	Да
О программе	Да	Да
Выход	Да	Да

Язык правил фильтрации

Синтаксис правил фильтрации

Правила фильтрации IP-пакетов имеют следующую структуру:

[pass] [in] [out] [log] [iface=<наименование соединения>]:[<текст правила>];

где:

- перед символом ":" указывают флаги, описывающие применение правила (см.стр.**42**);

  Примечание. Если указаны два флага — in и out или не указан ни один из них, правило применяется как к входящим, так и к исходящим IP-пакетам.

- между символами ":" и ";" содержится собственно текст правила (см. стр.**42**).

Флаги, символы ":" и ";" могут разделяться любым количеством символов табуляции, пробелов и переносов строки.

Синтаксис правил прикладной фильтрации

Правила прикладной фильтрации имеют формат:

[pass] [in] [out] [log]:[<текст правила>]:[<регулярное выражение>];

где:

- в заголовке допустимы следующие флаги: **pass**, **in**, **out**, **log** (см. стр.**42**);
- в тексте правила допустимы следующие примитивы: **tcp**, **udp**, **src port <port>, dst port <port>, src host <host>, dst host <host>, outbuf <size>, inbuf <size>** (см. стр.**43**);

  Примечание. Если указано не пустое регулярное выражение, в правиле должен быть указан параметр outbuf, inbuf или оба.

- регулярное выражение, если оно указано, должно соответствовать правилам синтаксиса regex (источник FreeBSD Man Pages). Дополнительно в регулярном выражении можно указывать числовые коды в шестнадцатеричном формате в виде "\xFF". Перечень метасимволов, используемых в регулярных выражениях, см. стр.**47**.

  Примечание. Для правил, принадлежащих одному диапазону IP-адресов, допустимо только одно регулярное выражение.

Флаги и параметры должны быть разделены пробелами, каждое правило должно заканчиваться символом ";" (точка с запятой).

Пример правила прикладной фильтрации: pass:tcp dst port 80 dst host 192.168.1.40 outbuf 100:google.com\x00;

Флаги правил фильтрации

Флаг	Описание
pass	Пакет, удовлетворяющий данному правилу, пропускается. Если данный флаг не указан — IP-пакет отбрасывается
in	Правило применяется только к входящим IP-пакетам
out	Правило применяется только к исходящим IP-пакетам
log	IP-пакет, удовлетворяющий данному правилу, записывается в файл IP_log.txt из каталога установки
log	В журнале регистрации событий через каждые 5 минут фиксируется сообщение, указывающее — сколько раз за последние 5 минут сработало данное правило
ifname	Правило применяется только к IP-пакетам, проходящим через указанное соединение. Наименование соединения должно быть идентичным наименованию, под которым оно указано в меню "Пуск > Настройка > Сетевые подключения". Если наименование соединения содержит пробелы, оно должно указываться в кавычках (например: "Local Area Connection 2")
alert	Уведомление пользователя об обработке IP-пакета правилом с таким флагом **Примечания:** • В правила фильтрации, в которых используется флаг alert, автоматически добавляется флаг log. • При постоянном применении флага alert ко всем IP-пакетам происходит быстрое заполнение журнала событий. В связи с этим рекомендуется выборочное применение данного флага к правилам фильтрации.
alert	Если включен режим оповещения о срабатывании правил (см. стр.**37**), в журнале регистрации событий через каждые 5 минут фиксируется сообщение, указывающее — сколько раз за последние 5 минут сработало данное правило, а над пиктограммой МСЭ в панели задач Windows появляется всплывающее сообщение с таким же содержанием. Если режим оповещения выключен, сообщение фиксируется только в журнале, всплывающие сообщения отсутствуют
sched	Правило действует по расписанию. После знака равно указывается идентификатор расписания. Например, sched = 1 означает, что правило будет работать только в период времени, указанный в расписании с идентификатором 1

Текст правил фильтрации

Каждое выражение, задающее фильтр, включает один или несколько примитивов, состоящих обычно из одного или нескольких идентификаторов объекта и предшествующих ему классификаторов. Идентификатором объекта может служить его имя или номер. Классификаторы объектов могут относиться к одному из трех видов:

type
указывает тип объекта, заданного идентификатором. В качестве типа объектов могут указываться значения host (хост), net (сеть) и port (порт). Если тип объекта не указан, предполагается значение host;

dir
задает направление по отношению к объекту. Для этого классификатора поддерживаются значения src (объект является отправителем), dst (объект является получателем), src or dst (отправитель или получатель) и src and dst (отправитель и получатель). Например, src foo указывает на пакеты, отправленные с хоста foo, dst net 128.3 — пакеты, адресованные в сеть

128.3.0.0/16, a src or dst port ftp-data — пакеты данных протокола FTP (порт ftp-data), передаваемые в обоих направлениях. Если классификатор dir не задан, предполагается значение src or dst. Для некоторых типов соединений (например, SLIP) и режимов захвата (например, захват с фиктивного интерфейса any в Linux-системах) могут использоваться классификаторы inbound и outbound;

proto
задает протокол, к которому должны относиться пакеты. Этот классификатор может принимать значения ether, tr, wlan, ip, arp, rarp, decnet, tcp и udp. Если примитив не содержит классификатора протокола, предполагается, что данному фильтру удовлетворяют все протоколы, совместимые с типом объекта.

Кроме объектов и классификаторов примитивы могут содержать ключевые слова gateway (шлюз), broadcast (широковещательный), less (меньше), greater (больше) и арифметические выражения.

Сложные фильтры могут содержать множество примитивов, связанных между собой с использованием логических операторов and, or и not (например, host foo and not port ftp and not port ftp-data). Для сокращения задающих фильтры выражений можно опускать идентичные списки классификаторов. Например, выражение tcp dst port ftp or ftp-data or domain будет краткой формой выражения

tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain

Примитивы фильтров

Примитив	Описание
dst host <хост>	Будет отбирать пакеты, в которых поле адреса получателя IPv4 содержит адрес хоста, заданного в примитиве
src host <хост>	Будет выбирать все пакеты, в которых поле отправителя содержит адрес указанного хоста
host <хост>	Будет отбирать все пакеты, для которых адрес хоста указан в поле получателя или отправителя. Все три приведенных выше выражения могут содержать идентификаторы протоколов ip, arp или rarp, как в выражении ip host <хост>, эквивалентном фильтру: ether proto ip and host <хост>. Если именем задан хост, с которым связано несколько адресов IP, фильтру будут соответствовать пакеты с любым из этих адресов в заголовках пакетов
ether src<ehost>	Будет выбирать все кадры, в которых поле MAC-адреса отправителя содержит значение ehost
ether host<ehost>	Будет отбирать все пакеты с адресом, указанным значением ehost в поле отправителя или получателя
gateway <шлюз>	Будет отбирать все пакеты, использующие указанный именем хост в качестве шлюза. Указанное параметром имя хоста должно преобразовываться в IP-адрес механизмами преобразования имен, доступными локальному компьютеру (файл /etc/hosts, DNS, NIS и т. п.), а также механизмами определения MAC-адреса по имени хоста (/etc/ethers и т. п.). Эквивалентное выражение ether host ehost and not host <хост> позволяет указывать хост по имени или адресу, указанному в файле host/ehost
dst net <сеть>	Отбирает все пакеты IPv4, направленные в указанную сеть. Для указания сети можно использовать имя из файла /etc/networks или номер сети
src net <сеть>	Выбирает все пакеты IPv4, отправленные из указанной сети
net <сеть>	Выбирает все пакеты IPv4, содержащие адреса из указанной сети в поле отправителя или получателя

Примитив	Описание
net <сеть> mask <маска сети>	Будет отбирать все пакеты IP, содержащие в поле отправителя или получателя адреса из сети, указанной с использованием маски
net <сеть/размер маски>	Будет отбирать все пакеты IPv4, содержащие в поле отправителя или получателя адреса из сети, указанной с использованием маски
dst port <порт>	Отберет все пакеты ip/tcp и ip/udp, направленные в указанный порт. Номера портов могут задаваться номерами или именами из файла /etc/services. При указании имени (протокол/порт) проверяется как порт, так и протокол. Если примитив содержит номер или неоднозначное обозначение порта (только порт, без протокола), фильтру будут соответствовать пакеты обоих протоколов (tcp и udp). Например, фильтру dst port 513 будут соответствовать пакеты tcp/login и udp/who, а фильтру port domain – трафик tcp/domain и udp/domain
src port <порт>	Отбирает все пакеты, отправленные из указанного порта
port <порт>	Отбирает все пакеты, содержащие указанный номер порта в поле отправителя или получателя. Любое из трех перечисленных правил для портов может включать в качестве префикса идентификатор протокола tcp или udp (например, tcp src port <порт> будет отбирать пакеты tcp, отправленные из указанного порта)
less <размер>	Будет собирать пакеты, размер которых не превышает указанного значения
greater <размер>	Будет собирать пакеты, размер которых не меньше указанного значения
ip proto <протокол>	Отбирает все пакеты IP, содержащие заданный идентификатор типа в поле типа протокола. Типы протоколов IP можно указывать по именам или (icmp, icmp6, igmp, igrp, pim, ah, esp, vrrp, udp, tcp) или номерам. Поскольку tcp, udp и icmp используются также в качестве ключевых слов, перед этими идентификаторами следует помешать символ (слеш). Отметим, что этот примитив не проверяет цепочки протокольных заголовков
ip protochain <протокол>	Отберет все пакеты IPv4, содержащие в цепочке протокольных заголовков идентификатор указанного типа протокола. Например, фильтру ip protochain 4 будут соответствовать все пакеты IPv4 с заголовками TCP в цепочке заголовков. Такой пакет может содержать, например, заголовок аутентификации (AH), маршрутный заголовок (routing header) или заголовок опции hop-by-hop между заголовками IPv4 и TCP. Отметим, что порождаемый этим примитивом код BPF достаточно сложен и не может быть оптимизирован средствами tcpdump, поэтому использование данного фильтра может замедлять работу программы
ether broadcast	Обеспечивает отбор всех широковещательных кадров Ethernet. Ключевое слово ether может быть опущено
ip broadcast	Отбирает все широковещательные пакеты IPv4. Этому правилу будут соответствовать широковещательные адреса, содержащие только нули (all-zeroes) и только единицы (all-ones) с учетом маски подсети для интерфейса, который используется для захвата пакетов. Если маска подсети для интерфейса недоступна, фильтр может работать некорректно
ether multicast	Собирает все кадры с групповыми адресами Ethernet. Ключевое слово ether использовать необязательно. Логически это правило эквивалентно выражению ether[0] & 1 != 0
ip multicast	Отбирает пакеты с групповыми адресами IP

Примитив	Описание
ether proto <протокол>	Отбирает кадры Ethernet с заданным типом протокола. Протокол может быть указан по номеру или имени (ip, arp, rarp, atalk, aarp, decnet, sca, lat, mopdl, moprc, iso, stp, ipx, netbeui). При использовании правила для протоколов Token Ring (например, tr protocol arp) и IEEE 802.11 (например, wlan protocol arp) в большинстве случаев идентификация протокола производится на основании заголовка 802.2 Logical Link Control (LLC), который обычно помещается после заголовка Token Ring или 802.11. При фильтрации для большинства протоколов Token Ring и 802.11 программа-фильтр проверяет только поле идентификатора протокола (protocol ID) в заголовке LLC так называемого SNAP-формата с идентификатором OUI = 0x000000 (Organizational Unit Identifier), указывающим на инкапсуляцию Ethernet. Проверка для пакетов использования формата SNAP с OUI = 0x000000 не выполняется, за исключением перечисленных ниже случаев: **iso** Фильтр проверяет поля DSAP11 и SSAP12 в заголовках LLC; **stp** **netbeui** Фильтр проверяет поле DSAP в заголовке LLC; **atalk** Фильтр проверяет использование в кадре формата SNAP с OUI = 0x080007 и тип (etype) AppleTalk. Для случая Ethernet проверяются поля типа Ethernet для большинства протоколов. Исключениями являются протоколы: **iso** **sap** **netbeui** Фильтр проверяет для кадра принадлежность к 802.3 и заголовок LLC (как это описано выше для Token Ring и 802.11); **atalk** Проверяется тип AppleTalk в кадре Ethernet и формат заголовка SNAP (как для Token Ring и 802.11); **aarp** Проверяется тип AppleTalk ARP в кадре Ethernet или использование формата 802.2 SNAP с OUI = 0x000000; **ipx** Фильтр проверяет тип IPX в кадре Ethernet, поле IPX DSAP в заголовке LLC, инкапсуляцию IPX и тип IPX в кадре SNAP
ifname <интерфейс>	Отбирает все пакеты, полученные от указанного интерфейса
on <интерфейс>	Синоним ifname
ip, arp, rarp, atalk, aarp, decnet, iso, stp, ipx, netbeui	Используются в качестве сокращения для: ether proto p, где p – один из перечисленных протоколов
tcp, udp, icmp	Используется в качестве сокращения для: ip proto p, где p – один из перечисленных протоколов
iso proto <протокол>	Собирает пакеты с указанным типом протокола OSI. Протокол может быть указан по номеру или имени (clnp, esis, isis)
clnp, esis, isis	Сокращения для выражений: iso proto p, где p – один из перечисленных протоколов
l1, l2, iih, lsp, snp, csnp, psnp	Сокращения для типов IS-IS PDU

Примитив	Описание
vpi n	Собирает пакеты ATM с указанным идентификатором виртуального пути для SunATM (Solaris)
vci n	Собирает пакеты ATM с указанным идентификатором виртуального канала для SunATM (Solaris)
lane	Собирает пакеты эмуляции ЛВС (ATM LANE) для SunATM (Solaris). Первое ключевое слово lane в выражении изменяет проверки для остальной части фильтра в предположении, что пакет относится к пакетам эмуляции Ethernet или LANE LE Control. Если ключевое слово lane не указано, проверки выполняются в предположении LLC-инкапсуляции
llc	Собирает пакеты ATM с инкапсуляцией LLC для SunATM (Solaris)
oamf4s	Собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами потока ячеек OAM F4 (VPI=0, VCI=3)
oamf4e	Собирает пакеты ATM для SunATM (Solaris), относящиеся к сквозным потокам OAM F4 (VPI=0, VCI=4)
oamf4	Собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами сквозного потока ячеек OAM F4 (VPI=0, (VCI=3 или VCI=4))
oam	Собирает пакеты ATM для SunATM (Solaris), являющиеся сегментами сквозного потока ячеек OAM F4 (VPI=0, (VCI=3 или VCI=4))
metac	Собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным мета-устройствам (VPI=0, VCI=1)
bcc	Собирает пакеты ATM для SunATM (Solaris), относящиеся к широковещательным сигнальным устройствам (VPI=0, VCI=2)
sc	Собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным устройствам (VPI=0, VCI=5)
ilmic	Собирает пакеты ATM для SunATM (Solaris), относящиеся к клиентским устройствам ILMI (VPI=0, VCI=16)
connectmsg	Собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным устройствам и содержащие сообщения Q.2931 Setup, Call Proceeding, Connect, Connect Ack, Release, Release Done
metaconnect	Собирает пакеты ATM для SunATM (Solaris), относящиеся к сигнальным мета-устройствам и содержащие сообщения Q.2931 Setup, Call Proceeding, Connect, Connect Ack, Release, Release Done
outbuf <size>	Определяет соединение, для которого в первых исходящих <size> байтах обнаружены данные, соответствующие регулярному выражению
inbuf <size>	Определяет соединение, для которого в первых входящих <size> байтах обнаружены данные, соответствующие регулярному выражению

Логические выражения

Выражения типа

expr <операция> expr

возвращают логическое значение, соответствующее отношениям между левой и правой частью. В качестве операции могут использоваться >, <, >=, <=, =, !=, а операнды expr могут быть арифметическими выражениями, включающими целые константы (запись в стандарте C), бинарные операторы +, -, *, /, &, |, <<, >>, оператор длины (offset) и данные из пакетов. Для получения значений полей из пакетов применяется синтаксис:

proto [offset : size]

Параметр proto может содержать идентификатор одного из протоколов (ether, tr, wlan, ppp, slip, link, ip, arp, rarp, tcp, udp, icmp) и задает уровень протокола 15, для которого извлекаются данные. Отметим, что tcp, udp и другие протоколы верхних уровней относятся только к пакетам IPv4, а не IPv616. Параметр offset задает смещение в байтах относительно начала заголовка указанного уровня.

Необязательный параметр size определяет размер интересующего поля в байтах. Допустимы значения размера 1, 2 и 4, по умолчанию просматривается 1 байт.

Оператор длины, указываемый ключевым словом len, определяет размер пакета в байтах. Например, выражению

ether[0] & 1 != 0

будет соответствовать весь multicast-трафик; выражение

ip[0] & 0xf != 5

позволяет собрать все пакеты IP, в которых присутствует поле опций, а фильтр

ip[6:2] & 0x1fff = 0

соберет только нефрагментированные дейтаграммы и первые фрагменты.

При выборе полей из заголовков учитывается структура пакетов соответствующего уровня. Например, tcp[0] всегда будет возвращать первый байт заголовка TCP, игнорируя фрагменты.

Некоторые поля и значения смещений могут задаваться не только числами, но и именами. В частности, для протокола поддерживается параметр icmptype (поле типа ICMP), который может принимать значения icmp-echoreply, icmp-unreach, icmp-sourcequench, icmp-redirect, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply. Для флагов TCP можно использовать идентификаторы tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack и tcp-urg.

Примитивы в выражениях можно группировать с использованием:

- скобок;
- отрицания (! или not);
- логического пересечения (&& или and);
- логического объединения (|| или or).

Оператор отрицания имеет высший уровень приоритета, операции объединения и пересечения имеют одинаковый приоритет и выполняются слева направо в порядке следования. Отметим, что для операции логического пересечения недостаточно просто указать операнды рядом, а требуется явно задать операцию (&& или and).

Если идентификатор указан без ключевого слова, предполагается ключевое слово, которое до этого использовалось последним. Например, выражение

not host vs and ace

является простым сокращением от

not host vs and host ace

Отметим, что эти выражения не эквивалентны фильтру not (host vs or ace).

Аргументы выражений могут передаваться программе фильтр как один или множество аргументов (используйте более удобную для вас форму). В общем случае выражения, содержащие метасимволы командного интерпретатора, должны передаваться как один аргумент, заключенный в кавычки.

Метасимволы в регулярных выражениях

Регулярное выражение представляет собой поисковый шаблон в виде строки, состоящей из обычных символов и метасимволов. Например, для поиска имен пользователей Ivanov или Ivanof можно использовать следующее регулярное выражение: Ivano(v|f), где | является метасимволом логического ИЛИ.

Наиболее применяемые метасимволы представлены в таблице ниже.

Метасимвол	Назначение	Пример
. (точка)	Любой символ	По шаблону a.c могут быть найдены последовательности символов abc, anc, a4c и т. п.
+	Совпадение 1 или более раз	По шаблону a+ могут быть найдены последовательности a, aa, aaa, aaaa и т. д.

Метасимвол	Назначение	Пример
?	Совпадение 1 или 0 раз	По шаблону ab?c могут быть найдены две последовательности abc и ac
*****	Совпадение 0 или более раз	По шаблону ab*c могут быть найдены последовательности ac, abc, abbc, abbbc, abbbbc и т. п.
{n}	Совпадение ровно n раз	По шаблону a{5} может быть найдена последовательность aaaaa
{n,}	Совпадение не менее n раз	По шаблону a{3,} могут быть найдены последовательности aaa, aaaa, aaaaa и т. д.
{n,m}	Совпадение от n до m раз	По шаблону a{3,5} могут быть найдены последовательности aaa, aaaa, aaaaa
|	Логическое ИЛИ	По шаблону a|b будут найдены символы a или b

Примеры правил фильтрации

Правило	Описание
pass :tcp port 25;	Разрешается прохождение любых TCP-пакетов по протоколу TCP через порт 25 (например, для получения почты)
pass :tcp port 110;	Разрешается прохождение любых TCP-пакетов по протоколу TCP через порт 110 (например, для отправки почты)
pass :tcp port 21;	Разрешается прохождение TCP-пакетов по протоколу TCP через порт 21 (например, для доступа на FTP-порты)
:tcp port 80; :tcp port 8080;	Запрещается прохождение TCP-пакетов по протоколу TCP через порты 80 и 8080 (например, для запрета выхода в сеть интернет)
:net <адрес сети>;	Запрещается прохождение IP-пакетов в определенную сеть
Pass iface="Local Area Connection 2":tcp port 80;	Разрешается прохождение TCP-пакетов через соединение "Local Area Connection 2" по протоколу TCP через порт 80
pass:;	Прохождение всех пакетов разрешается
alert : ip proto 1;	Запрещается прохождение всех IP-пакетов по протоколу ICMP. При срабатывании правила выдается оповещение
pass sched = 1 : ip proto 1;	Разрешается прохождение IP-пакетов по протоколу ICMP в период времени, определенный в расписании идентификатором 1
pass log:;	Пропускаются все (ICMP, UDP, ARP, TCP) пакеты. Журнал пакетов регистрирует детальную информацию о пакетах
pass:arp: pass in log:;	Пропускаются все входящие пакеты, все исходящие блокируются. Журнал пакетов регистрирует детальную информацию о пропущенных, входящих пакетах
pass:arp; pass out log:;	Пропускаются все исходящие пакеты, все входящие блокируются. Журнал пакетов регистрирует детальную информацию о пропущенных, исходящих пакетах
pass log alert :icmp [icmptype]=icmp-echo; pass:;	Пропускаются icmp-запросы, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-запросах
pass log alert: icmp [icmptype]=icmp-echoreply; pass:;	Пропускаются icmp-ответы, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-ответах. Остальные пакеты пропускаются без регистрации

Правило	Описание
pass log ifname="<имя интерфейса>":;	Пропускаются все пакеты через указанный интерфейс. Журнал пакетов регистрирует информацию обо всех пропущенных пакетах
pass log alert ifname="<имя интерфейса>": icmp [icmptype]=icmp-echo; pass:;	Пропускаются icmp-запросы через указанный сетевой интерфейс, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-запросах. Остальные пакеты пропускаются без регистрации
pass log alert ifname="<имя интерфейса>": icmp [icmptype]=icmp-echoreply; pass:;	Пропускаются icmp-ответы через указанный сетевой интерфейс, появляется окно с информацией о пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о icmp-ответах. Остальные пакеты пропускаются без регистрации
log:;	Блокируются все входящие и исходящие (ICMP, UDP, ARP, TCP) пакеты. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
pass:arp; in log:; pass out:;	Блокируются все входящие пакеты, все исходящие пропускаются. Журнал пакетов регистрирует детальную информацию, о заблокированных входящих пакетах
pass:arp; out log:; pass in:;	Блокируются все исходящие пакеты, все входящие пропускаются. Журнал пакетов регистрирует детальную информацию о заблокированных исходящих пакетах
pass:arp; log alert: icmp [icmptype]=icmp-echo; pass:;	Блокируются icmp-запросы. Появляется окно с информацией о заблокированных пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о заблокированных icmp-запросах
pass:arp; log alert: icmp [icmptype]=icmp-echoreply; pass:;	Блокируются icmp-ответы. Появляется окно с информацией о заблокированных пакетах (при включенном оповещении). Журнал пакетов регистрирует детальную информацию о заблокированных cmp-ответах
log ifname="<имя интерфейса>":;	Блокируются все пакеты через указанный интерфейс. Журнал пакетов регистрирует детальную информацию обо всех заблокированных пакетах
pass:arp; log ifname="<имя интерфейса>": icmp [icmptype]=icmp-echo; pass:;	Блокируются icmp-запросы через указанный интерфейс. Журнал пакетов регистрирует детальную информацию о заблокированных icmp-запросах
pass:arp; log ifname="<имя интерфейса>": icmp [icmptype]=icmp-echoreply; pass:;	Блокируются icmp-ответы через указанный интерфейс. Журнал пакетов регистрирует детальную информацию о заблокированных icmp-ответах
pass:arp; log ifname="<имя интерфейса>": tcp; pass:;	Блокируются только tcp-соединения через указанный интерфейс. Журнал пакетов регистрирует детальную информацию о заблокированных tcp-пакетах
pass:arp; log ifname="<имя интерфейса>":icmp; pass:;	Блокируются только icmp-соединения. Журнал пакетов регистрирует детальную информацию о заблокированных icmp-пакетах

Правило	Описание
pass:arp; log ifname="<имя интерфейса>": tcp port 21; pass:;	Блокируются только tcp-соединения на 21-й порт (подключения к ftp). Журнал пакетов регистрирует детальную информацию о заблокированных соединениях через 21-й порт
pass:arp; log ifname="<имя интерфейса>": tcp port 80; pass:;	Блокируются только tcp-соединения, проходящие через 80-й порт (http). Журнал пакетов регистрирует детальную информацию о заблокированных соединениях через 80-й порт
pass:arp; out log ifname="<имя интерфейса>": udp port 68; pass:;	Блокируются только исходящие соединения на 68-й udp-порт. Журнал пакетов регистрирует детальную информацию о заблокированных исходящих соединениях через 68-й порт
log ifnameace="<имя интерфейса>":greater 100; pass:;	Блокируются через указанный интерфейс пакеты размером более 100 байт. Меньше 100 — проходят. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
log ifname="<имя интерфейса>":greater 100 and less 200; pass:;	Блокируются через указанный интерфейс пакеты размером от 100 до 200 байт. Остальные проходят. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
log ifname="<имя интерфейса>":udp and greater 100; pass:;	Блокируются через указанный интерфейс udp-пакеты размером более 100 байт. Меньше 100 — проходят. Журнал пакетов регистрирует детальную информацию о заблокированных udp-пакетах
log ifname=”имя интерфейса”:udp and (greater 100 and less 250); pass:;	Блокируются через указанный интерфейс udp-пакеты размером от 100 до 250 байт. Остальные проходят. Журнал пакетов регистрирует детальную информацию о заблокированных udp-пакетах
log ifname="<имя интерфейса>":src port 21; pass:;	Через указанный интерфейс блокируется отправка пакетов с указанного порта источника. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
log ifname="<имя интерфейса>": tcp and (dst port 1025); pass:;	Блокируются через указанный интерфейс только tcp-соединения на порт 1025. Остальные пакеты разрешены. Журнал пакетов регистрирует детальную информацию о заблокированных tcp-соединениях
log ifname="<имя интерфейса>":udp and (portrange 2000-3000); pass:;	Блокируются через указанный интерфейс пакеты с и/или на заданный диапазон портов. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
log ifname="<имя интерфейса>":udp and (dst portrange 2000-3000); pass:;	Блокируются через указанный интерфейс пакеты с и/или на заданный диапазон портов. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах
out log ifname="<имя интерфейса>":icmp and dst host 192.x.x.x; pass:;	Блокируются через указанный интерфейс исходящие пакеты на указанный хост (указывается свой адрес хоста). Журнал пакетов регистрирует детальную информацию о заблокированных исходящих пакетах
log ifname="<имя интерфейса>":net 10.2; pass:;	Блокируется через указанный интерфейс трафик из/в сеть 10.2.0.0/16. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах

Правило	Описание
log ifname="<имя интерфейса>":src net 10.2; log ifname="<имя интерфейса>":dst net 10.2.2;	Блокируется через указанный интерфейс трафик из/в сеть 10.2.2.0/24. Журнал пакетов регистрирует детальную информацию о заблокированных пакетах

Правила фильтрации до авторизации

Список "Правила фильтрации до авторизации", действующий по умолчанию после установки программного обеспечения МСЭ на компьютер.

Доменные правила фильтрации

При установке ПО для параметра "Вхождение компьютера в домен" указано значение "Да" (см. стр.**12**).

Правило	Описание открытого порта
pass:arp;	Определение MAC-адреса по известному IP-адресу
pass:rarp;	Определение IP-адреса по известному MAC-адресу
pass:port 42;	Репликация WINS
pass:port 53;	Разрешение имен DNS
pass:udp port 67;	DHCP. Пакеты для сервера
pass:udp port 68;	DHCP. Пакеты от сервера
pass:port 88;	Протокол Kerberos
pass:udp port 123;	Протокол NTP, служба времени
pass:tcp port 135;	Сервис RPC
pass:udp port 137;	Служба имен NetBIOS
pass:udp port 138;	Служба датаграмм NetBIOS
pass:tcp port 139;	Служба сеансов NetBIOS
pass:port 389;	Протокол LDAP. Active Directory
pass:tcp port 443;	HTTPS, используется службой RRAS
pass:tcp port 445;	Протокол SMB. Доступ к ресурсам сети
pass:udp port 500;	Протокол IKE (IPSec)
pass:port 636;	Протокол LDAP (SSL). Active Directory
pass:tcp port 1025;	Сервис RPC
pass:tcp port 3268;	Доступ к Active Directory
pass:tcp port 3269;	Доступ к Active Directory
pass:tcp port 3389;	Сервис терминалов. RDP
pass:udp port 4433;	Сервер доступа АПКШ "Континент"
pass:udp port 4500;	Протокол IKE (IPSec)
pass:tcp port 21326;	СЗИ Secret Net
pass:tcp port 21327;	СЗИ Secret Net
pass:portrange 49152-65535;	Вход в домен Windows 7, порт назначается динамически через RPC

Локальные правила фильтрации

При установке ПО для параметра "Вхождение компьютера в домен" указано значение "Нет" (см. стр.**12**).

Правило	Описание открытого порта
pass:udp port 67;	DHCP. Пакеты для сервера
pass:udp port 68;	DHCP. Пакеты от сервера

Структура файла с расписаниями

Файл с расписаниями состоит из строк вида:

id [daily|weekly] [mon|tue|wed|thu|fri|sat|sun] [HH:MM-HH:MM];

где:

- **Id** — уникальный идентификатор расписания, число;
- **daily|weekly** — тип расписания, ежедневное или недельное;
- далее:
  - для ежедневных расписаний — временные интервалы в формате ЧасНачала:МинутаНачала- ЧасОкончания:МинутаОкончания;
  - для недельных расписаний — дни недели в виде строк (mon|tue|wed|thu|fri|sat|sun), после каждой из которых идут временные интервалы в формате ЧасНачала:МинутаНачала- ЧасОкончания:МинутаОкончания.

Каждая строка задает отдельное расписание и завершается точкой с запятой.

Пример	Пояснение
1 daily 10:00-18:00;	Правила фильтрации с идентификатором расписания "1" работают ежедневно с 10 до 18 часов
2 weekly mon 10:00-18:00 tue 10:00-18:00 wed 10:00-18:00 thu 10:00-18:00 fri 10:00-17:00;	Правила фильтрации с идентификатором расписания "2" работают с понедельника по четверг с 10 до 18 часов и в пятницу с 10 до 17

Перечень регистрируемых событий

Название события	Комментарий
Ошибка построения цепочки сертификатов сервера. Возможно, один из сертификатов цепочки был отозван (Error building server certificate chain. Maybe one or more certificates was revoked)	Клиент. Ошибка построения цепочки сертификатов. Один из сертификатов цепочки невалиден
Неверное значение поля "extended key usage" у сертификата сервера (Bad "extended key usage" of server certificate)	Клиент. Неверное значение поля "extended key usage" у сертификата сервера
Неверное значение поля "intended key usage" у сертификата сервера (Bad intended key usage of server certificate)	Клиент. Неверное значение поля "intended key usage" у сертификата сервера
Ошибка открытия хранилища PKCS7, присланного сервером (Failed to open store from PKCS7)	Клиент. Ошибка открытия хранилища PKCS7, присланного сервером
Не найдены цепочки сертификатов в хранилище PKCS7, присланном сервером (Failed to Find certificate chain in PKCS7 store)	Клиент. Не найдены цепочки сертификатов в хранилище PKCS7, присланном сервером

Название события	Комментарий
Ошибка получения DN сертификата сервера (Failed to retrieve certificate DN)	Клиент. Ошибка получения DN сертификата сервера
Ошибка получения DN корневого сертификата (Failed to retrieve issuer certificate DN)	Клиент. Ошибка получения DN корневого сертификата
Ошибка получения криптографического контекста (Failed to acquire cryptographic context)	Ошибка получения криптографического контекста
Неправильный или дуплицированный идентификатор сессии (Wrong or duplicated session)	Неправильный или дуплицированный идентификатор сессии
Неправильное или дуплицированное случайное число сервера (Wrong or duplicated server random)	Клиент. Состояние CERT_ WAIT. Неправильное или дуплицированное случайное число сервера
Неправильное или дуплицированное проверочное значение сервера (Wrong or duplicated server validation value)	Клиент. Состояние CERT_ WAIT. Неправильное или дуплицированное проверочное значение сервера
Дуплицированный сертификат сервера (Duplicated Server Certificate)	Клиент. Состояние CERT_ WAIT. Дуплицированный сертификат сервера
Неизвестный сервер (Unknown server)	Клиент. Состояние CERT_ WAIT. Неизвестный сервер
Ошибка хэширования (Failed to hash)	Состояние CERT_WAIT. Ошибка хэширования
Неправильная длина хэша (Wrong hash length)	Состояние CERT_WAIT. Неправильная длина хэша
Ошибка получения проверочного значения (Failed to get validation value)	Ошибка получения проверочного значения
Неправильное проверочное значение (Wrong validation value)	Неправильное проверочное значение
Неправильные данные от пользователя (Wrong interactive data)	Клиент. Неправильные данные от пользователя
Пользователь отказался добавить сервер и/или корневой сертификат (User cancel server addition)	Клиент. Пользователь отказался добавить сервер и/или корневой сертификат в список доверенных
Неправильные данные из сети (Wrong data from net)	Клиент. Неправильные данные из сети
Ошибка импорта сессионного ключа (Failed to import session key)	Клиент. Ошибка импорта сессионного ключа
Ошибка установки параметра ключа (Failed to set key param)	Ошибка установки параметра ключа
Ошибка расшифровки ключа (Failed to decrypt key)	Клиент. Ошибка расшифровки ключа
Неправильная длина ключа (Wrong key len)	Клиент. Неправильная длина ключа
Ошибка изменения таблицы маршрутизации (Failed to modify route table)	Клиент. Ошибка изменения таблицы маршрутизации
Ошибка преобразования номера телефона в IP-адрес (Failed to convert phone number to ip)	Клиент. Ошибка преобразования номера телефона в IP-адрес

Название события	Комментарий
Ошибка получения номера телефона из свойств соединения (Failed to retrieve phone number of connection)	Клиент. Ошибка получения номера телефона из свойств соединения
Неправильные данные соединения (Wrong connection data)	Клиент. Неправильные данные соединения
Неправильные данные пользователя (Wrong user data)	Клиент. Неправильные данные пользователя
Ошибка генерации ключа (Failed to generate key)	Ошибка генерации ключа
Ошибка экспорта ключа (Failed to export key)	Ошибка экспорта ключа
Ошибка получения серверного сертификата из бинарных данных (Failed query server certificate from binary data)	Клиент. Ошибка получения серверного сертификата из бинарных данных
Ошибка импорта публичного ключа ответной стороны (Failed to import peer public key)	Ошибка импорта публичного ключа ответной стороны
Ошибка экспорта серверного открытого ключа (Failed to export server public key)	Клиент. Ошибка экспорта серверного открытого ключа
Ошибка импорта ключа Диффи-Хеллмана (Failed to import Diffie-Hellman key)	Клиент. Ошибка импорта ключа Диффи-Хеллмана
Ошибка открытия хранилища сертификатов (Failed to open certificate store)	Ошибка открытия хранилища сертификатов
Ошибка конвертации DN сертификата (Failed to convert DN)	Ошибка конвертации DN сертификата
Ошибка поиска сертификата в системном хранилище (Failed to find certificate in store)	Ошибка поиска сертификата в системном хранилище
Плохой сертификат компьютера (Bad computer certificate)	Клиент. Плохой сертификат компьютера
Ошибка подписи ключа (Failed to sign key)	Клиент. Ошибка подписи ключа
Непонятное состояние (Wrong state)	Непонятное состояние
Ожидаемая длина сообщения меньше уже существующей (Expecting message length is less then the length of existing message)	Ожидаемая длина сообщения меньше уже существующей
Ожидаемая длина сообщения не равна полученной (Expecting message length is not equal of the length of existing message)	Ожидаемая длина сообщения не равна полученной
Длина пакета меньше, чем длина служебной информации (Length of packet is less than the length of packet header)	Длина пакета меньше, чем длина служебной информации
Нет пакета на отсылку (No packet to send)	Нет пакета на отсылку
Недостаточная длина буфера (Wrong buffer length)	Недостаточная длина буфера
Ошибка установки ключа для драйвера (Error setting key for driver)	Ошибка установки ключа для драйвера
Ошибка открытия драйвера (Error opening driver)	Ошибка открытия драйвера
Нарушена целостность файлов абонентского пункта. Обратитесь к системному администратору	Результат проверки целостности файлов абонентского пункта отрицательный

Название события	Комментарий
В системе установлен Secret Net	Результат проверки наличия СЗИ Secret Net положительный
Не обнаружен Secret Net	Результат проверки наличия СЗИ Secret Net отрицательный

Перечень файлов для контроля целостности

Контроль целостности выполняется для следующих служебных файлов абонентского пункта и МСЭ:

Наименование	Месторасположение
Все поддерживаемые ОС	
ngc.exe	Каталог установки программы
runsetublib.exe	Каталог установки программы
setuplib.dll	Каталог установки программы
tsservice.exe	Каталог установки программы
tsconndlg.dll	Каталог установки программы
tscert.dll	Каталог установки программы
uninst.exe	Каталог установки программы
ap_mgr.exe	Каталог установки программы\vpn
eapsigner161.exe	Каталог установки программы\vpn
scc3svc.exe	Каталог установки программы\vpn
sstart.exe	Каталог установки программы\vpn
vpn.chm	Каталог установки программы\vpn
sobolchecker.dll	%windir%\system32
eapext161.dll	%windir%\system32
infscerimport.dll	%windir%\system32
msvcp100.dll	%windir%\system32
mfc100.dll	%windir%\system32
mfc100enu.dll	%windir%\system32
advapi32.dll	%windir%\system32
crypt32.dll	%windir%\system32
rpcrt4.dll	%windir%\system32
secur32.dll	%windir%\system32
winscard.dll	%windir%\system32
infoseceappeer151.dll	%windir%\system32
c3ppp_vi.sys	%windir%\system32\drivers
c3mse_vi.sys	%windir%\system32\drivers
msegui.exe	Каталог установки программы\firewall
vistafwimport.exe	Каталог установки программы\firewall
firewall.chm	Каталог установки программы\firewall
sccsp.dll	%windir%\system32
sckcsp.sys	%windir%\system32\drivers

Наименование	Месторасположение
cspservice.exe	Каталог установки программы\csp
cspconfig.exe	Каталог установки программы\csp
csp_uninst.exe	Каталог установки программы\csp
etsdk.dll - на Windows x86 etsdkx64.dll - на Windows x64	Каталог установки программы\csp
ikey.dll	Каталог установки программы\csp
SneToken.dll	Каталог установки программы\csp
SnETokenEx.dll	Каталог установки программы\csp
SnETokenSC.dll	Каталог установки программы\csp
SnHwAPIExp.dll	Каталог установки программы\csp
snhwapiexp.ini	Каталог установки программы\csp
SniKey.dll	Каталог установки программы\csp
SnJacarta.dll	Каталог установки программы\csp
SnRutoken.dll	Каталог установки программы\csp
SnSable.dll	Каталог установки программы\csp
SnTmCard.dll	Каталог установки программы\csp
bio.dll	Каталог установки программы КриптоПро\CSP
cpcsp.dll	Каталог установки программы КриптоПро\CSP
cpcspi.dll	Каталог установки программы КриптоПро\CSP
cprdr.dll	Каталог установки программы КриптоПро\CSP
cprndm.dll	Каталог установки программы КриптоПро\CSP
cpssl.dll	%windir%\system32
cpsspap.dll	%windir%\system32
cpsuprt.dll	Каталог установки программы КриптоПро\CSP
cpui.dll	Каталог установки программы КриптоПро\CSP
cpverify.exe	Каталог установки программы КриптоПро\CSP
csptest.exe	Каталог установки программы КриптоПро\CSP
dallas.dll	Каталог установки программы КриптоПро\CSP
ds199x.dll	Каталог установки программы КриптоПро\CSP
etok.dll	Каталог установки программы КриптоПро\CSP
fat12.dll	Каталог установки программы КриптоПро\CSP
reg.dll	Каталог установки программы КриптоПро\CSP
rtSupCP.dll	Каталог установки программы КриптоПро\CSP
sable.dll	Каталог установки программы КриптоПро\CSP
snet.dll	Каталог установки программы КриптоПро\CSP
wipefile.exe	Каталог установки программы КриптоПро\CSP
clbcatq.dll	%windir%\system32
comctl32.dll	%windir%\system32
comdlg32.dll	%windir%\system32
cryptui.dll	%windir%\system32
gdi32.dll	%windir%\system32
iertutil.dll	%windir%\system32

Наименование	Месторасположение
imm32.dll	%windir%\system32
iphlpapi.dll	%windir%\system32
kernel32.dll	%windir%\system32
msvcrt.dll	%windir%\system32
mswsock.dll	%windir%\system32
ole32.dll	%windir%\system32
oleacc.dll	%windir%\system32
oleaut32.dll	%windir%\system32
shell32.dll	%windir%\system32
shlwapi.dll	%windir%\system32
sxs.dll	%windir%\system32
uiautomationcore.dll	%windir%\system32
urlmon.dll	%windir%\system32
user32.dll	%windir%\system32
userenv.dll	%windir%\system32
usp10.dll	%windir%\system32
uxtheme.dll	%windir%\system32
version.dll	%windir%\system32
wininet.dll	%windir%\system32
winmm.dll	%windir%\system32
ws2_32.dll	%windir%\system32
wshtcpip.dll	%windir%\system32
ОС на платформе x64	
ntdll.dll	%windir%\system32
ОС на платформе x86	
imagehlp.dll	%windir%\system32
dciman32.dll	%windir%\system32
ОС от Windows 7 и выше	
cryptbase.dll	%windir%\system32
cryptsp.dll	%windir%\system32
dhcpcsvc.dll	%windir%\system32
dhcpcsvc6.dll	%windir%\system32
dnsapi.dll	%windir%\system32
dwmapi.dll	%windir%\system32
dwrite.dll	%windir%\system32
kernelbase.dll	%windir%\system32
nsi.dll	%windir%\system32
profapi.dll	%windir%\system32
sechost.dll	%windir%\system32
sspicli.dll	%windir%\system32
winnsi.dll	%windir%\system32
wship6.dll	%windir%\system32
ОС от Windows 7 и ниже	

Наименование	Месторасположение
normaliz.dll	%windir%\system32
psapi.dll	%windir%\system32
rsaenh.dll	%windir%\system32

Программный модуль SStart

В состав абонентского пункта входит программный модуль SStart, предназначенный для автоматического управления установлением и разрывом соединения с сервером доступа АПКШ "Континент". В рамках управления модуль обеспечивает обращение стороннего приложения к абонентскому пункту и выполнение команд по установлению и разрыву соединения.

Для автоматического управления соединением используется командный файл.

При установке ПО абонентского пункта на компьютер файл SStart.exe автоматически помещается в папку \Program Files\Security Code\vpn.

Необходимые условия для работы модуля

Для корректной работы модуля SStart необходимо выполнение следующих условий:

- зарегистрированы корневой сертификат, сертификат сервера доступа и сертификат пользователя;
- в настройках абонентского пункта определен сервер доступа по умолчанию;
- в настройках аутентификации абонентского пункта установлен режим "Использовать расширенный сертификат" и указан сертификат пользователя для подключения по умолчанию.

Выполняемые команды и коды завершения работы

Ниже в таблице приведено описание команд, выполняемых модулем SStart.

Команда	Описание
sstart init [<имя соединения>]	Подготовка к выполнению команд для указанного соединения; по умолчанию имя соединения "Континент-АП"
sstart connect	Установление защищенного соединения абонентского пункта с сервером доступа; выполняется после команды sstart init
sstart break	Разрыв защищенного соединения абонентского пункта с сервером доступа
sstart isconnection [<имя соединения>]	Проверка соединения с указанным именем (по умолчанию <Континент-АП>)
sstart connection	Вывод на экран имени установленного соединения
sstart stop	Сброс настроек, выполненных командой sstart init

Для вывода на экран кода завершения используется команда echo %errorlevel%.

В следующей таблице приведены значения кодов, возвращаемых после выполнения команды.

Значение	Описание	Команды
0	Корректное завершение	Все команды
1	Командная строка не содержит исполняемых команд	Все команды

Значение	Описание	Команды
3	Исполнение команды произошло с ошибкой, не поддающейся детализации	Кроме sstart isconnection и sstart connection
	Соединение не установлено	sstart isconnection sstart connection
4	Не удалось установить соединение	sstart connect
5	Не выполнена команда init	Кроме sstart init

Применение COM для управления АП

Управление абонентским пунктом возможно с помощью COM-компонентов.

В комплект входит программный модуль tsservice_ example.vbs, использующий такие компоненты. Взяв за основу этот модуль, можно создать скрипты для автоматического управления установлением и разрывом соединения с сервером доступа АПКШ "Континент". Эти скрипты можно запускать вручную из программной строки или автоматически с помощью планировщика заданий. Необходимые условия для работы скриптов те же , что и для программного модуля SStart (см. стр.**58**).

При установке ПО абонентского пункта на компьютер файл tsservice_ example.vbs автоматически помещается в папку \Program Files\Security Code\Continent Client.

Ниже приведены примеры скриптов, созданных на основе программного модуля tsservice_example.vbs.

Установление соединения с сервером доступа

```
On Error Resume Next
' Пример вызова функций COM для работы с RAS-соединениями
' Создаем объект конфигурации
Set Cfg = CreateObject("seccode.ts.terminalstation")
' создаем объект диалога
Set Dlg = CreateObject("seccode.ts.conndlg")
' От корневого объекта спускаемся до соединения
' "default" -- название профиля, создается по умолчанию с
таким именем (не изменяется)
' "Континент АП" -- имя соединения по умолчанию (может быть
изменено, тогда нужно указать измененное)
Set Vpn = Cfg.get_vpn()
Set ConnSet = Vpn.get_connections()
For cntItem = 1 To ConnSet.Count
If ConnSet.Item(cntItem).get_name() = "Континент АП" Then
Exit For
End If
Next
' Имя телефонной книги
Dim Pbk
Pbk = ConnSet.Item(cntItem).get_pbk()
' Имя соединения
Dim Name
Name = ConnSet.Item(cntItem).get_name()
' ---
' Функции RAS-соединения
' ---
' Установить соединение
Dlg.set_pbk(Pbk)
Dlg.set_name(Name)
Dlg.set_silent(0)
```

```
Dlg.do_connect()
' в Err.Number будет HRESULT операции (0 -- ошибки нет)
If Err.Number <> 0 Then
WScript.Echo "Соединение не установлено!"
Wscript.Quit
End If
' Запросить статус соединения
Class ConnectionStatus
Public Idle, Connecting, Connected
Private Sub Class_Initialize
Idle = 0
Connecting = 1
Connected = 2
End Sub
End Class
set cs = New ConnectionStatus
If ConnSet.Item(cntItem).get_connection_status() <>
cs.Connected Then
WScript.Echo "Соединение не установлено (возможно, разорвано
пользователем)!"
Wscript.Quit
End If
```

Разрыв соединения

```
On Error Resume Next
' Пример вызова функций COM для работы с RAS-соединениями
' Создаем объект конфигурации
Set Cfg = CreateObject("seccode.ts.terminalstation")
' создаем объект диалога
Set Dlg = CreateObject("seccode.ts.conndlg")
' От корневого объекта спускаемся до соединения
' "default" -- название профиля, создается по умолчанию с
таким именем (не изменяется)
' "Континент АП" -- имя соединения по умолчанию (может быть
изменено, тогда нужно указать измененное)
Set Vpn = Cfg.get_vpn()
Set ConnSet = Vpn.get_connections()
For cntItem = 1 To ConnSet.Count
If ConnSet.Item(cntItem).get_name() = "Континент АП" Then
Exit For
End If
Next
' Запросить статус соединения
Class ConnectionStatus
Public Idle, Connecting, Connected
Private Sub Class_Initialize
Idle = 0
Connecting = 1
Connected = 2
End Sub
End Class
set cs = New ConnectionStatus
If ConnSet.Item(cntItem).get_connection_status() <>
cs.Connected Then
WScript.Echo "Соединение не установлено (возможно, разорвано
пользователем)!"
Wscript.Quit
End If
WScript.Echo "Соединение установлено! Разрываем
соединение..."
```

```
' Закрыть соединение
ConnSet.Item(cntItem).do_break(True)
' в Err.Number будет HRESULT операции (0 -- ошибки нет)
If Err.Number <> 0 Then
WScript.Echo "Ошибка при разрыве соединения!"
Wscript.Quit
End If
WScript.Echo "Соединение разорвано"
```

Документация

1.	Средство криптографической защиты информации "Континент-АП". Руководство администратора. Windows
2.	Средство криптографической защиты информации "Континент-АП". Руководство пользователя. Windows