А Д М И Н И С Т Р И Р О В А Н И Е

системы защиты информации

ViPNet [CUSTOM]

ОАО “ИнфоТеКС”, Москва
(495) 737-61-92

education@infotecs.ru
www.infotecs.ru

infotecs®

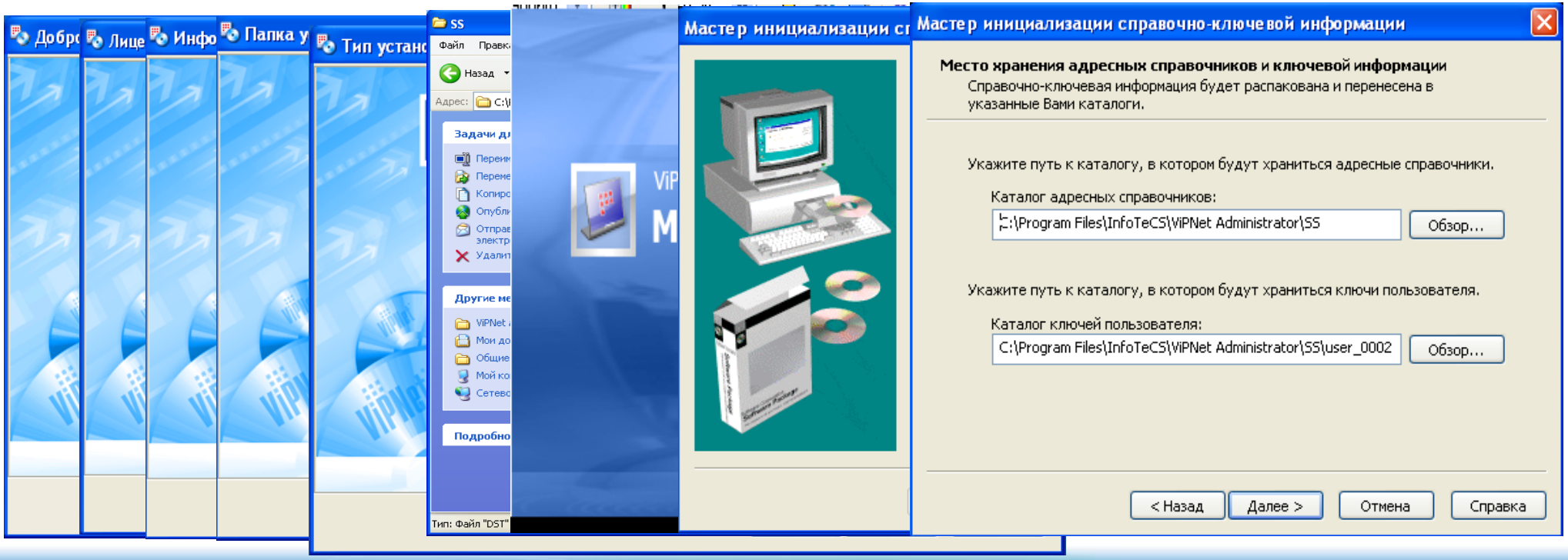
ViPNet Клиент

Установка ПО ViPNet Клиент

1. После принятия соглашения и ввода имени и организации следует указать путь установки. По умолчанию это:
   C:\Program Files\InfoTeCS\ViPNet Client (для клиента);
   C:\Program Files\Infotecs\ViPNet [Администратор]\SS (для администратора).
Не рекомендуется менять пути установки.

2. Поместить в каталог установки файл-дистрибутив abn_AAAA.dst.

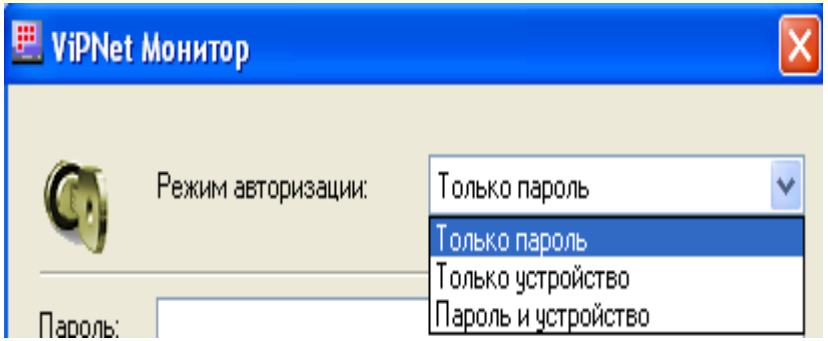
3. После перезагрузки необходимо произвести первичную инициализацию системы защиты, во время которой необходимо указать имя пользователя, его пароль, данные для сертификата ЭЦП, место размещения ключевой информации и другую информацию.



Первый запуск программы ViPNet Клиент

ПО ViPNet Клиент поддерживает три вида авторизации:

- *Только пароль* – в этом случае пользователь для авторизации будет использовать ручной ввод пароля;
- *Только устройство* – в этом случае парольный ключ пользователя будет считываться с внешнего устройства хранения данных. Для осуществления входа в программу пользователь должен обеспечить контакт ключа с устройством хранения данных.
- *Пароль и устройство* – в этом случае на устройстве размещается так называемый Случайный Ключ Защиты Пользователя (СКЗП). Для осуществления входа в программу пользователь должен обеспечить контакт ключа с устройством хранения данных и ввести пароль.



ViPNet Клиент выполняет функции:

1. Сетевой экран

Обеспечение надежной защиты от атак из локальных и глобальных сетей посредством:

- фильтрации IP-трафика по заданным параметрам (по IP-адресу, протоколу, порту, типу сервисов и приложений)
- выбора режима безопасности (безопасная работа при сохранении функциональности - 3 режим: «бумеранг»)
- контроля сетевой активности приложений для обнаружения программ-Троянов (белые и черные списки)
- обнаружения сетевых вторжений (IDS)

2. Шифратор TCP/IP-трафика

Защита ЛЮБОГО вида трафика ЛЮБЫХ приложений между объектами защищенной сети ViPNet.

Защита обеспечивается сохранением конфиденциальности, подлинности, целостности путем применения технологий

ШИФРОВАНИЯ

ХЭШИРОВАНИЯ

ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

ViPNet Клиент включает:

1. Драйвер защиты IPLir (ViPNet-драйвера)

- обеспечивает фильтрацию ВСЕГО трафика – входящего и исходящего;
- обеспечивает шифрование указанного трафика (на основе криптоядра ДОМЕН-К);
- взаимодействует с драйверами сетевых карт компьютера с целью обеспечения независимости ПО ViPNet от операционной системы.

2. Программу Watchdog

- обеспечивает слежение за наличием в памяти компьютера ViPNet-драйвера и программы [Монитор].
- при некорректной работе ViPNet-драйвера перезапускает операционную систему;
- при некорректной работе [Монитора] перезапускает программу указанное количество раз и, в случае неработоспособности [Монитора], перезапускает операционную систему.

3. Транспортный модуль MFTP – обеспечивает настройку транспортных каналов и передачу конвертов [Деловой Почты] и файлового обмена между узлами сети.

4. Программу Контроль приложений – обеспечивает наблюдение за программами и службами операционной системы на предмет их работы в сети.

ViPNet Клиент включает:

5. **Регистрацию в прикладной задаче** [Защита трафика]**, позволяющую работать с интерфейсом** ViPNet-драйвера **и транспортным модулем** MFTP

- обеспечивает настройку фильтров IP-пакетов, выбор режимов безопасности, ведение журнала IP-пакетов, конфигурации работы сетевого экрана;
- ограничивает полномочия пользователей по работе с системой ViPNet;
- обеспечивает защищенный обмен файлами и сообщениями (защищенные чат и конференция) посредством шифрования;
- издает и регистрирует сертификат открытого ключа ЭЦП пользователя;
- формирует асимметричные ключи шифрования связи на прикладном уровне (ТК);
- настраивает режимы работы СУ с компьютерами, не имеющими ПО ViPNet;
- позволяет получить с удаленных компьютеров их Журналы IP-пакетов.

ViPNet [Клиент] включает:

6. Регистрацию в прикладной задаче [Деловая почта], обеспечивающую работу защищенного почтового клиента

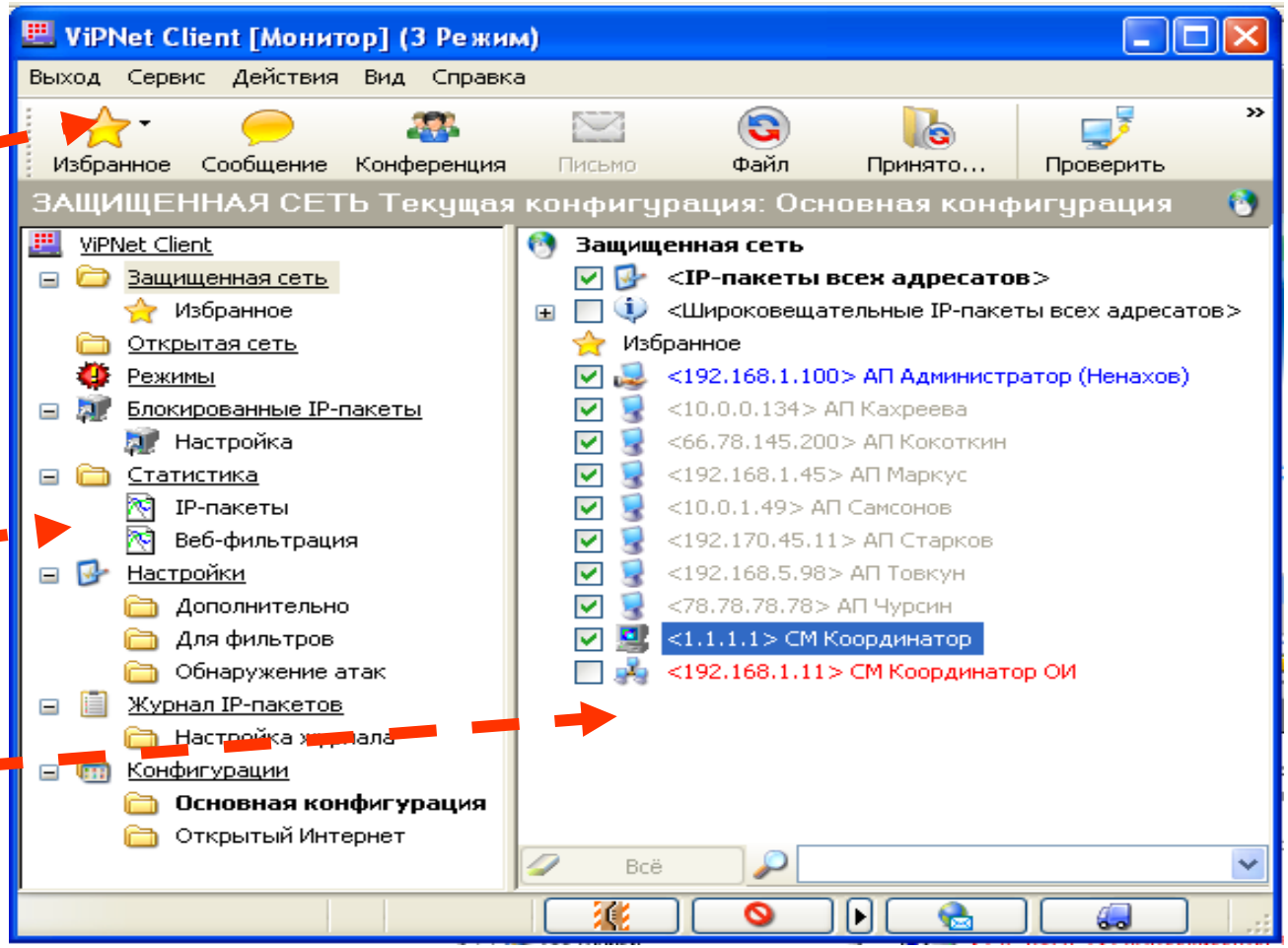
- обеспечивает защищенный обмен почтовыми сообщениями (посредством шифрования и подписания электронной цифровой подписью письма и/или его вложения);
- обеспечивает ведение базы данных и архивов писем (в том числе удаленных писем) в защищенном виде;
- обеспечивает автоматизацию работы с конфиденциальной документацией посредством применения **автопроцессинга** – процесса автоматической обработки **исходящих файлов и входящих писем.**

После прохождения первичной инициализации в ViPNet Клиенте появится окно «Защищенная сеть»

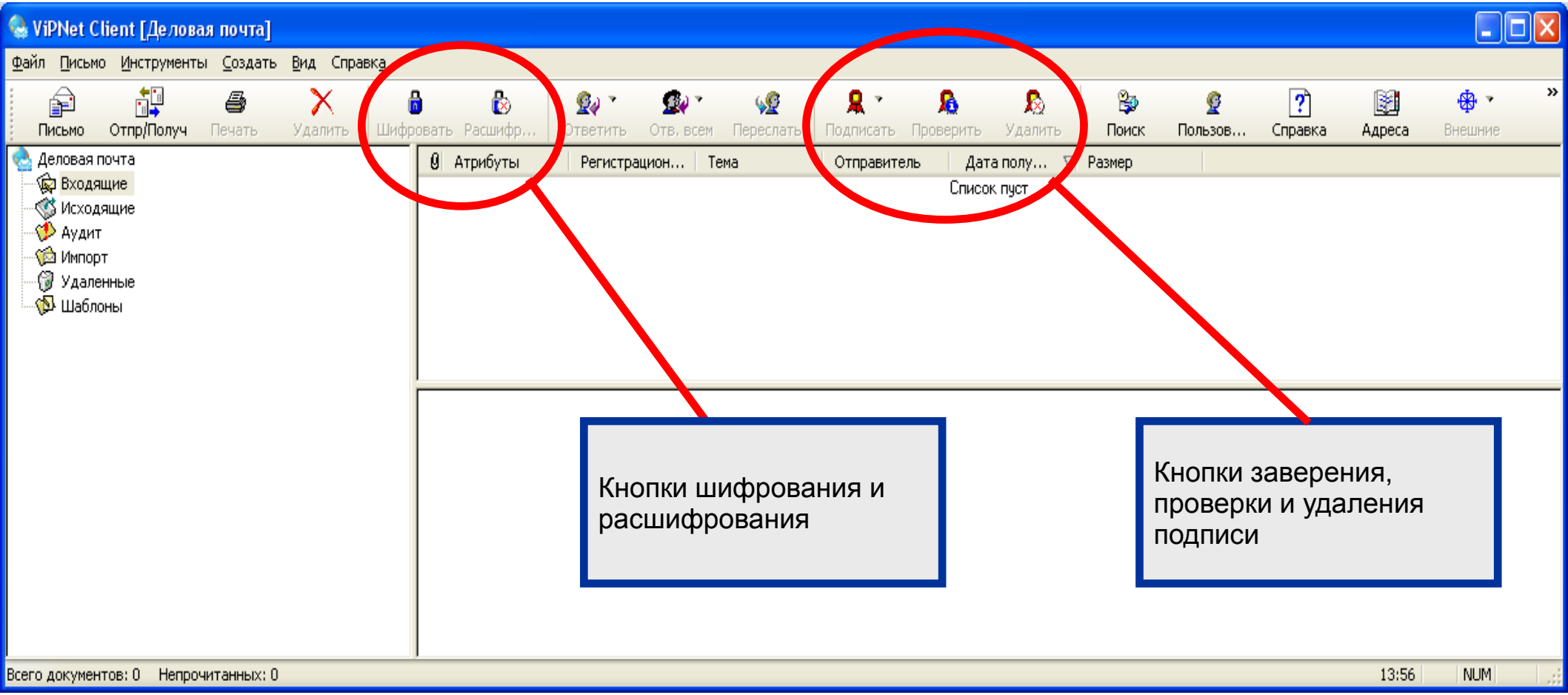
Панель пользовательских приложений

Дерево настроек программы

Окно настроек



ViPNet Деловая почта



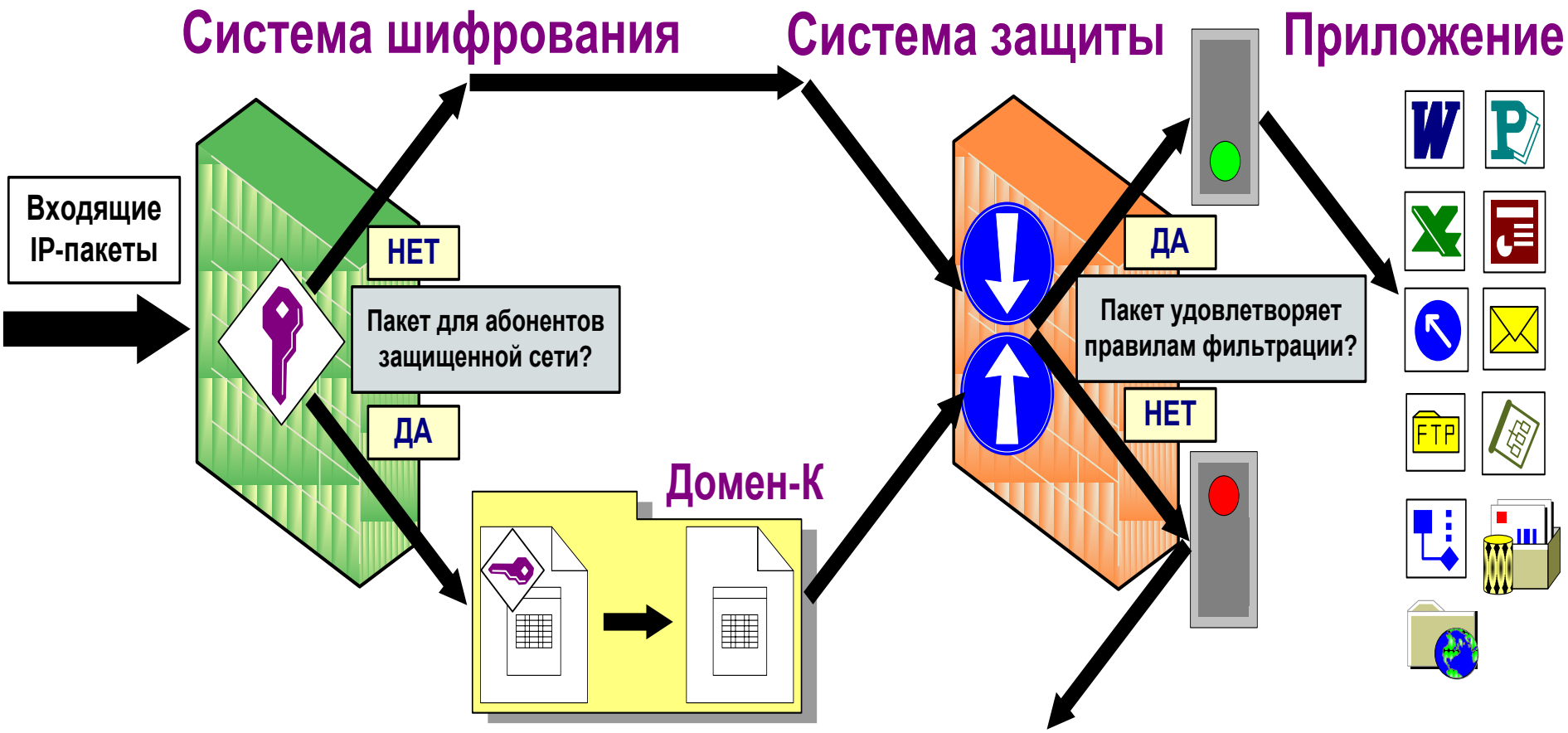
«Защищенная сеть» – совокупность компьютеров, входящих в состав виртуальной сети ViPNet (т.е. с установленным ПО ViPNet). В окне (настройках) Защищенной Сети указаны компьютеры с Типами Коллективов (ТК), с которыми данный ТК имеет связь.

На ViPNet Клиенте для всех сетевых интерфейсов будет установлена одна политика безопасности (один режим безопасности).

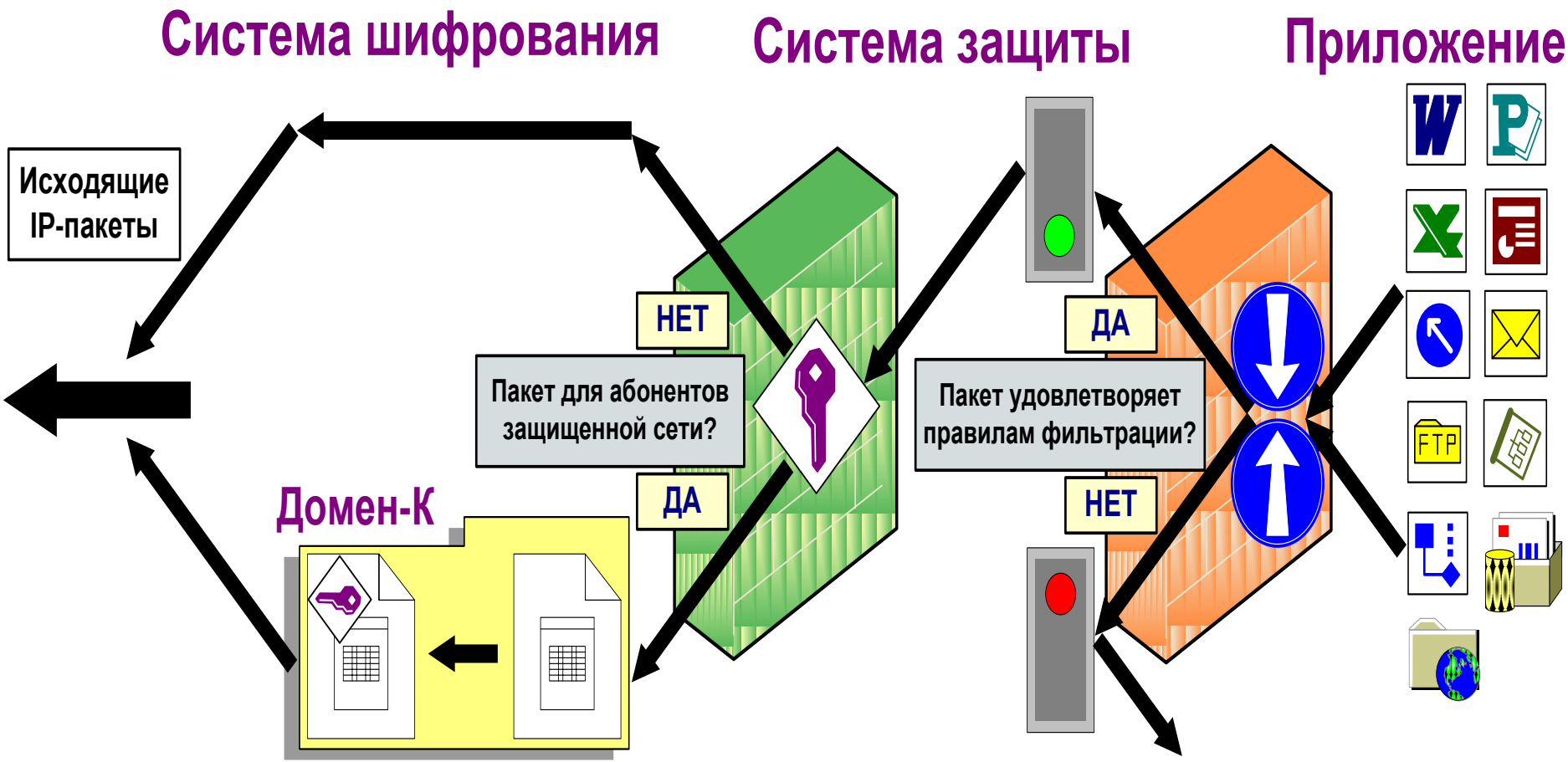
«Открытая сеть» – совокупность незащищенных компьютеров (не имеющих установленного ПО ViPNet), которые имеют право обмениваться информацией с защищенными компьютерами (межсетевой экран компьютера VPN-сети не блокирует информацию, полученную от незащищенного компьютера).

infotecs®

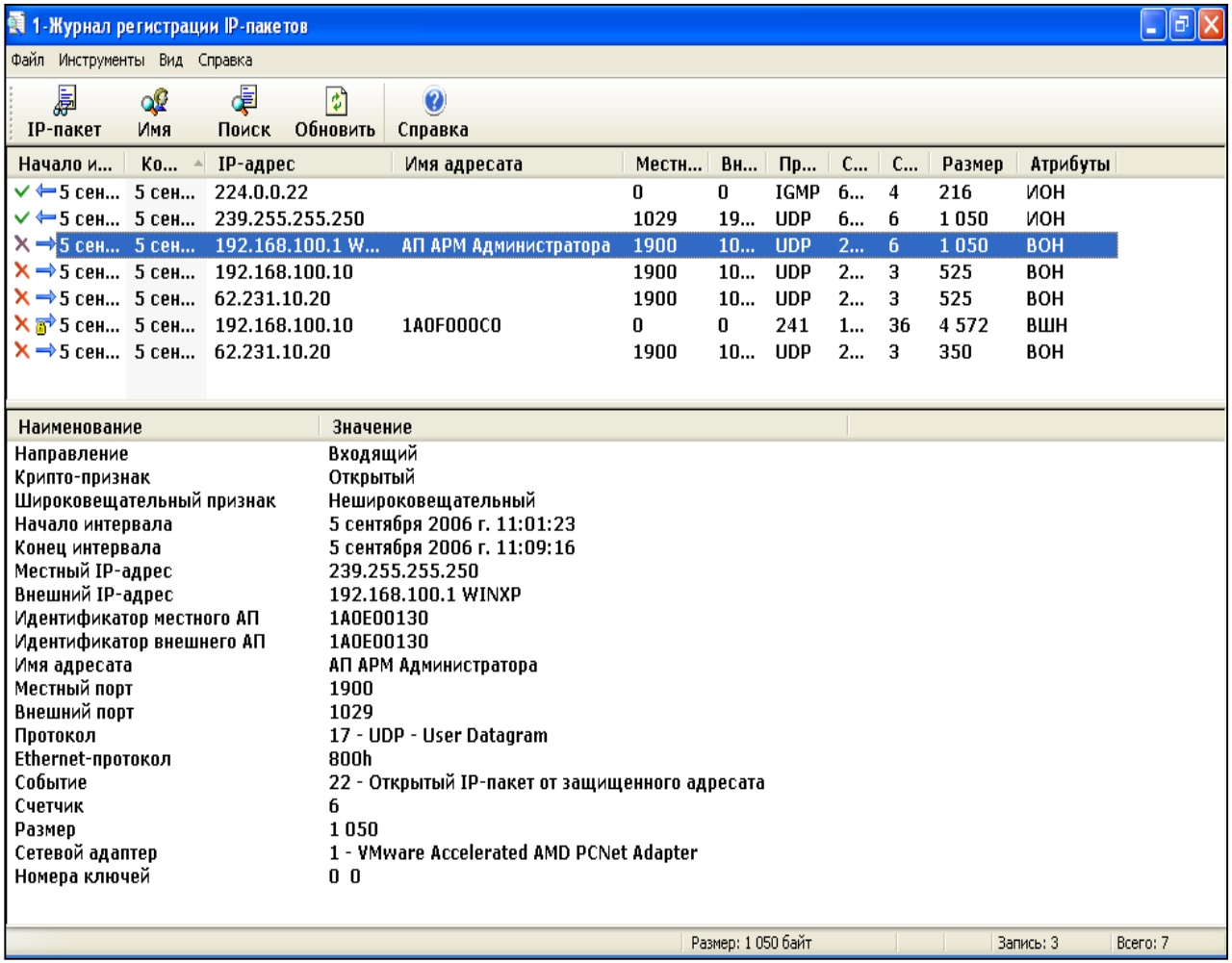
Технология обработки входящих IP-пакетов



Технология обработки исходящих IP-пакетов



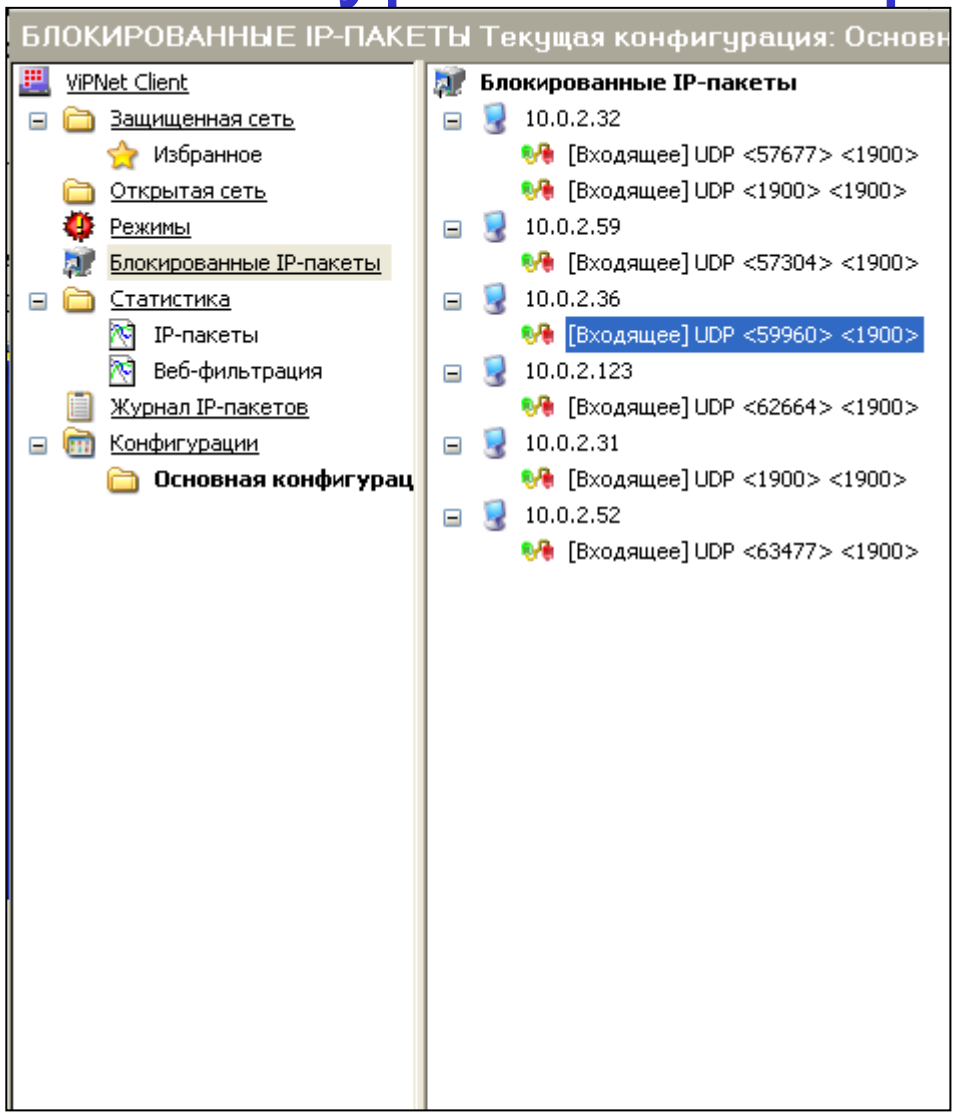
В Журнале IP-пакетов производится Регистрация ВСЕХ IP-пакетов

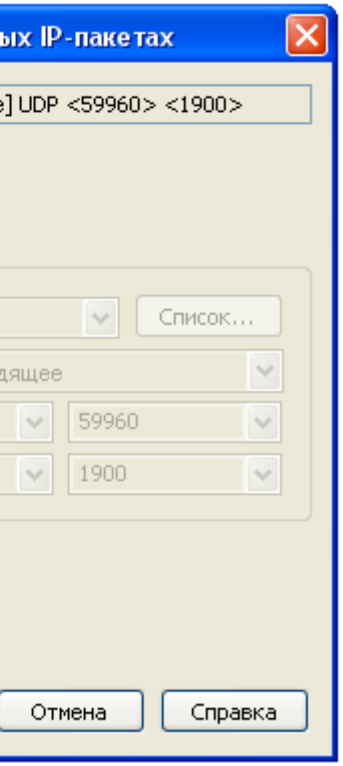


Журнал фиксирует характеристики входящих и исходящих пакетов за заданный промежуток времени:

- направление пакета;
- время прохождения пакетов;
- IP-адрес получателя для исходящих пакетов;
- IP-адрес отправителя для входящих пакетов;
- результат обработки пакета (зашифрован/расшифрован, пропущен/не пропущен, и т.п.);
- номер протокола;
- номер порта (для TCP, UDP и ICMP).

Журнал блокированных IP-пакетов





Режимы безопасности

Режим безопасности – набор правил (политик безопасности), в соответствии с которыми производится обработка входящих/исходящих и зашифрованных/незашифрованных IP-пакетов.

1 режим – «Блокировать IP-пакеты всех соединений»
блокируется весь открытый (незашифрованный) трафик: работа только внутри VPN

2 режим – «Блокировать все соединения кроме разрешенных»
разрешает работу с зарегистрированными открытыми ресурсами

3 режим – «**Бумеранг** (Пропускать все исходящие соединения кроме запрещенных)»
режим инициативных исходящих соединений, оптимален для работы с Интернет

4 режим – «Не блокировать открытый IP-трафик»
ничего не блокируется, но все фиксируется

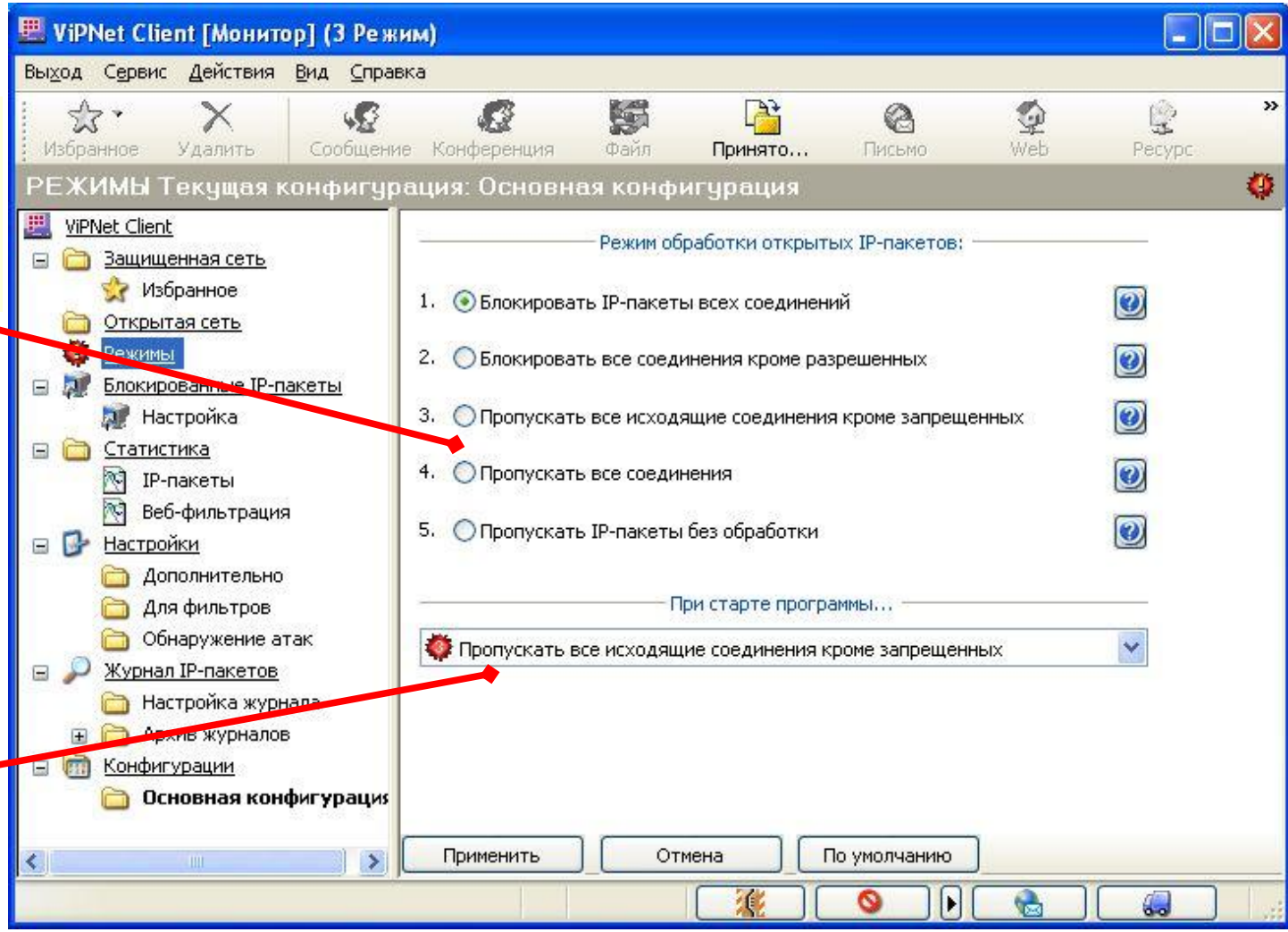
5 режим – «Отключение драйвера ViPNet»

Тестовые режимы!

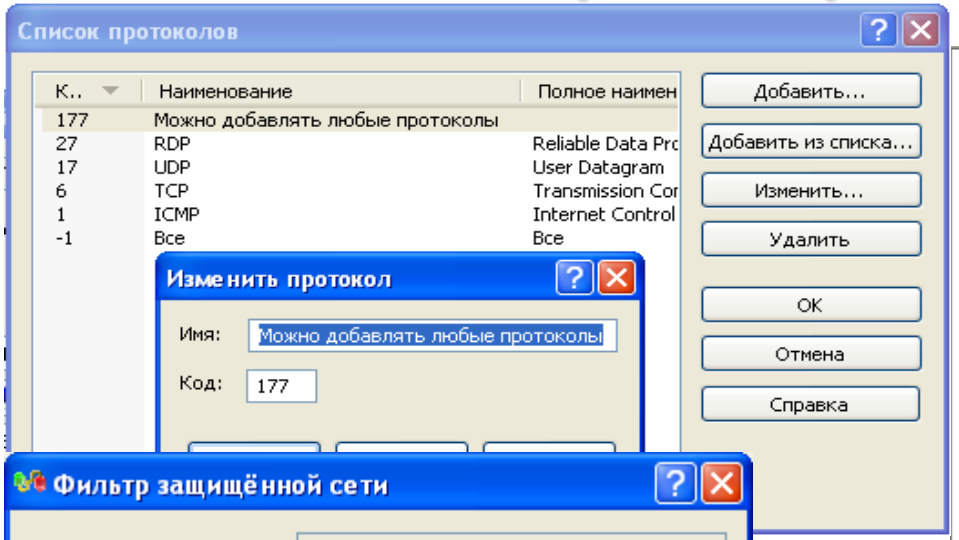
Выбор режимов безопасности

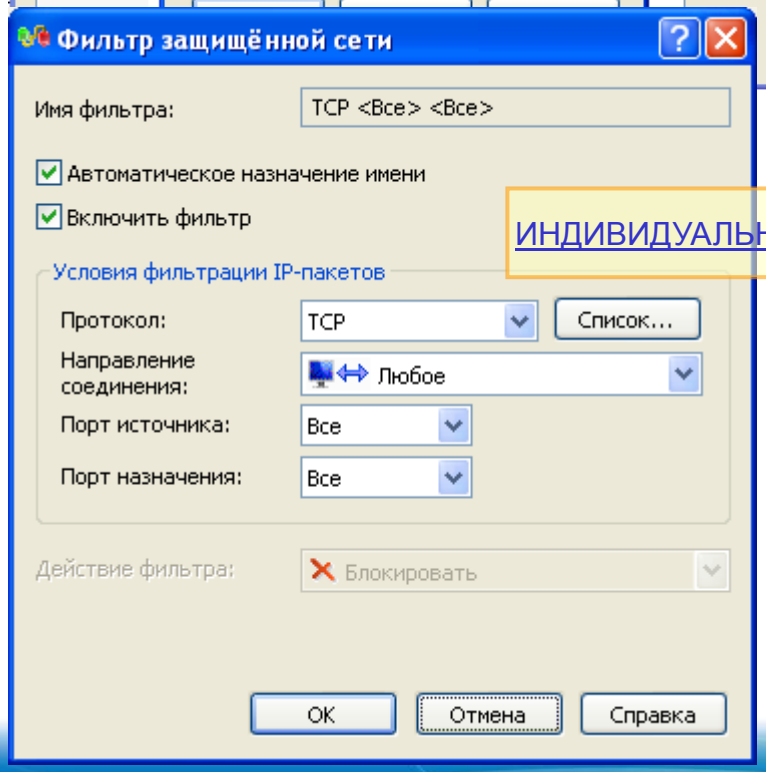
Смена текущего режима безопасности (по умолчанию установлен третий режим безопасности)

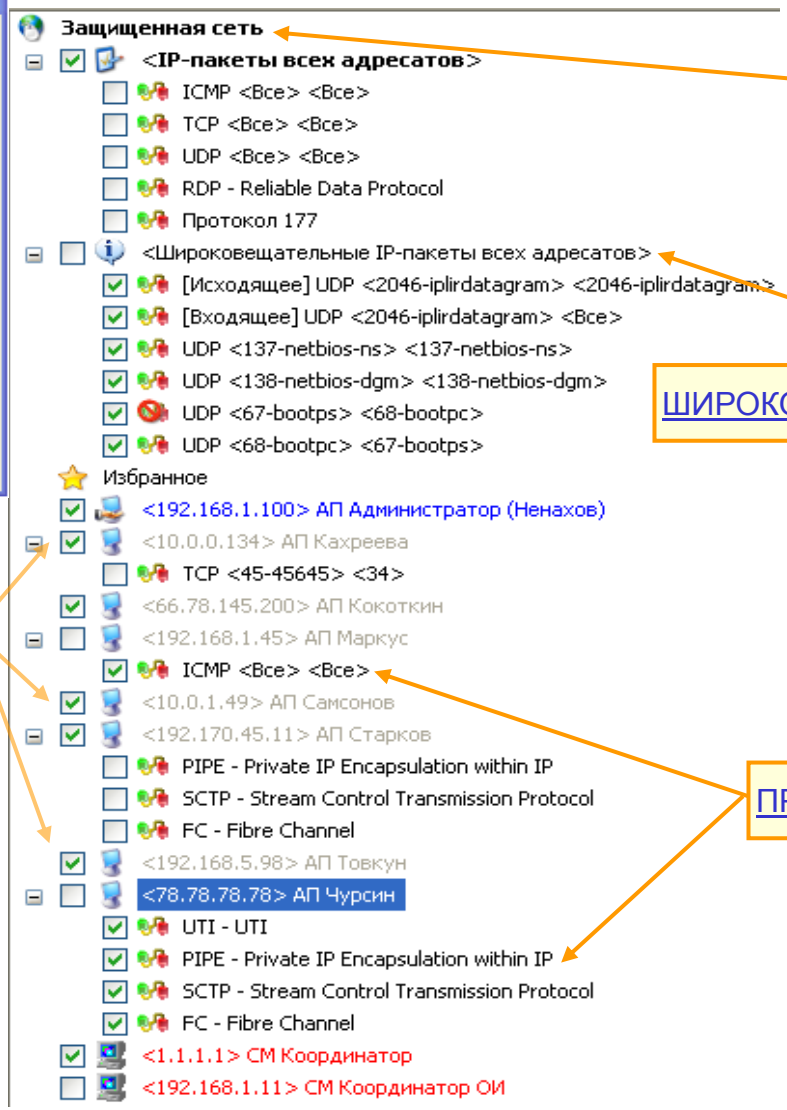
Выбор режима безопасности при старте программы (В этот режим будет установлен драйвер IPLir при запуске программы Монитор)



Виды фильтров *Защищенной сети*







ГЛАВНЫЙ

ШИРОКОВЕЩАТЕЛЬНЫЙ

ИНДИВИДУАЛЬНЫЙ

ПРОТОКОЛОВ

Виды фильтров *Открытой сети*

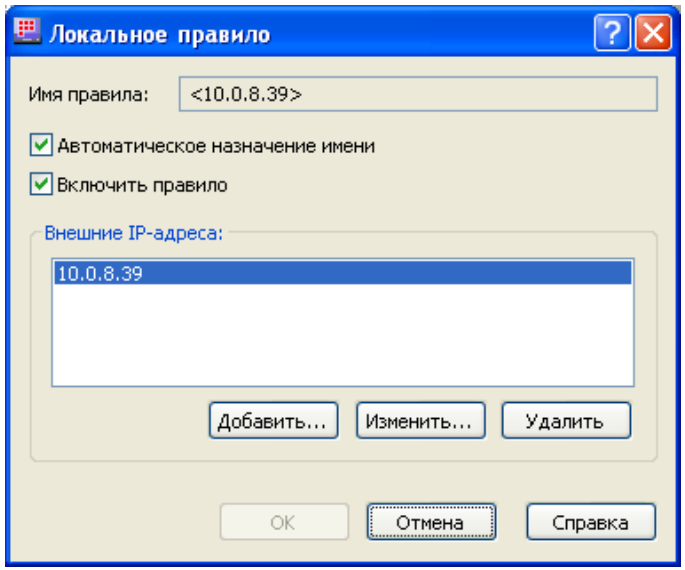
ШИРОКОВЕЩАТЕЛЬНЫЙ

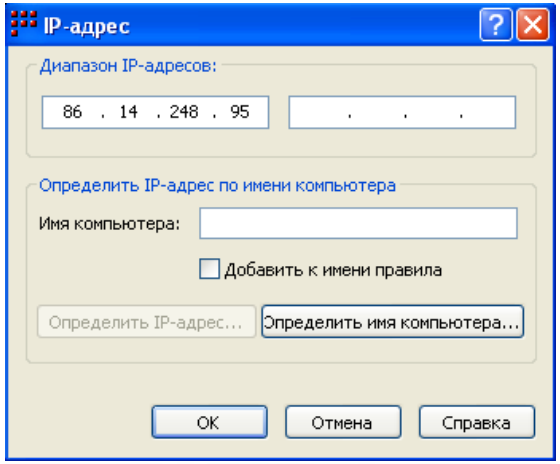
ИНДИВИДУАЛЬНЫЙ

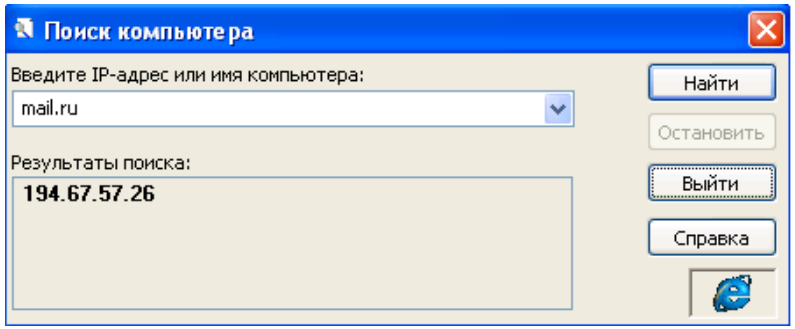
ГЛАВНЫЙ

ПРОТОКОЛОВ

Наименование	Действие	Порт отп...	Порт по...	Прот...	Расписание
Открытая сеть					
Широковещательные IP-пакеты					
Все широковещательные IP-пакеты					
Сервис имён NETBIOS	Пропускать	137	137	UDP	
Сервис датаграмм NETBIOS	Пропускать	138	138	UDP	
DHCP сервер	Пропускать	67	68	UDP	
DHCP клиент	Пропускать	68	67	UDP	
Локальные входящие IP-пакеты					
Бабушка из Конотопа					
Локальный входящий фильтр	Блокиров...	Все	Все	TCP	
Все протоколы	Пропускать			Все	
Все локальные входящие IP-пакеты					
DHCP сервер	Пропускать	67	68	UDP	
Локальные исходящие IP-пакеты					
Мое рабочее место					
Локальный исходящий фил...	Блокиров...			ICMP	
Все протоколы	Пропускать			Все	
Все локальные исходящие IP-пакеты					
DHCP клиент	Пропускать	68	67	UDP	







Транспортный модуль ViPNet

Обеспечивает:

- надежную и безопасную передачу транспортных конвертов различных прикладных задач (например, ЦУС, УКЦ, Деловая Почта) между сетевыми узлами ViPNet-сети

- весь служебный информационный обмен сетевых узлов сети ViPNet

Связь:

по каналу **MFTP** (протокол *TCP*):

✓проводится идентификация узлов-корреспондентов и устанавливается соединение по протоколу TCP;

✓проводится аутентификация узлов и осуществляется прием/передача транспортных конвертов.

по каналу **SMTP/POP3:**

✓ транспортный модуль MFTP переадресует конверты для отправки модулю MailTrans;

✓ модуль MailTrans передает конверты узлу-получателю через сервер SMTP и забирает с сервера POP3 конверты, предназначенные для узла-отправителя

Выключен:

✓ Данный параметр доступен только при настройке канала для своего координатора. Используется для запрета обмена конвертами через свой координатор. Для того чтобы полностью прекратить передачу конвертов, нужно настроить такой же параметр и на самом координаторе в настройках для Вашего АП. Иначе, при инициировании соединения с Вашим АП со стороны координатора, произойдет прием и передача всех имеющихся конвертов от и для Вашего АП.

Через сервер

✓ Этот параметр доступен только при настройке канала для АП. Настройка этого параметра для какого-либо АП означает, что обмен конвертами с данным АП осуществляется через свой координатор по каналу MFTP.

Транспортный модуль ViPNet

В составе **ViPNet Клиента** транспортный модуль **MFTP** работает в режиме **клиента** и передает конверты другим АП в соответствии с установленным каналом.

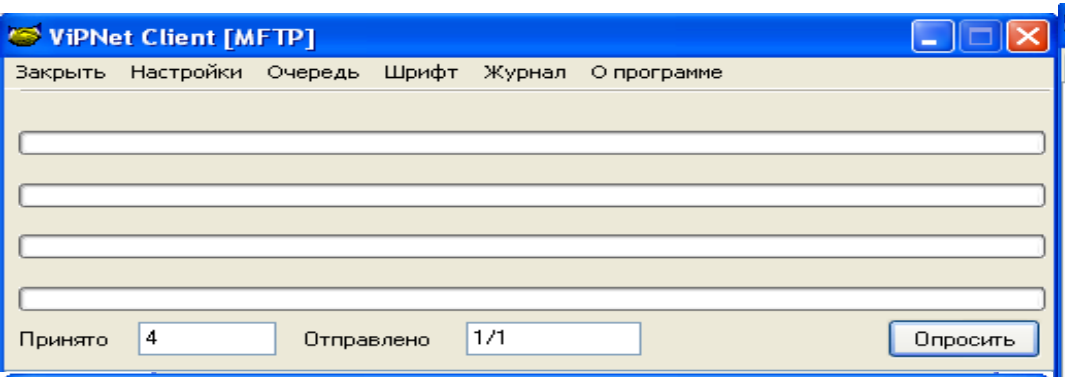
В составе **ViPNet Координатора** транспортный модуль работает в режиме **сервера**. В этом случае передача конвертов осуществляется в соответствии с таблицами маршрутизации.

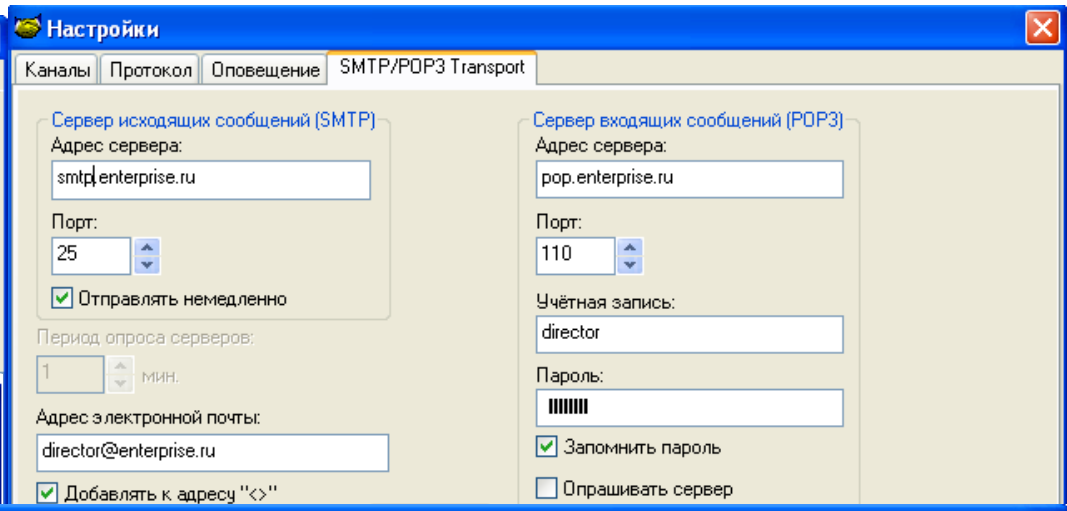
При разрывах соединений передача информации всегда продолжается с точки разрыва!

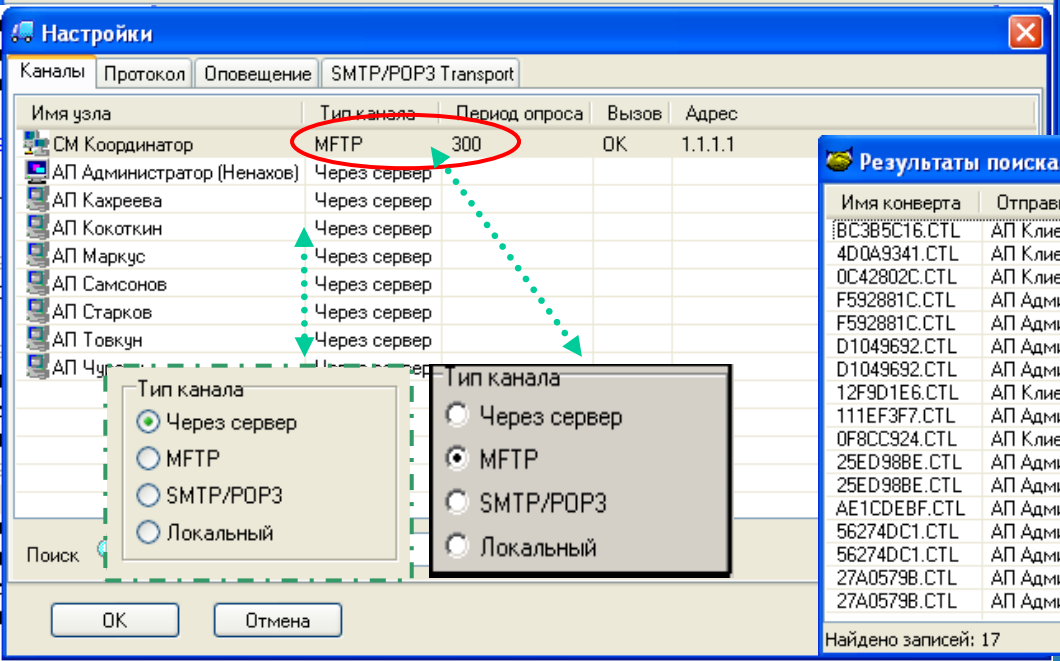
Управление транспортным уровнем занимается модуль MFTP

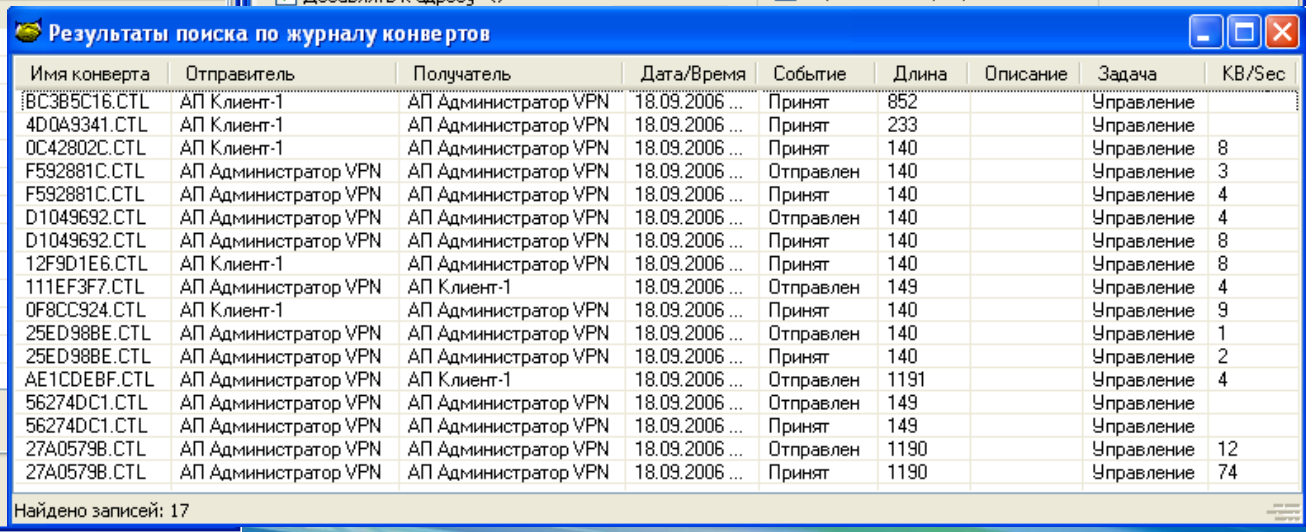
Возможно:

- указывать каналы работы сетевых узлов (путь прохождения информации от отправителя к получателю);
- настраивать протоколы вывода событий на экран и в файл, а также настройки оповещения о приходе новой почты на АП;
- обеспечивать работу канала по протоколам SMTP и POP3;
- просматривать журнал конвертов и очередь конвертов, ожидающих отправки.







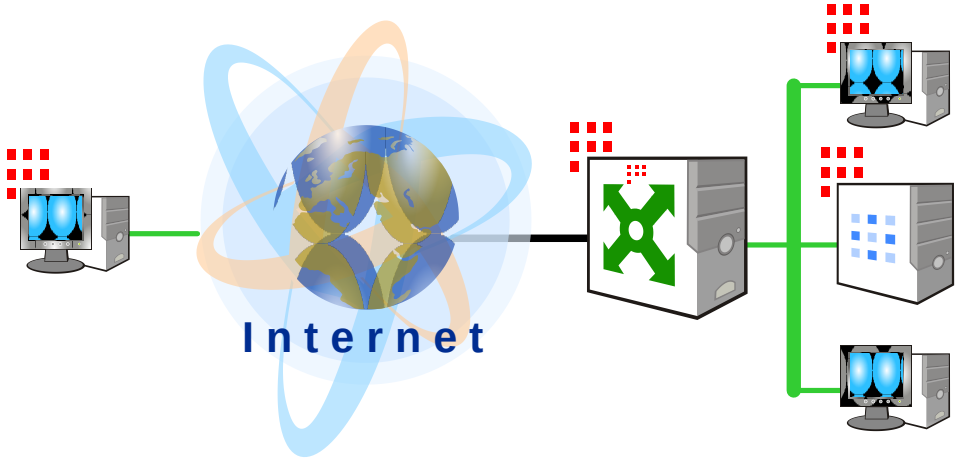


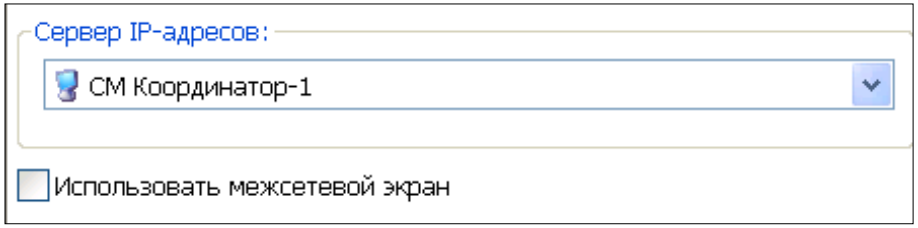
Настройки работы ViPNet Клиента через сетевой экран

Режим работы через межсетевой экран («за межсетевым экраном») означает, что Клиент защищенной сети выходит в сеть общего пользования посредством какого-либо устройства, выполняющего функцию шлюза. Т.е. весь трафик, которым обменивается Клиент с сетью, будет проходить через посредника – межсетевой экран.

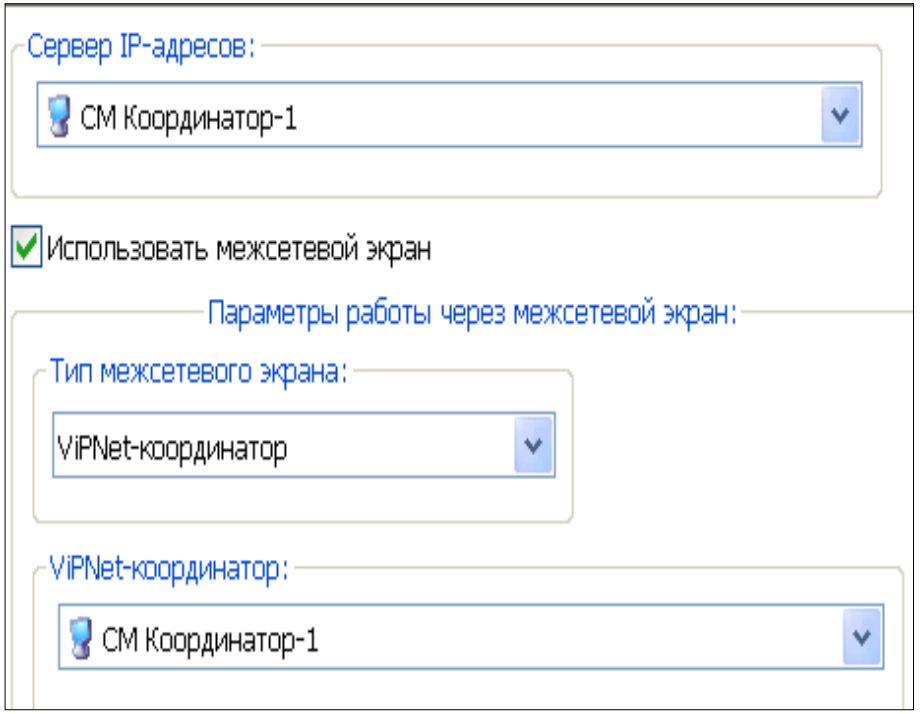
Каждый Клиент сети ViPNet в реальной локальной сети может работать в четырех режимах:

Автономная работа («сам за собой»)





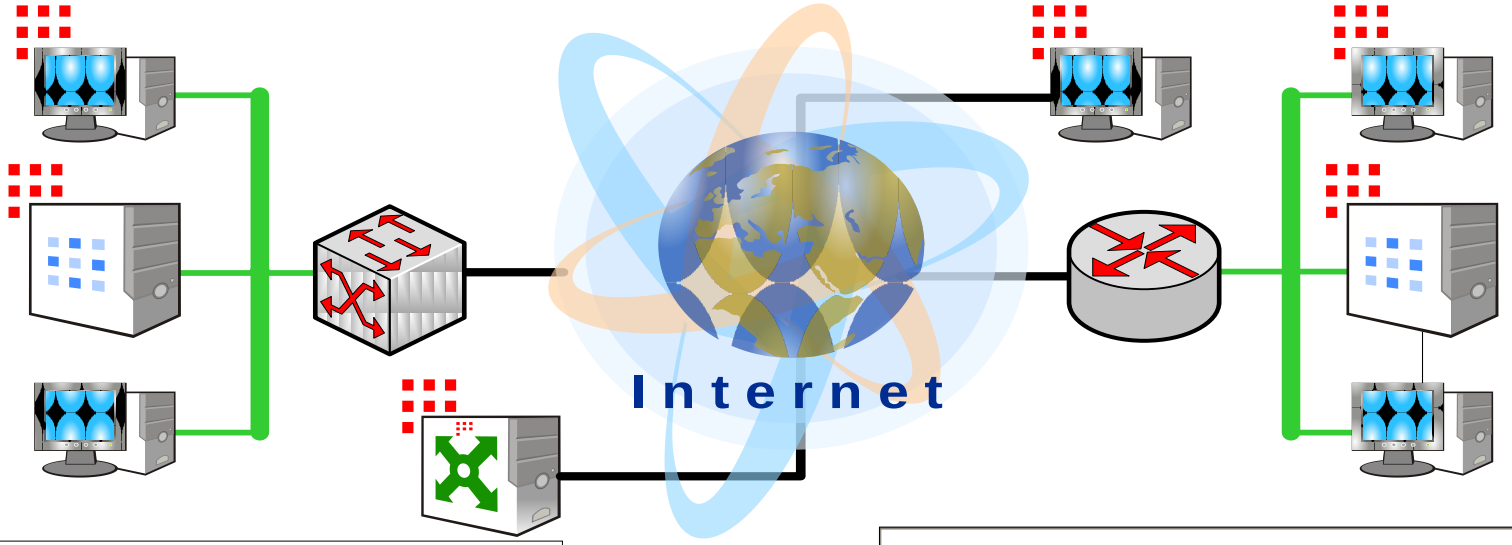
За ViPNet-Координатором



infotecs®

За устройством с DNAT

За устройством с SNAT



Сервер IP-адресов:

СМ Координатор-1

Использовать межсетевой экран

Параметры работы через межсетевой экран:

Тип межсетевого экрана:

С динамической трансляцией адресов

Порт UDP:

55777

25

Период опроса сервера IP-адресов для обеспечен
пропуска входящего трафика через межсетевой э
(секунд)

Любой трафик с внешними узлами направлять через сервер IP-адресов

IP-адрес доступа:

192 . 168 . 1 . 5

Список внешних IP-адресов

192.168.1.5
218.64.79.42
18.36.72.144

OK

Отмена

Сервер IP-адресов:

СМ Координатор-1

Использовать межсетевой экран

Параметры работы через межсетевой экран:

межсетевого экрана:

статической трансляцией адресов

Порт доступа UDP:

55777

фиксировать внешний IP-адрес доступа через межсетевой экран

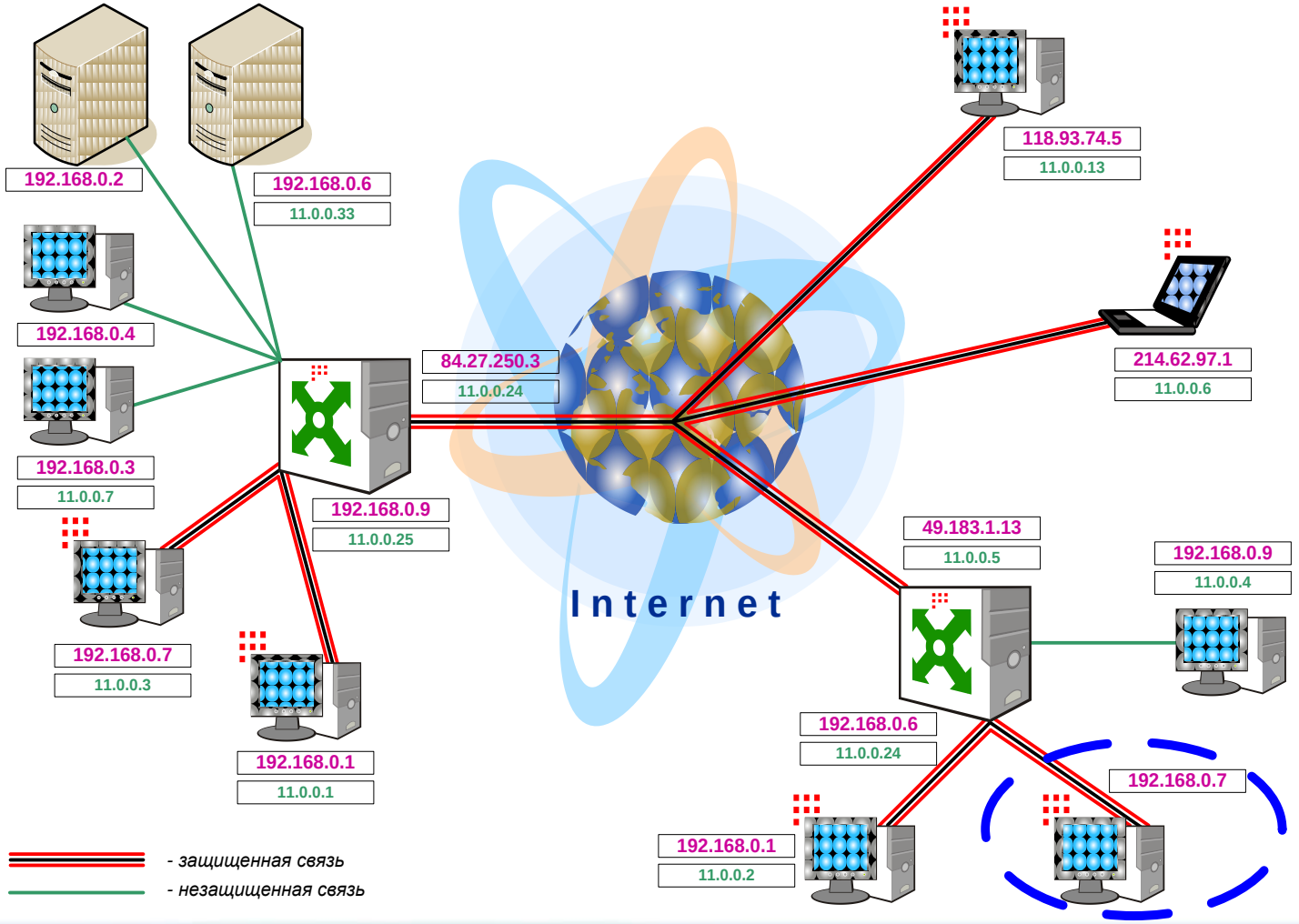
дрес доступа:

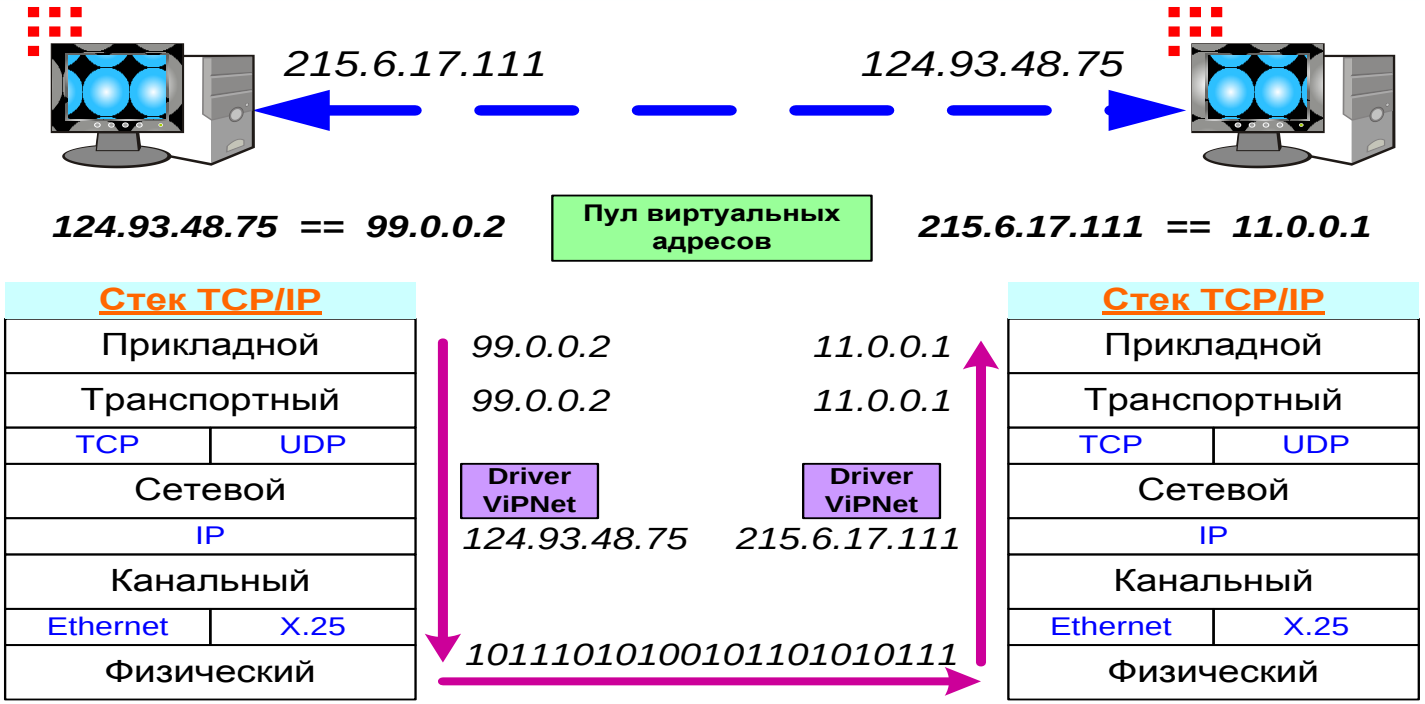
192 . 168 . 1 . 5

Виртуальный IP-адрес

- это IP-адрес сетевого интерфейса компьютера, используемого приложением ОС для более удобной и прозрачной работы внутри виртуальных локальных/глобальных сетей (VPN).

ПО ViPNet каждого Сетевого Узла (СУ) присваивает каждому из СУ сети VPN его виртуальный IP-адрес, этот адрес используется исключительно для сети ViPNet и позволяет работать всем компьютерам виртуально в одной *локальной* сети





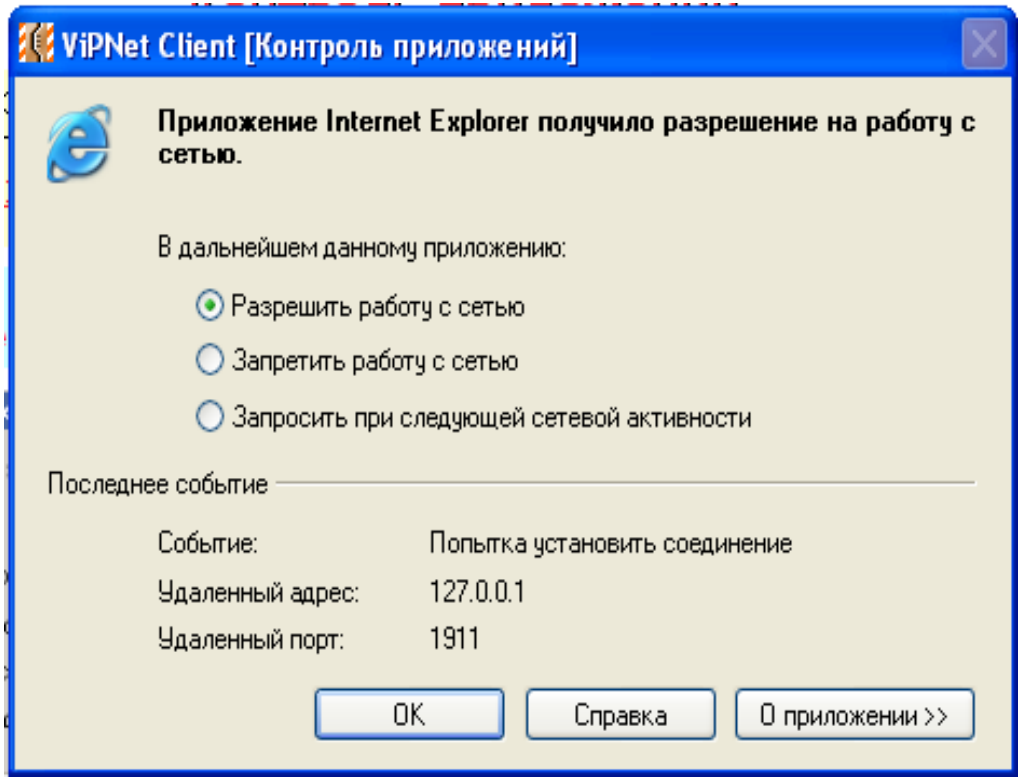
Виртуальные IP-адреса:

- определяются на прикладном уровне стека протоколов TCP/IP, на сетевом уровне стека драйвер ViPNet заменяет виртуальные адреса на реальные для передачи информации через реальные сети.
- Привязаны к уникальным шестнадцатиричным идентификаторам узлов (задаются в Центре управления сетью ViPNet)
- используются при взаимодействии с компьютерами с ПО ViPNet Клиент или Координатор, которые установлены за устройствами, выполняющие функции NAT, proxy, firewall. Также используются при взаимодействии с компьютерами, которые туннелируются (защищаются) ViPNet Координатором.
- для обеспечения связи с защищенными компьютерами и туннелируемыми открытыми компьютерами в локальных сетях с пересекающимися внутренними адресами

Контроль приложений

Программа «Контроль Приложений» (Reverse Firewall) предназначена для управления приложениями ОС, пытающихся получить доступ к сетевым картам компьютера, и ограничения несанкционированных попыток приложений выйти в локальную/глобальную сеть.

Возможность работы с программой Reverse firewall **определяется файлом infotecs.re.**
Полномочия по работе с программой Reverse firewall **определяются в ЦУСе в ПЗ Защита трафика.**



Работающий Контроль приложений

Неработающий Контроль приложений

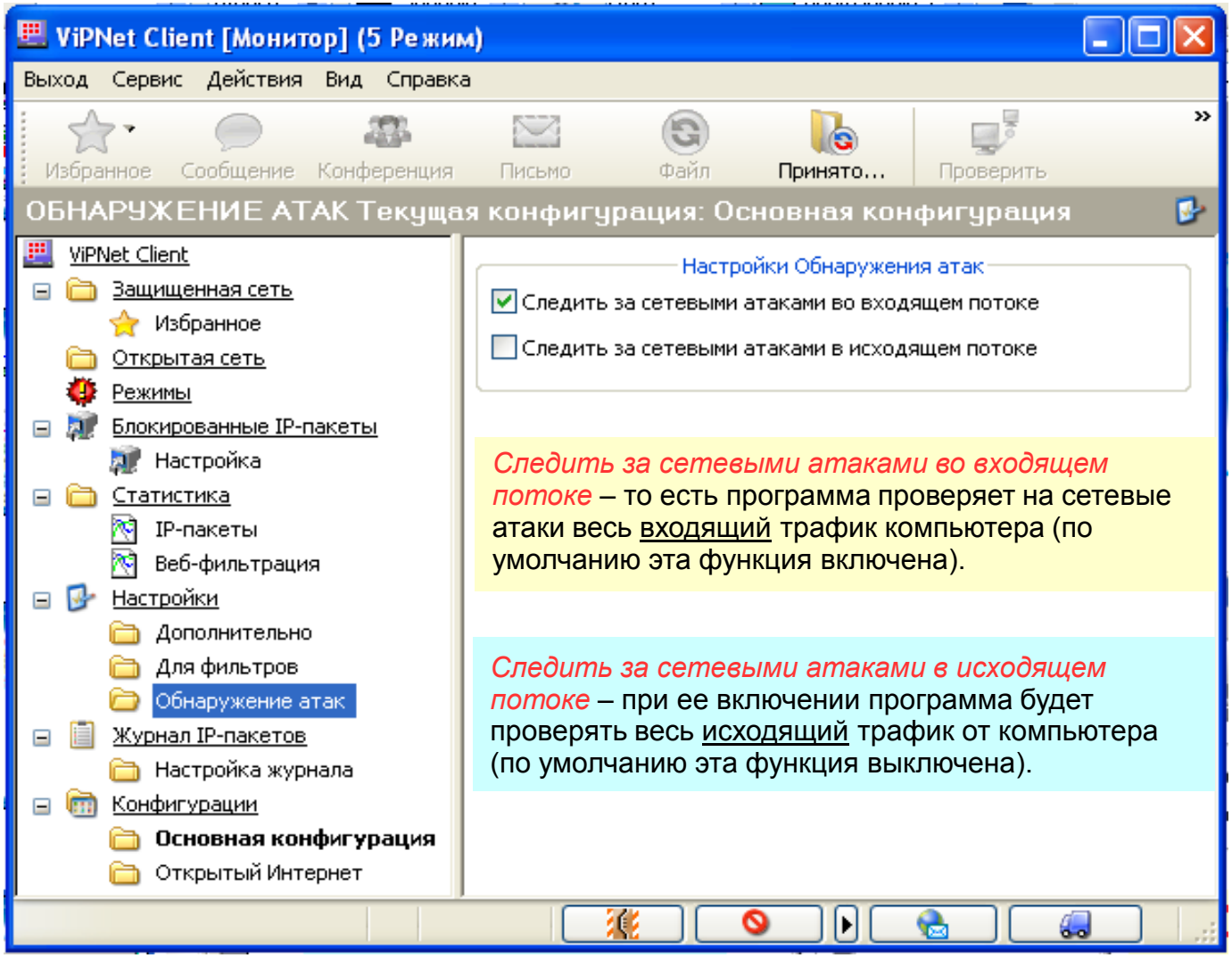
Список	Приложение	Причина
Белый	C:\Program Files\InfoTeCS\ViPNet [A...	Регистрация приложен...
Белый	C:\Program Files\InfoTeCS\ViPNet [A...	Регистрация приложен...
Белый	C:\WINDOWS\system32\ping.exe	Помещен пользователем
Белый	C:\WINDOWS\system32\svchost.exe	Помещен пользователем

Список	Приложение	Причина
Белый	C:\Program Files\InfoTeCS\ViPNet [A...	Регистрация приложен...
Белый	C:\Program Files\InfoTeCS\ViPNet [A...	Регистрация приложен...
Черный	C:\WINDOWS\system32\ping.exe	Помещен пользователем
Белый	C:\WINDOWS\system32\svchost.exe	Помещен пользователем

Intrusion Detection Systems - IDS

Система обнаружения атак (IDS) работает на сетевом уровне стека TCP/IP.

- Обнаруживает и блокирует сетевые пакеты до обработки их стеком TCP/IP и этим защищает стек от атак на него самого (такие атаки, как WinNuke)
- Блокирует на ранней стадии атаки, направленные на перезагрузку ОС, приводящие к отказу от обслуживания (например, jolt2 (CAN-2000-0305))
- В случае установки IDS на шлюз, контролирует сразу все компьютеры, находящиеся за этим шлюзом.



Следить за сетевыми атаками во входящем потоке – то есть программа проверяет на сетевые атаки весь входящий трафик компьютера (по умолчанию эта функция включена).

Следить за сетевыми атаками в исходящем потоке – при ее включении программа будет проверять весь исходящий трафик от компьютера (по умолчанию эта функция выключена).

Администратор Сетевого Узла

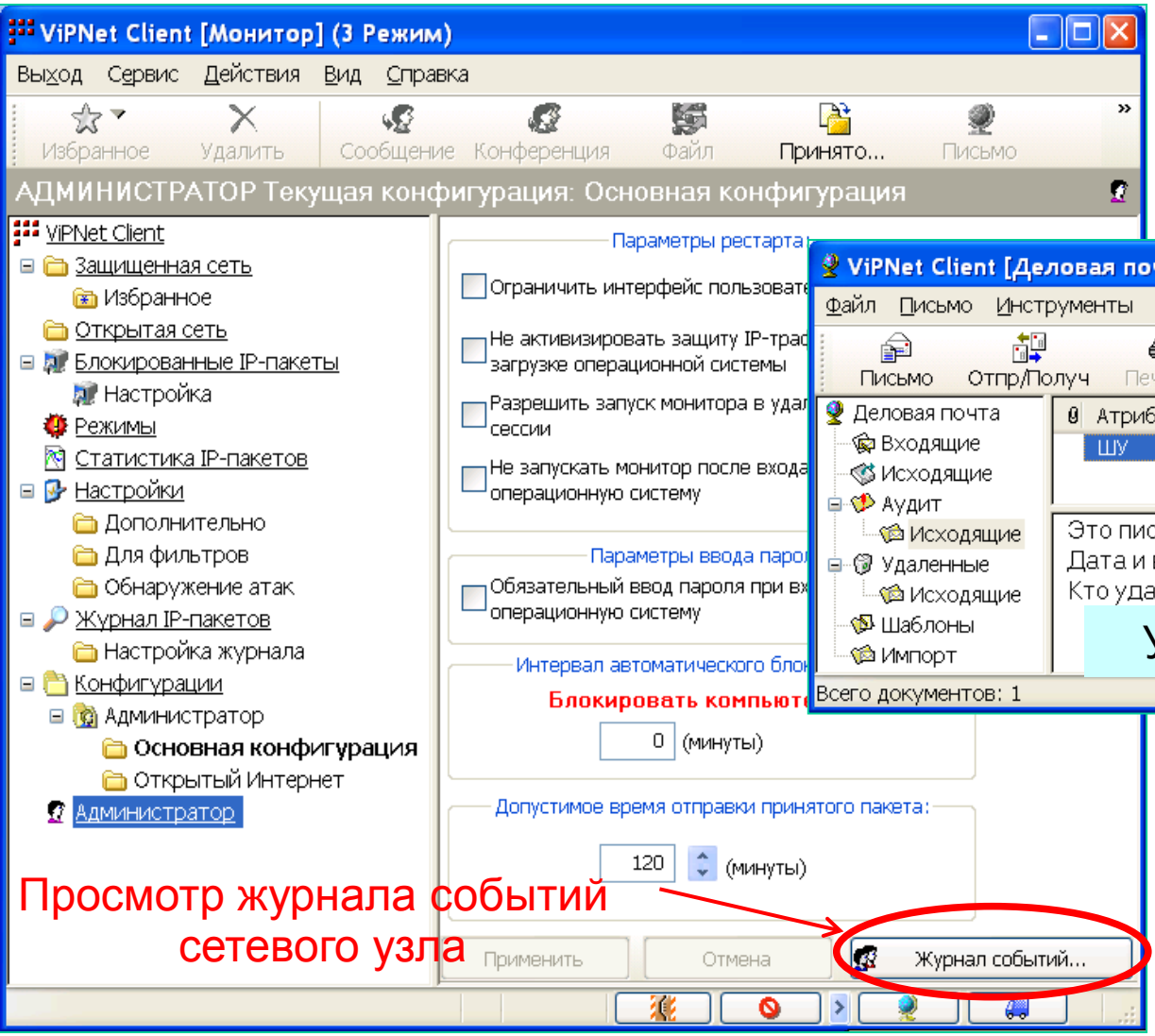
Администратор СУ – это пользователь системы защиты ViPNet на данном СУ, **обладающий полным доступом к самой системе защиты**. Полный доступ означает, что Администратор СУ **может изменять настройки системы защиты** (максимальные полномочия) и использовать дополнительные (специальные) полномочия.

Пароль Администратора СУ – пароль, с помощью которого рядовой пользователь системы, зарегистрированный на данном СУ (какими бы правами и полномочиями он не обладал) может получить **полный доступ к системе защиты.**

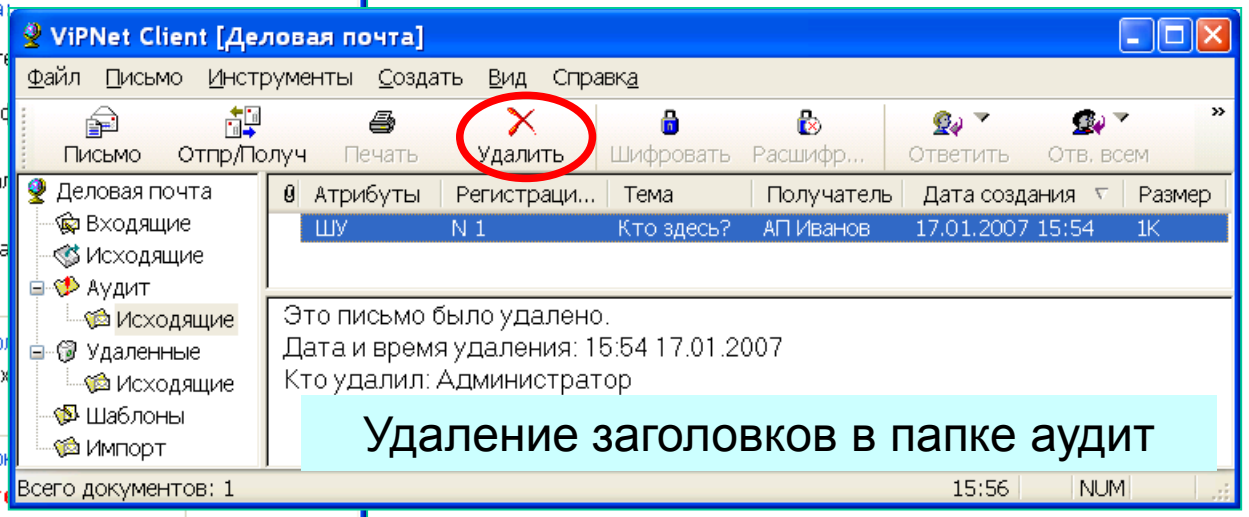
Права Администратора СУ могут быть получены как для Монитора, так и для Деловой Почты:

!! После завершения работы с правами Администратора СУ необходимо вернуть права рядового пользователя !!

Возможности Администратора Сетевого Узла



Права администратора сетевого узла дают ряд дополнительных функций в программах Монитор и Деловая почта.



Удаление заголовков в папке аудит

Защита трафика при помощи асимметричных ключей

Первоначальная ключевая структура защищенной сети ViPNet формируется в УКЦ и состоит из матрицы симметричных ключей шифрования.

Каждому пользователю системы ViPNet Администратор выдает дистрибутив, включающий в себя ключевую информацию для входа в защищенную сеть. Соответственно, Администратор VPN имеет полный доступ к ключевой информации пользователя и может читать деловую переписку пользователя (при использовании шифрования в Деловой Почте).

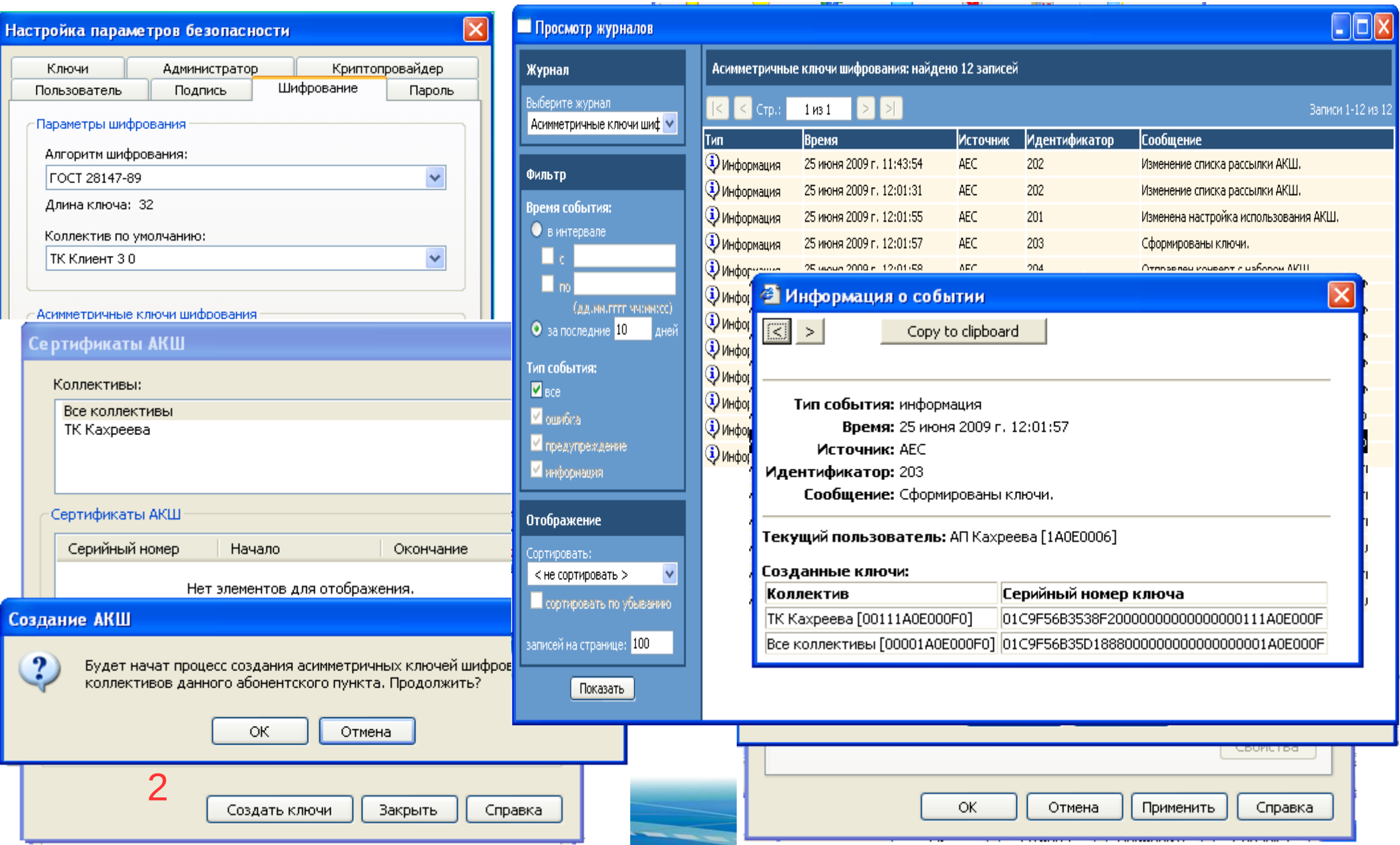
Для сохранения конфиденциальности своей переписки пользователь в Деловой Почте может использовать асимметричные ключи шифрования (по одной паре ключей для связи с каждым партнером).

Для этого необходимо указать системе защиты своего АП, что с данным конкретным пользователем будут использоваться асимметричная система шифрования.

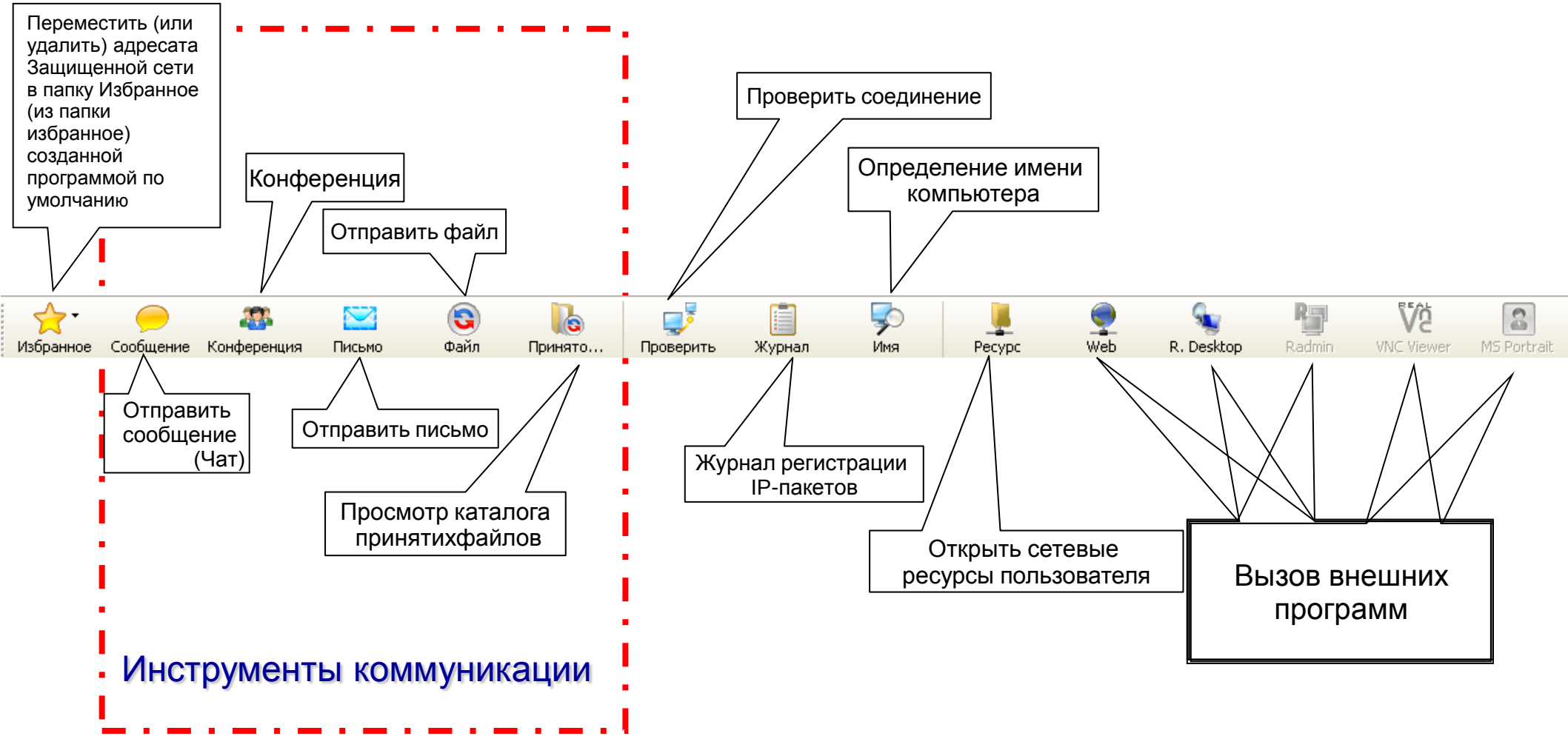
Установка режима работы с асимметричными ключами шифрования (АКШ) производится в меню *Сервис → Настройка параметров безопасности*, закладка *Шифрование*.

Администратор VPN и **Координатор**
не могут использовать асимметричные ключи шифрования !

Защита трафика при помощи асимметричных ключей



Назначение кнопок на Панели приложений



Чат

Отправить сообщение

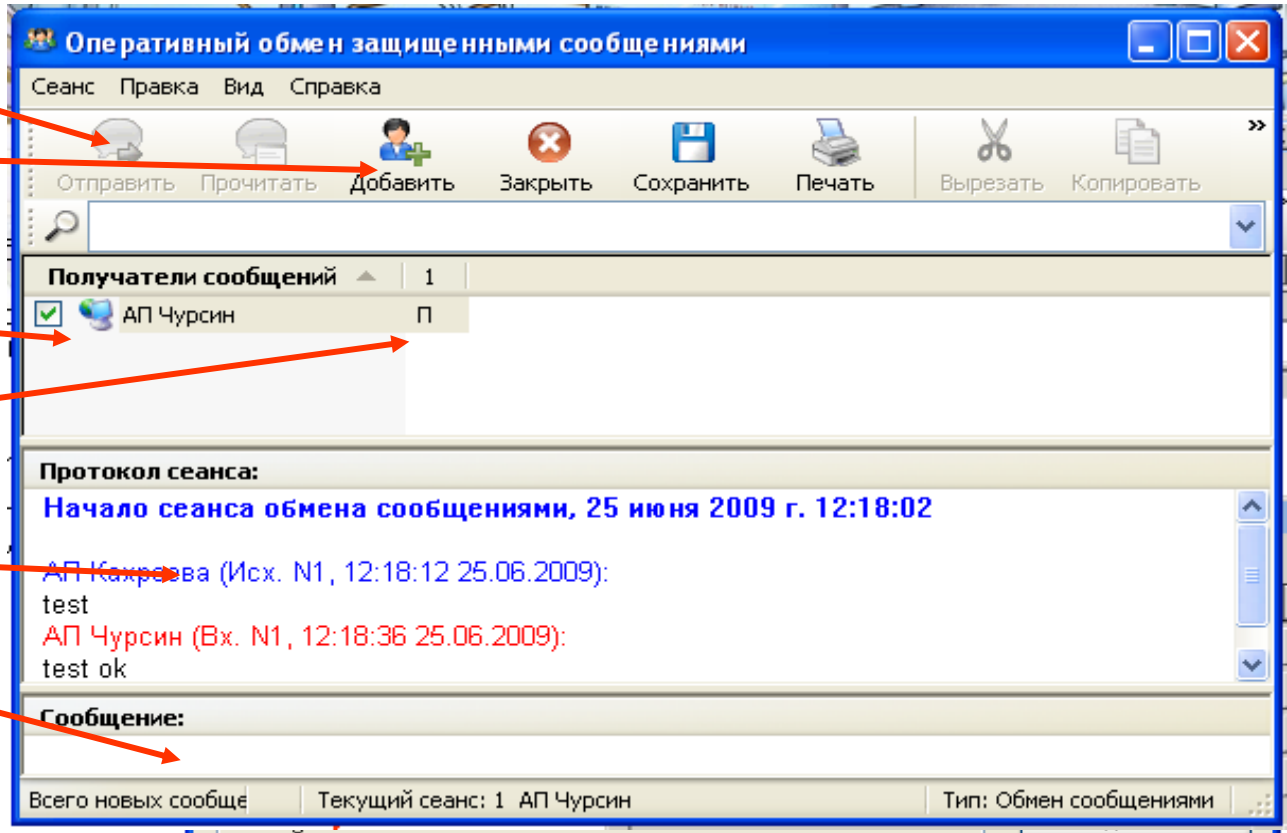
Здесь можно добавить пользователей к чату или организовать конференцию.

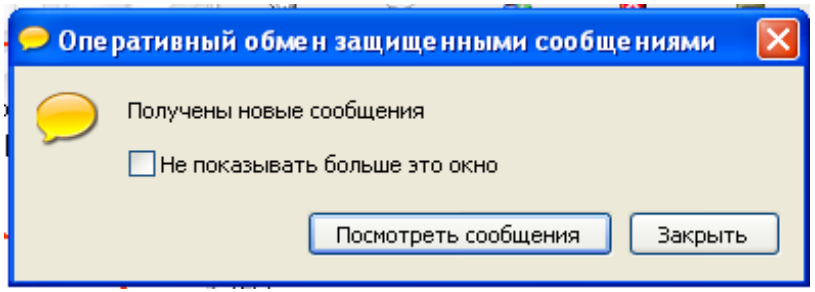
Список участников чата

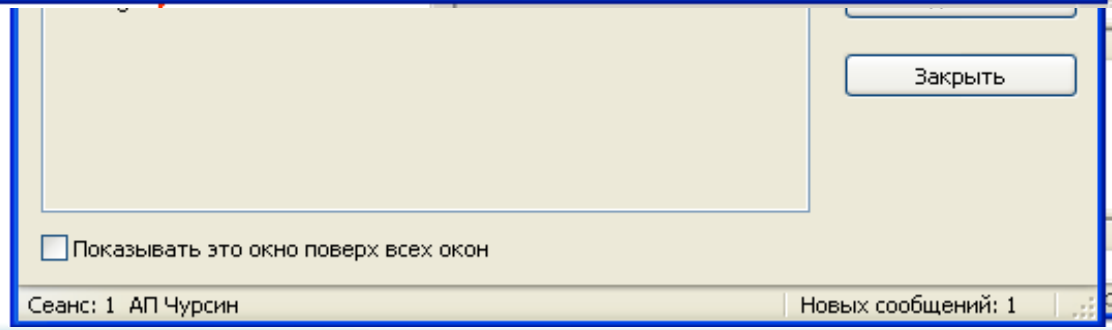
Статус сообщения: О=Отправлено, Д=Доставлено, Ч=прочитано П=Печатает ответ

Все сообщения текущей сессии

Область для написания сообщений

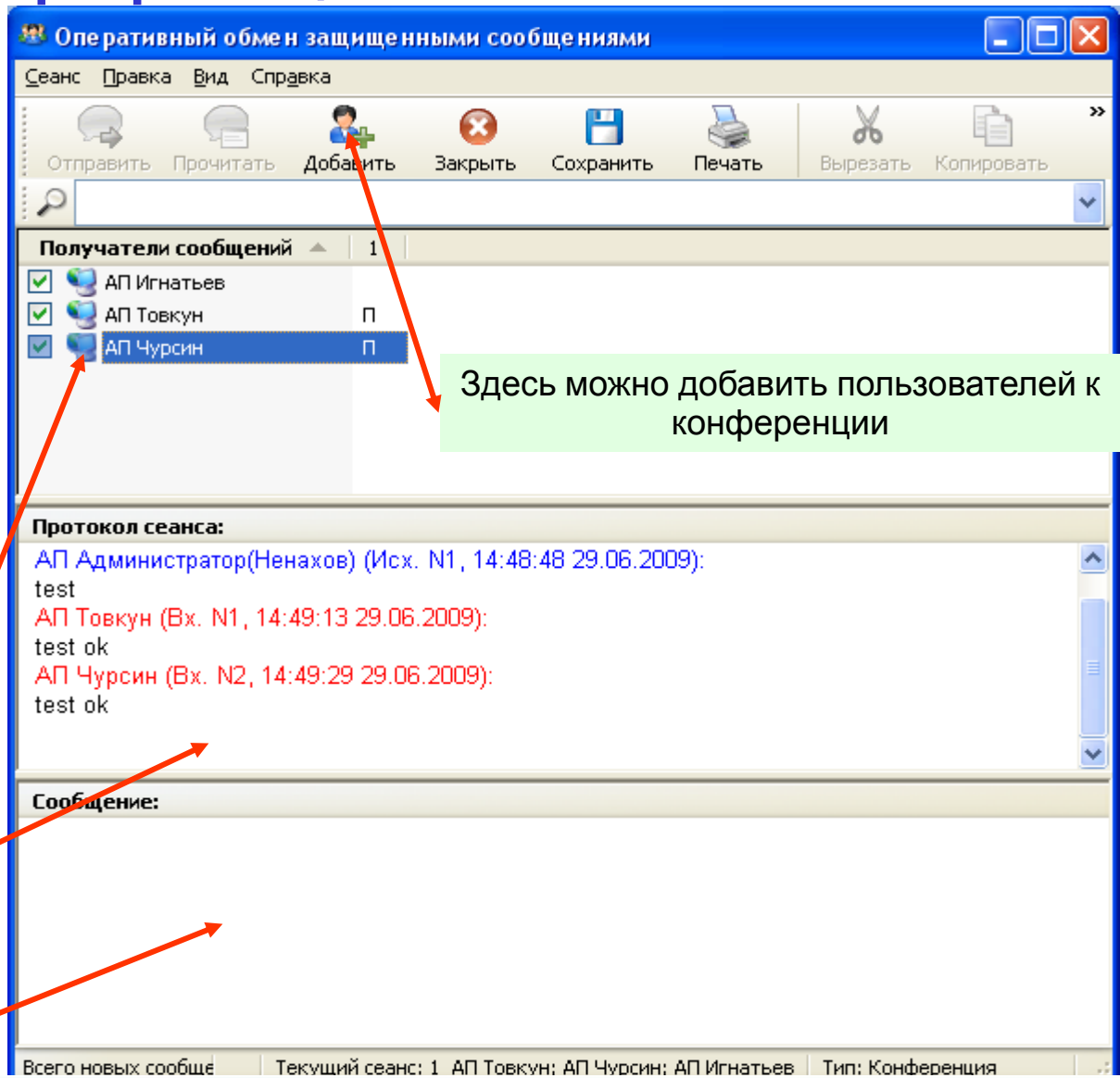






Конференция

Инициируется в окне **Защищенная сеть** по команде главного (или контекстного) меню **Действия -> Конференция**… Инициатор сеанса конференции может рассылать одно и то же сообщение нескольким пользователям ViPNet, а затем получать ответы от всех этих пользователей. При этом все пользователи (с которыми организована конференция) получают ответы друг друга, т.е. все участники сеанса конференции видят сообщения друг друга. В процессе сеанса добавлять других пользователей, выключать и включать существующих пользователей может только инициатор сеанса конференции.



Здесь можно добавить пользователей к конференции

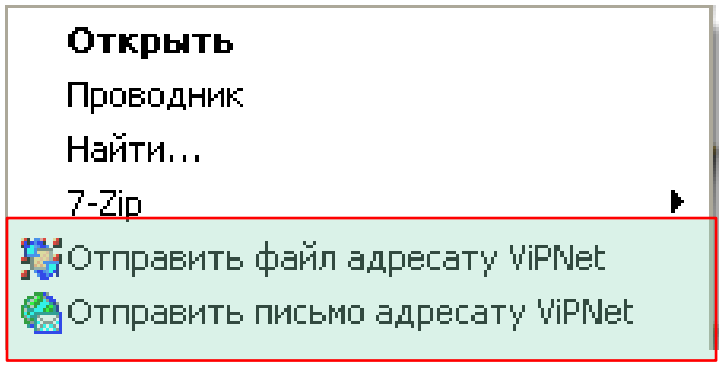
Список участников чата

Все сообщения текущей сессии

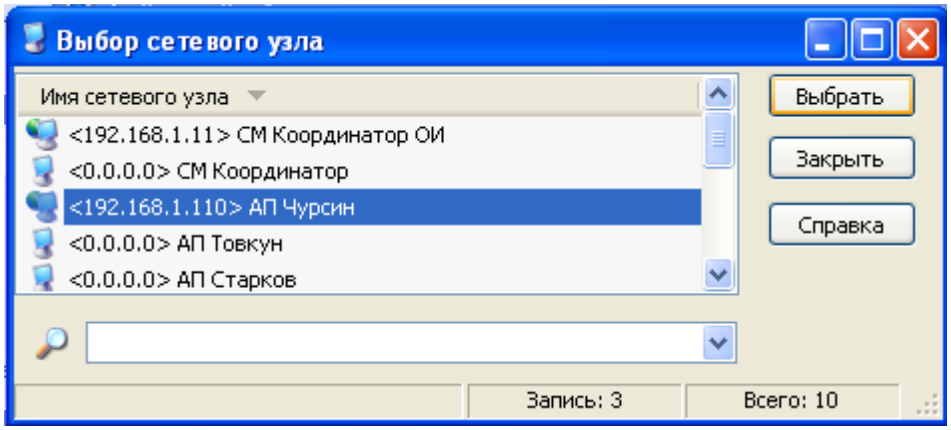
Область для написания сообщений

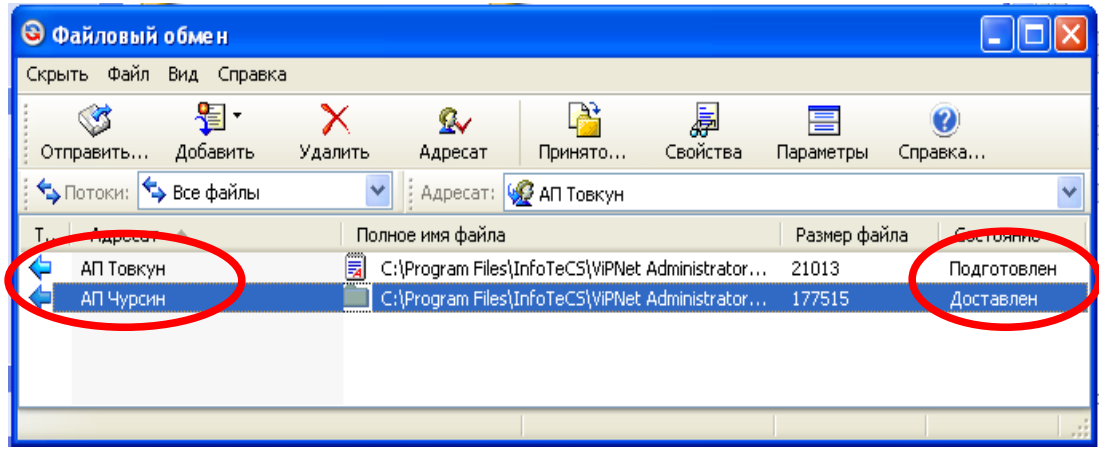
Инструменты защищенной коммуникации

Файловый обмен и Деловую почту можно вызвать из контекстного меню для любого файла и документа, что максимально облегчает их посылку в рамках VPN-сети.



В окне файлового обмена ViPNet-пользователь может определить получателей, организовать полученные файлы и проверить статус посланных файлов





infotecs®

Деловая почта

Комплекс программ для автоматизации работы с документами

Функциональные возможности Деловой почты

- Защищенный документооборот;
- Защищенный автопроцессинг;
- Архивация документов;
- Шифрование;
- Электронная цифровая подпись;
- Внешние программы;
- Адресная книга.

Защищенный документооборот

Закрытая почтовая система **для работы с корпоративными документами**

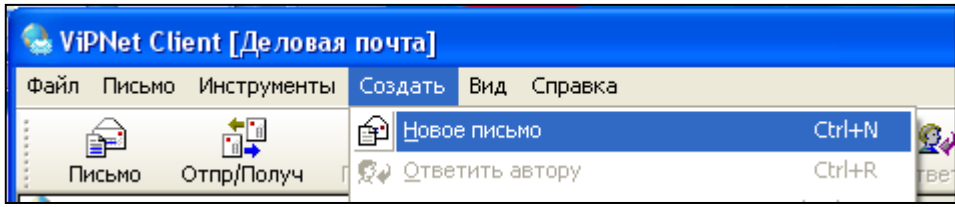
- Заголовок;
- Текст письма;
- Вложения;
- Список получателей;
- Атрибуты.

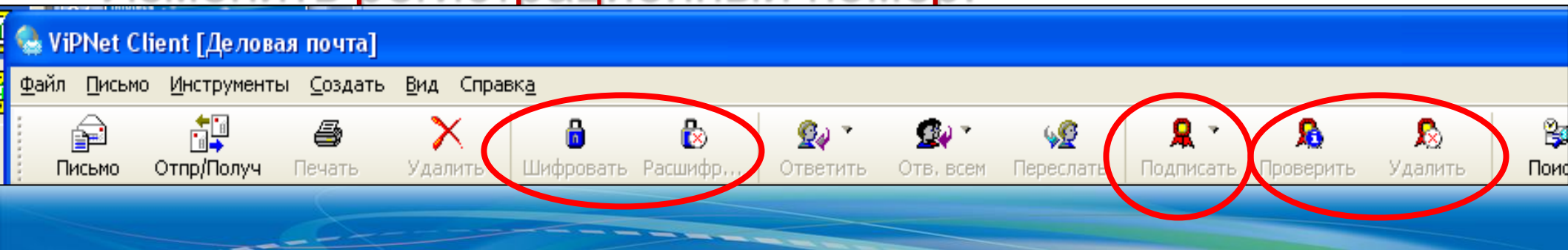
Шифрование в Деловой почте

- Шифрование (симметричное) осуществляется в соответствии с алгоритмом ГОСТ 28147-89
- Длина симметричного ключа шифрования – 256 бит
- Операции шифрования и расшифрования выполняются с письмом и его вложениями
- Документы хранятся на диске в зашифрованном виде

Действия с документами

- Создать новый документ;
- Добавить вложение к письму;
- Подписать текст / вложения документа;
- Проверить / Удалить подпись;
- Зашифровать текст / вложения документа;
- Расшифровать текст / вложения документа;
- Послать / получить / переслать документ;
- Ответить адресату;
- Проконтролировать доставку документа;
- Изменить регистрационный номер.





Преимущества Защищенного документооборота

- Возможность шифрования и подписания документа;
- Регистрация действий с письмом;
- Статистика прохождения письма (атрибуты)
- Иерархическая система хранения писем;
- Автоматическая архивация;
- Сквозная нумерация писем.

Автопроцессинг

Система автоматической обработки
- отправляемых файлов и
- входящих писем

в соответствии с правилами, заданными пользователем

- ✓ Автопроцессинг входящих писем;
- ✓ Автопроцессинг файлов.

Автопроцессинг файлов

Предназначен **для автоматической пересылки файлов по правилам, заданным пользователем** системы

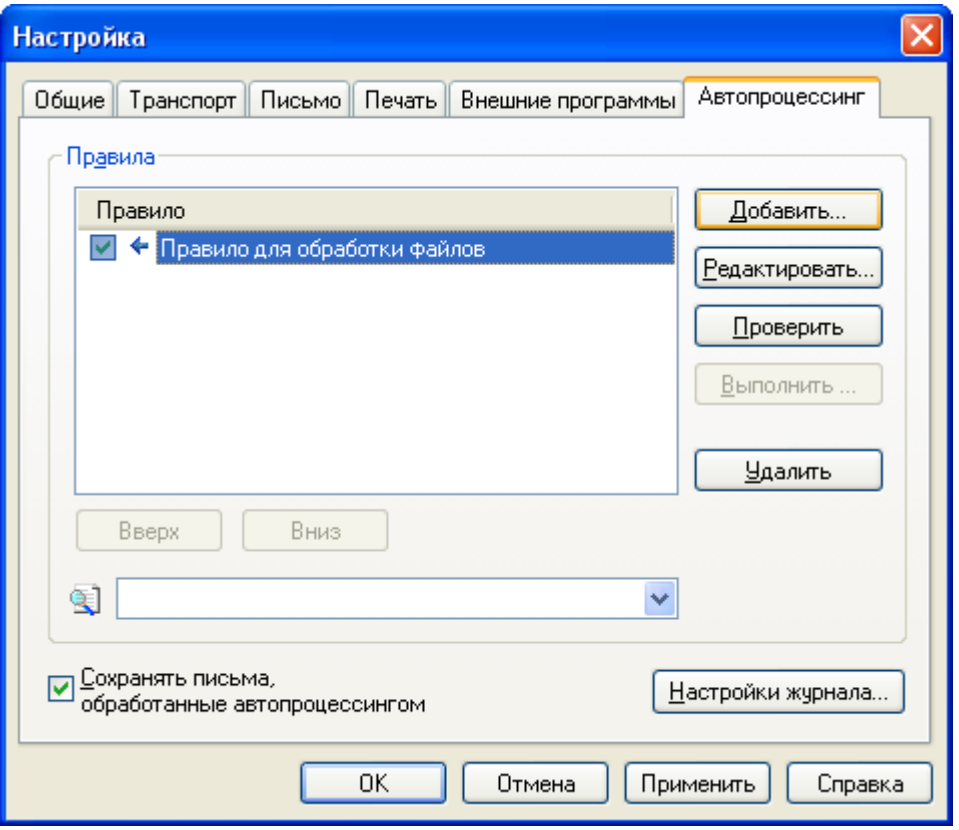
Параметры правил для обработки файлов:

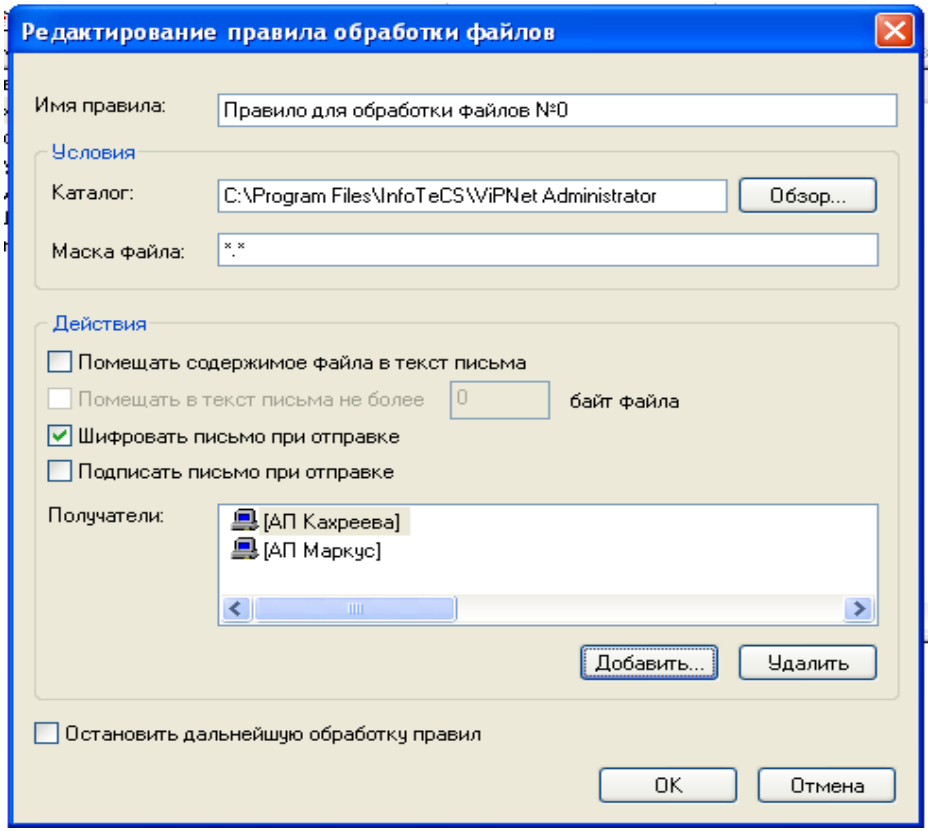
- Получатели файлов;
- Каталог для файлов;
- Маска файлов;
- Автоматическое шифрование;
- Автоматическая цифровая подпись.

Автопроцессинг файлов

Редактирование правил автопроцессинга в Деловой почте находится

Инструменты → Настройка → Автопроцессинг





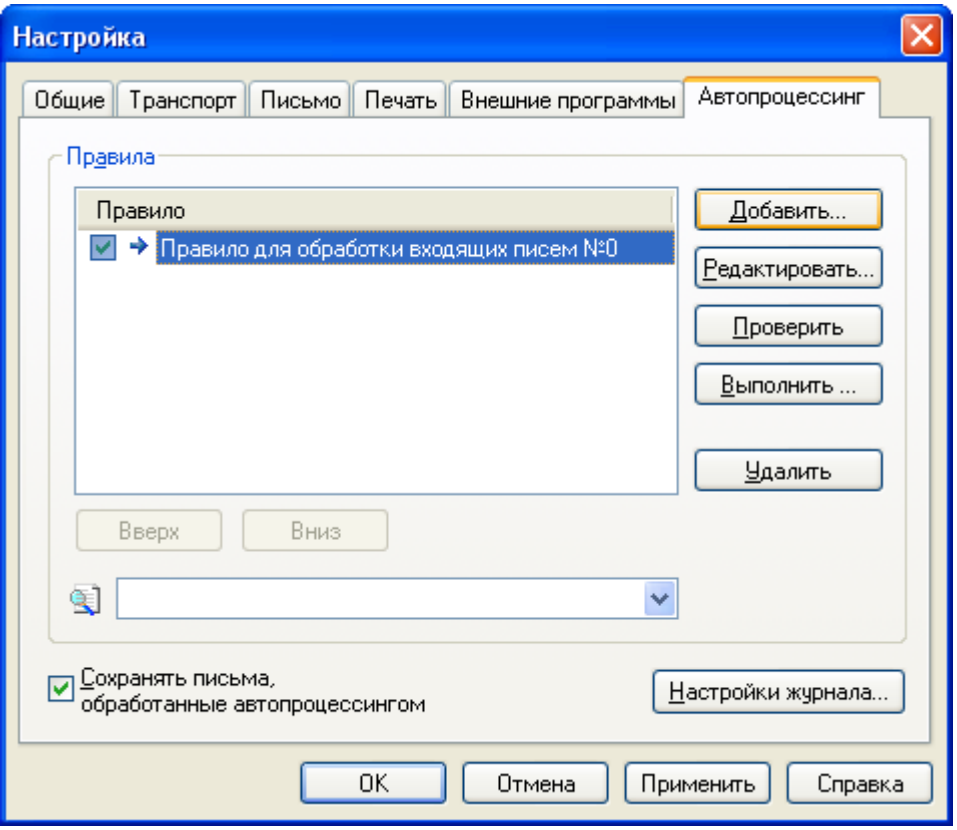
Автопроцессинг входящих писем

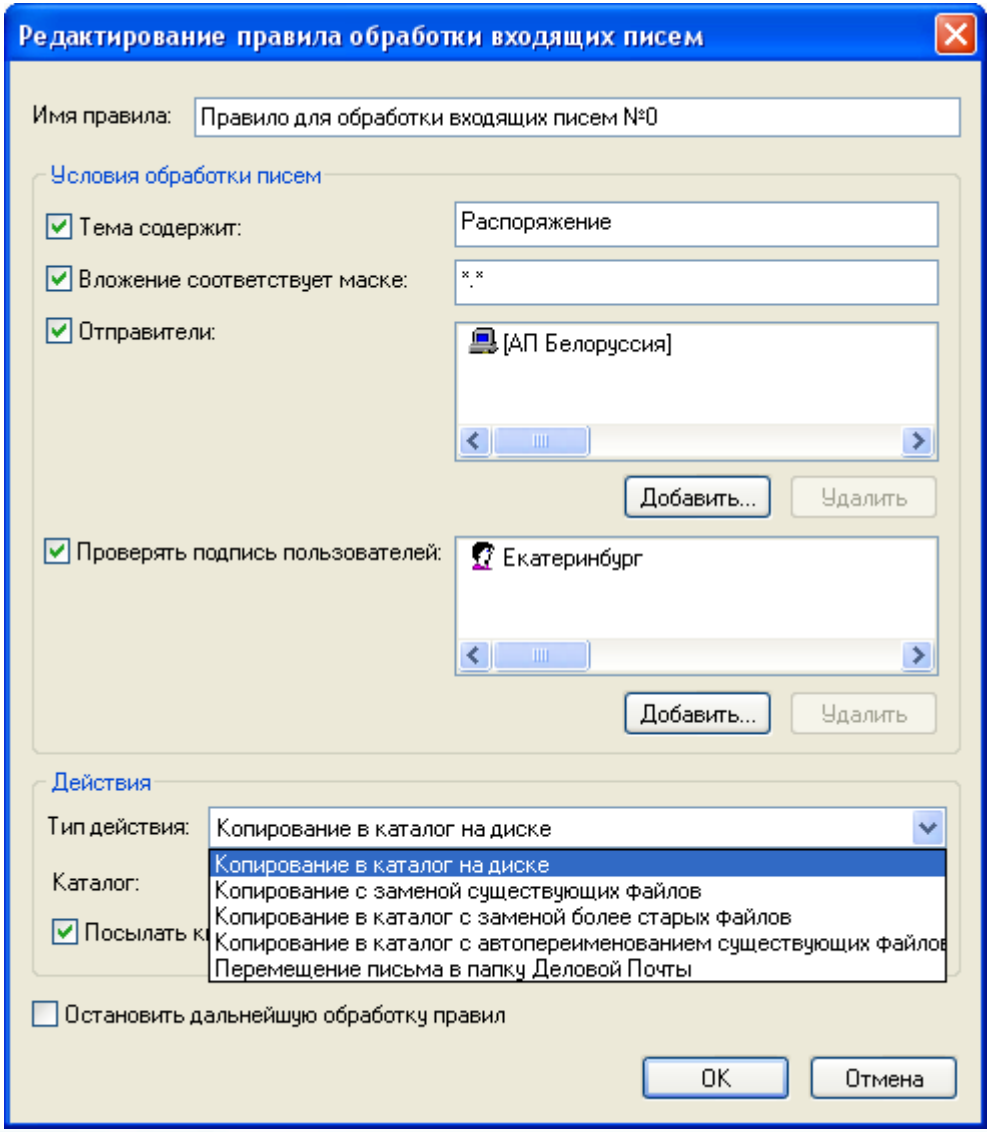
Предназначен для автоматизации действий с входящими письмами по правилам, заданным пользователем

Параметры правил для обработки писем:

- Отправитель письма
- Содержание темы письма
- Соответствие вложения маске
- Проверка подписи письма
- Посылка квитанции о доставке
- Действия с письмом

Автопроцессинг входящих писем





Автопроцессинг входящих писем

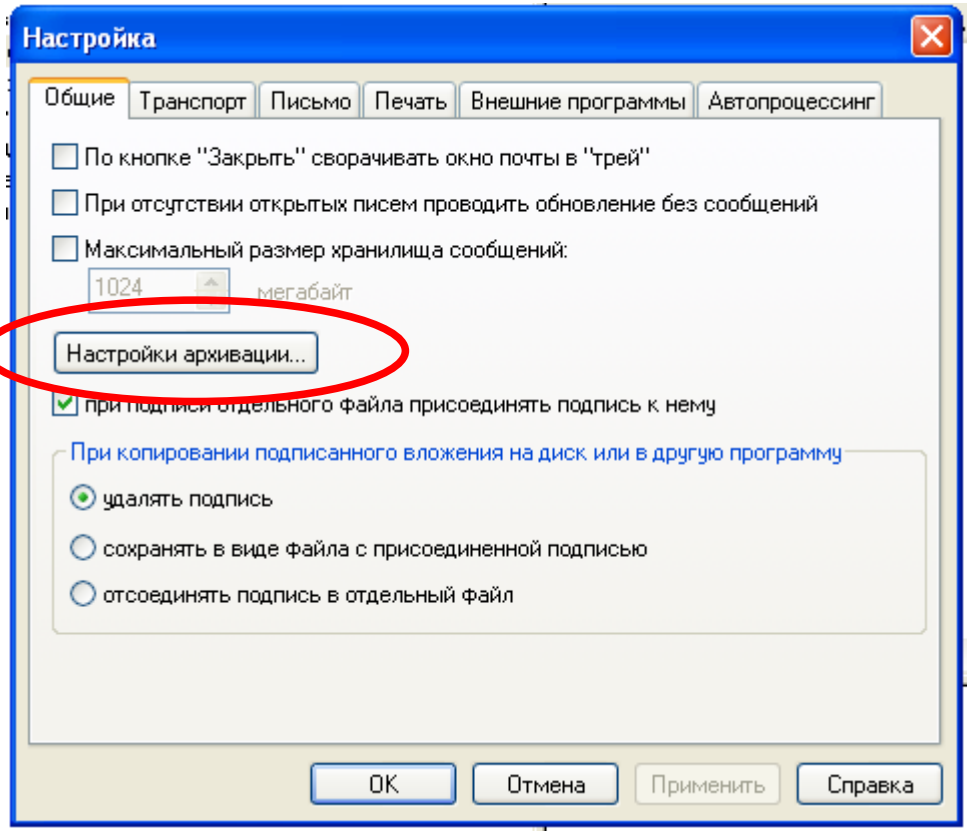
Действия с письмом

- Копирование письма в каталог на диске;
- Копирование письма с заменой существующих файлов;
- Копирование письма в каталог с заменой старых файлов;
- Копирование в каталог с автопереименованием существующих файлов;
- Перемещение письма в папку деловой почты.

Автоматическая архивация

Изменение настроек автоматической архивации производится в

Инструменты → настройка → общие



Предназначена для автоматизации создания архива папок деловой почты по правилам, заданным пользователем системы.

Параметры правил для архивации

- Тип архивируемых писем
- Условия для начала автоматической архивации

Автоматическая архивация

Тип файлов для архивации

- Любые;
- Отправленные;
- Доставленные;
- Прочитанные;

Условия начала архивации

- Через определенные интервалы времени;
- В установленное время;
- Перед каждой операцией с письмами;
- При превышении определенного количества писем;
- При превышении заданного размера архива.

Электронная цифровая подпись в Деловой почте

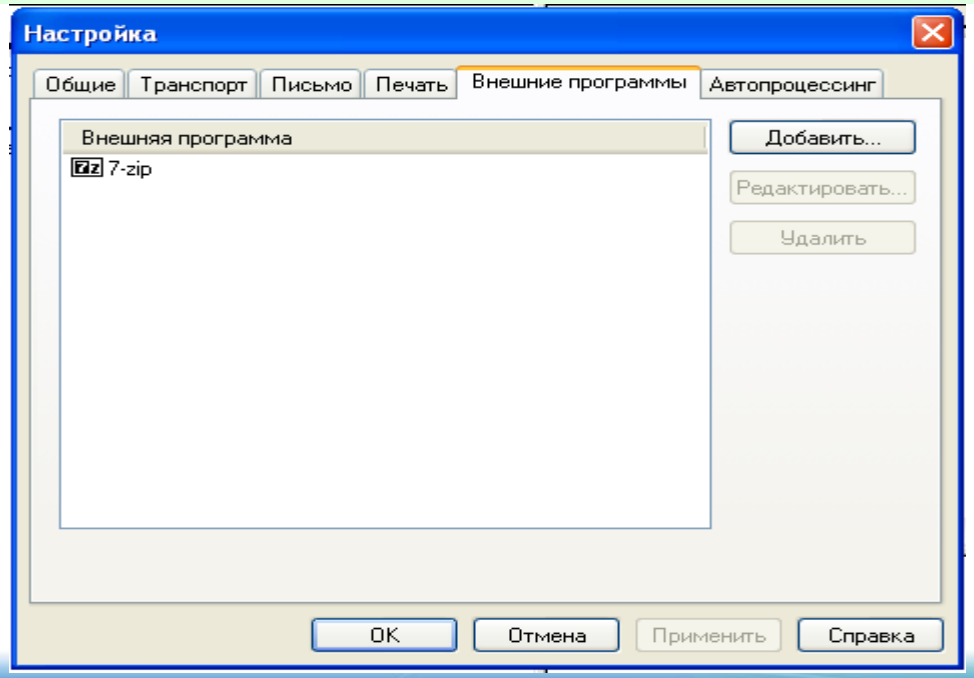
- Подпись осуществляется в соответствии с алгоритмом ГОСТ Р 34.10-2001
- Длина открытого ключа ЭЦП – 512 бит
- Действия с подписью: подписать, проверить подпись, удалить подпись
- Подпись, проверка и удаление подписи выполняются для письма и для его вложений отдельно

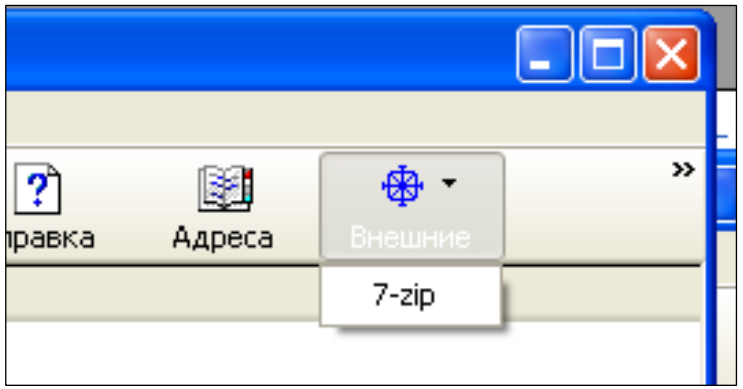
Внешние программы

Существует возможность запуска внешних программ (MS Word, MS OFFICE и т.д.) без выхода из комплекса «Деловая почта»
Эта возможность используется для удобства работы персонала

Добавление внешних программ производится в

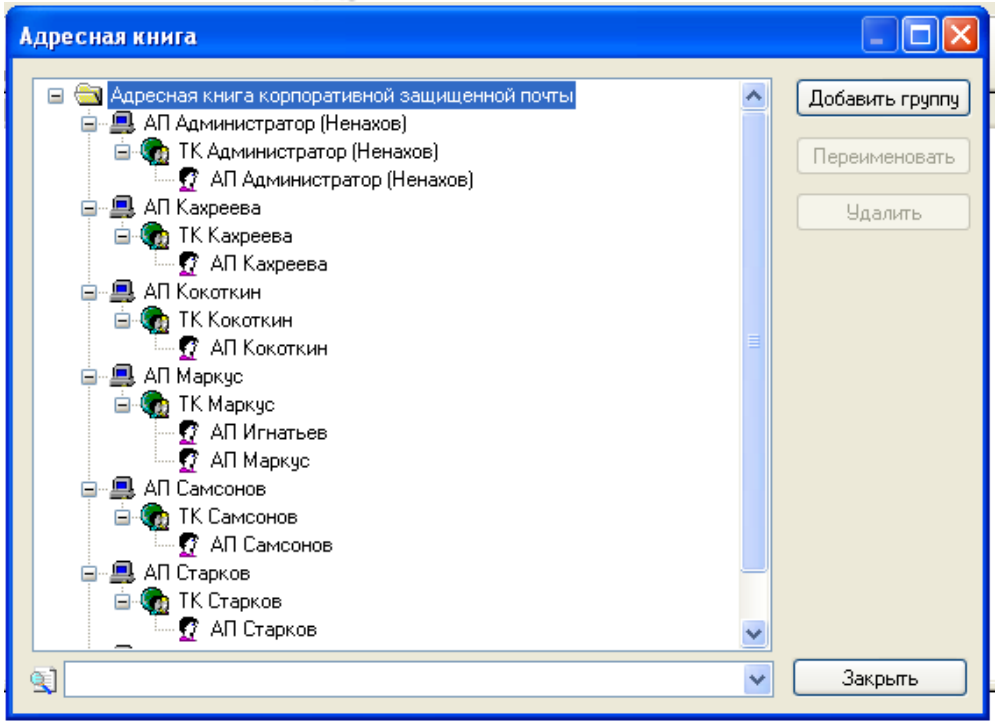
Инструменты → настройка → внешние программы - добавить





Адресная книга

Для выбора или просмотра списка адресатов «Деловой почты» используется Адресная книга



Возможности при работе с Адресной книгой:

- Трехуровневая система адресации
- Создание групп адресатов
- Поиск адресата по строке поиска

Преимущества Деловой почты

- Удобный интерфейс программы;
- Шифрование и подпись конфиденциальных документов;
- Контроль доставки и исполнения документов;
- Создание деловых архивов и работа с ними;
- Создание и удобная работа с адресной книгой;
- Запуск любых внешних программ;
- Использование любых типов программ редактирования и печати;
- Регистрация всех действий с документами с журнале;
- Невысокая цена продукта;
- Поддержка и сопровождение продукта специалистами ИнфоТеКС.

Спасибо за внимание!

ОАО “ИнфоТеКС”, Москва
(495) 737-61-92

education@infotecs.ru
www.infotecs.ru