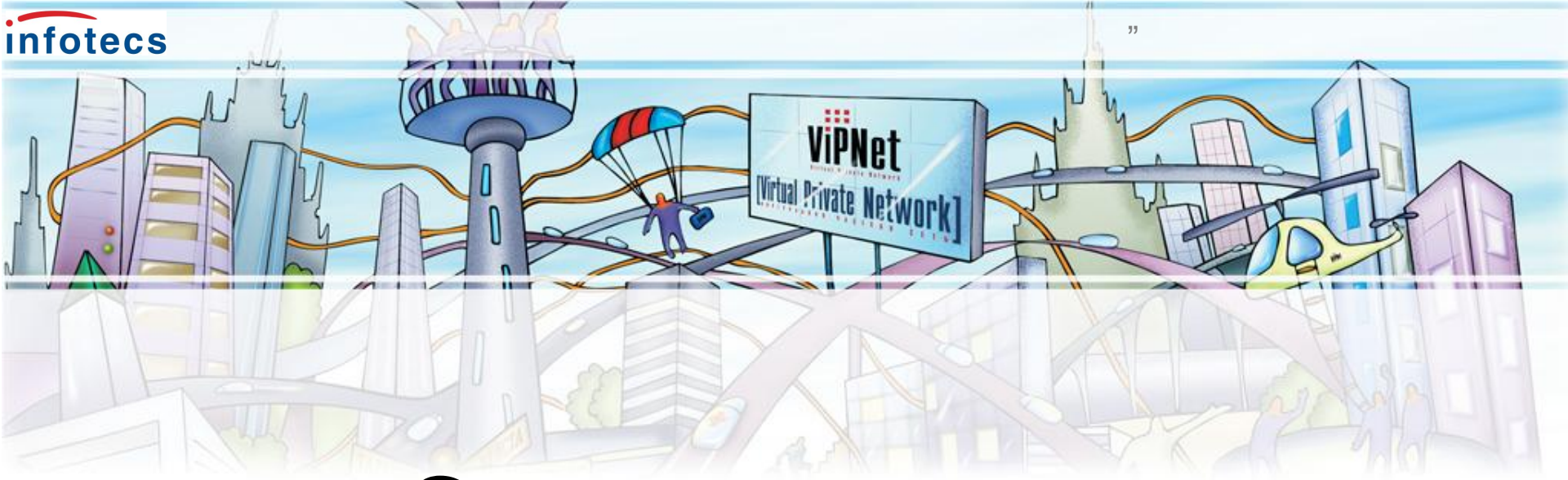
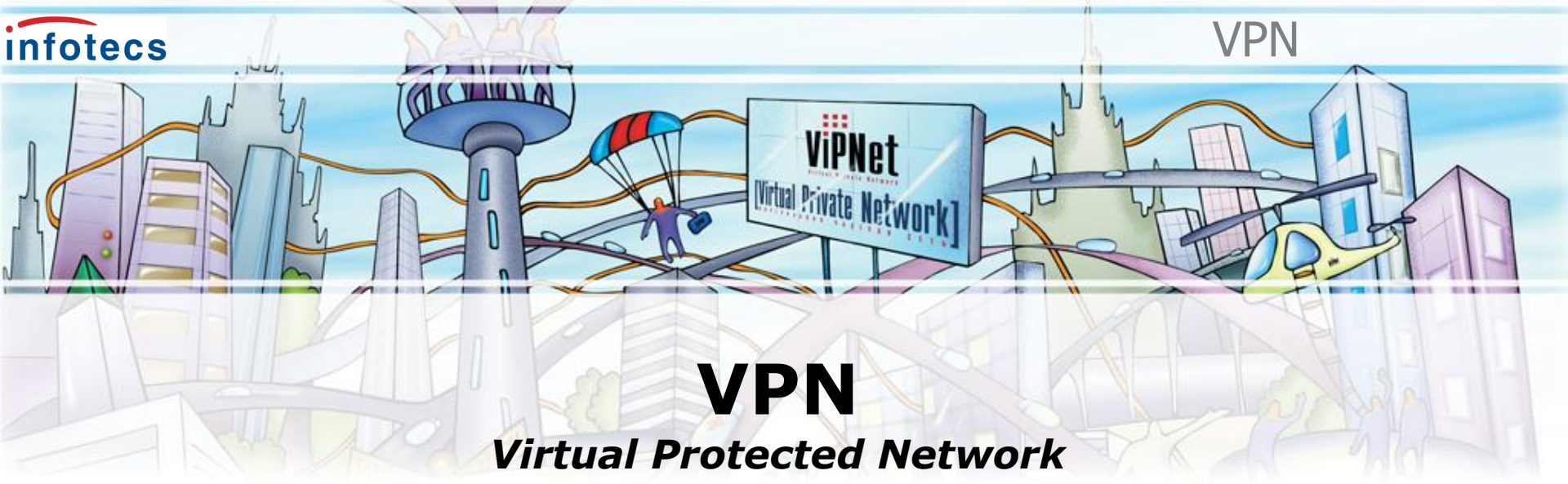


Система защиты информации ViPNet

Территориальный фонд ОМС Саратовской области

general@sartfoms.ru

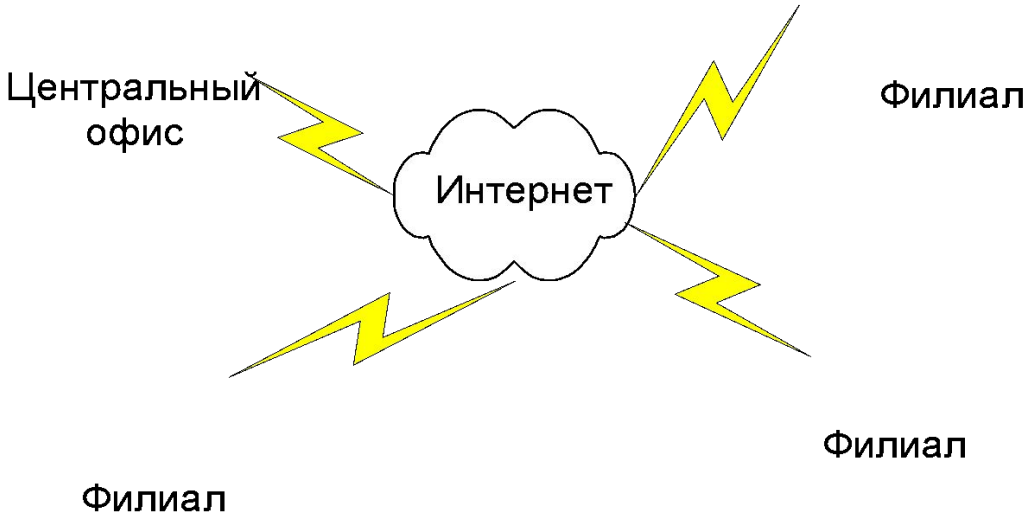


VPN

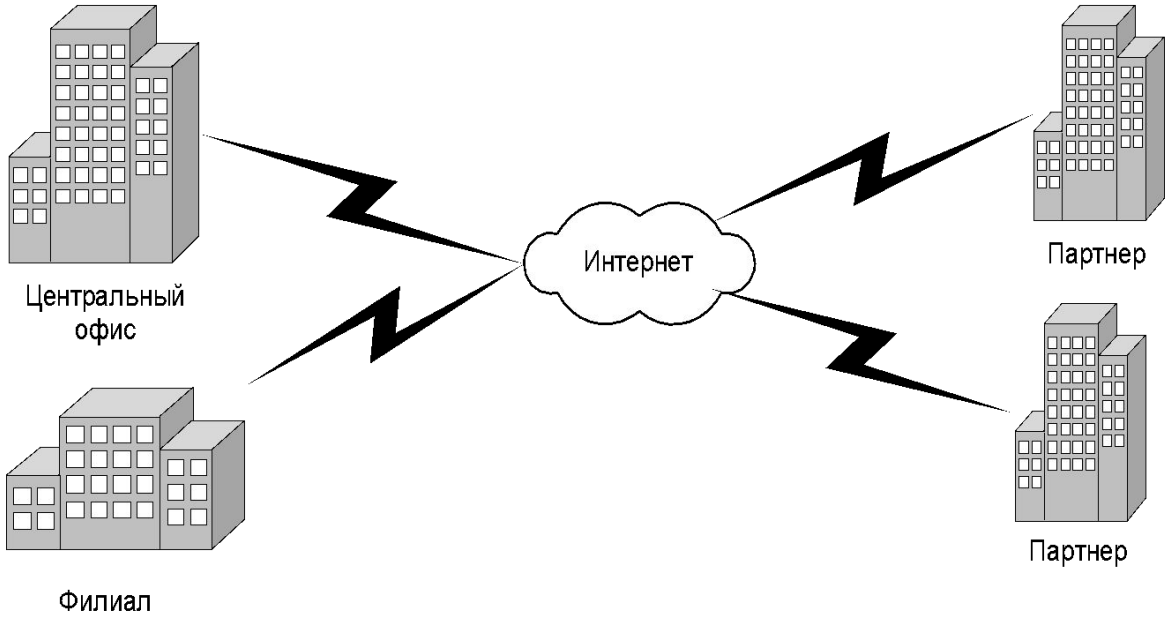
Virtual Protected Network
(Виртуальная Защищенная Сеть).

Технология ViPNet предназначена для создания целостной системы доверительных отношений и безопасного функционирования технических средств и информационных ресурсов корпоративной сети организации, взаимодействующей также и с внешними техническими средствами и информационными ресурсами.

Intranet VPN – объединяет в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.



Extranet VPN – реализует защищенное соединение с пользователями "со стороны" (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым ниже, чем к своим сотрудникам.



Лицензии ОАО Инфотекс

- Лицензии ФАПСИ на право осуществлять производство и проектирование средств защиты информации; осуществлять деятельность по техническому обслуживанию и распространению шифровальных средств;
- Лицензия Центра ФСБ по лицензированию на осуществление работ с использованием сведений, составляющих государственную тайну;
- Лицензия Государственной технической комиссии на выполнение работ (оказание услуг) по защите информации;
- Лицензия Министерства Обороны РФ на деятельность в области создания средств защиты информации

Сертификаты на ПО ViPNet?

Сертификаты Государственной технической комиссии №№545, 546:

- На программный комплекс ViPNet по классу защищенности 1В для АС;
- На Межсетевой экран ViPNet – по 3 классу защищенности для МЭ и по 3 уровню контроля отсутствия НДВ.


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ И ИНФОРМАЦИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-0471

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ И ИНФОРМАЦИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/525-0558

Сертификаты Федерального Агентства Правительственной Связи и Информации:

- На средство криптографической защиты информации «Домен-К 2.0» по классам КС1 и КС2, для защиты информации, не составляющей сведений составляющих государственной тайны;
- На персональный сетевой экран ViPNet по 4-му классу для межсетевых экранов.


ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ № 546

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ И ИНФОРМАЦИИ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/114-0470

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ № РОСС RU.0001.01БИ00

СЕРТИФИКАТ № 545

Что такое ViPNet?

ViPNet™ – программный комплекс для построения системы сетевой защиты корпоративных сетей на ОС Windows, Linux, Solaris.

Реализует:

- Формирование структуры защищенных сетей и централизованное управление конфигурацией, неограниченную масштабируемость;
- Шифрование информации на сетевом и прикладном уровнях (любой IP-трафик: видео-, аудиоконференции, файловый обмен, электронная почта);
- Разграничение доступа к информационным ресурсам (межсетевые и персональные сетевые экраны, виртуальные подсети, доверенный доступ к базам данных);
- Безопасный доступ к каналам общего пользования, включая Интернет.

ViPNet состоит из трех программных модулей

ViPNet[Клиент] — устанавливается на компьютер каждого VPN-пользователя, обеспечивает защищенное соединение по TCP/IP с другими пользователями и защиту самого компьютера от сетевых атак

ViPNet[Координатор] — VPN-сервер с интегрированным межсетевым экраном, защищенным почтовым сервером и туннельным сервером для защищенных соединений.

ViPNet[Администратор] — конфигурирование и создание VPN

ViPNet[Клиент]

Персональный сетевой экран

надежная защита рабочей станции/сервера от сетевых атак из LAN и Internet, включая такие возможности как:

- фильтрация IP-трафика по заданным параметрам (“белые” и “черные” списки по типу соединений, номерам портов и протоколов);
- безопасную работу VPN-пользователя с открытыми ресурсами (режим «невидимки»);
- обнаружение сетевых вторжений с помощью встроенной IDS;
- контроль сетевой активности приложений для обнаружения программ-«троянцев».

Шифратор TCP/IP-трафика

включает защиту (шифрование, аутентификацию) любого IP-трафика (сгенерированного приложением или операционной системой) проходящего между любыми VPN-объектами, такими как рабочие станции, серверы приложений, данных и др.

ViPNet[Координатор]

многофункциональное программное обеспечение, которое в зависимости от настроек может выполнять функции:

- VPN-сервера с набором служебных функций
- Туннелирующего сервера (защита связи типа LAN-LAN)
- Межсетевого экрана
- Сервера для безопасной работы с Internet
- Почтового сервера для работы встроенной в ViPNet[Клиент] защищенной почтовой службы

ViPNet[Администратор] состоит из двух программ:

Центр Управления Сетью(ЦУС)

Ключевой Удостоверяющий Центр (КУЦ)

Центр Управления Сетью (ЦУС)

- Определяет узлы защищенной сети, пользователей и допустимые связи между ними, создает необходимые справочники и базу данных для работы Ключевого Удостоверяющего Центра;
- Определяет политику безопасности на каждом узле и формирует список прикладных задач, которые могут быть на этом узле запущены (шифрование трафика, ЭЦП, Деловая Почта и т.д.);
- Поддерживает сервис автоматической доставки (с квитированием) до узлов сети разнообразной справочно-ключевой информации (справочников связей узлов, корневых и отозванных сертификатов, новых ключей шифрования, информации о связях с другими ViPNet-сетями и др.);
- Позволяет проводить автоматическое обновление ПО ViPNet на удаленных компьютерах;
- Поддерживает удаленный доступ к журналам событий на узлах защищенной сети.

Ключевой Удостоверяющий Центр(КУЦ)

- Ключевой Центр: формирует и обновляет все необходимые ключи (шифрования, авторизации) и пароли узлов/пользователей защищенной сети. Ключевая информация пользователя может быть сохранена на аппаратном носителе (дискета, Touch-memory, eToken, смарт-карта и т.п.);

- Удостоверяющий Центр: поддерживает все необходимые механизмы по работе с ЭЦП в формате X.509v3 для аутентификации различных сетевых объектов, включая внешних пользователей (издание секретного ключа, сертификация ЭЦП, формирование списка отозванных сертификатов, кроссертификация с другими УЦ и т.д.).

Защита при загрузке

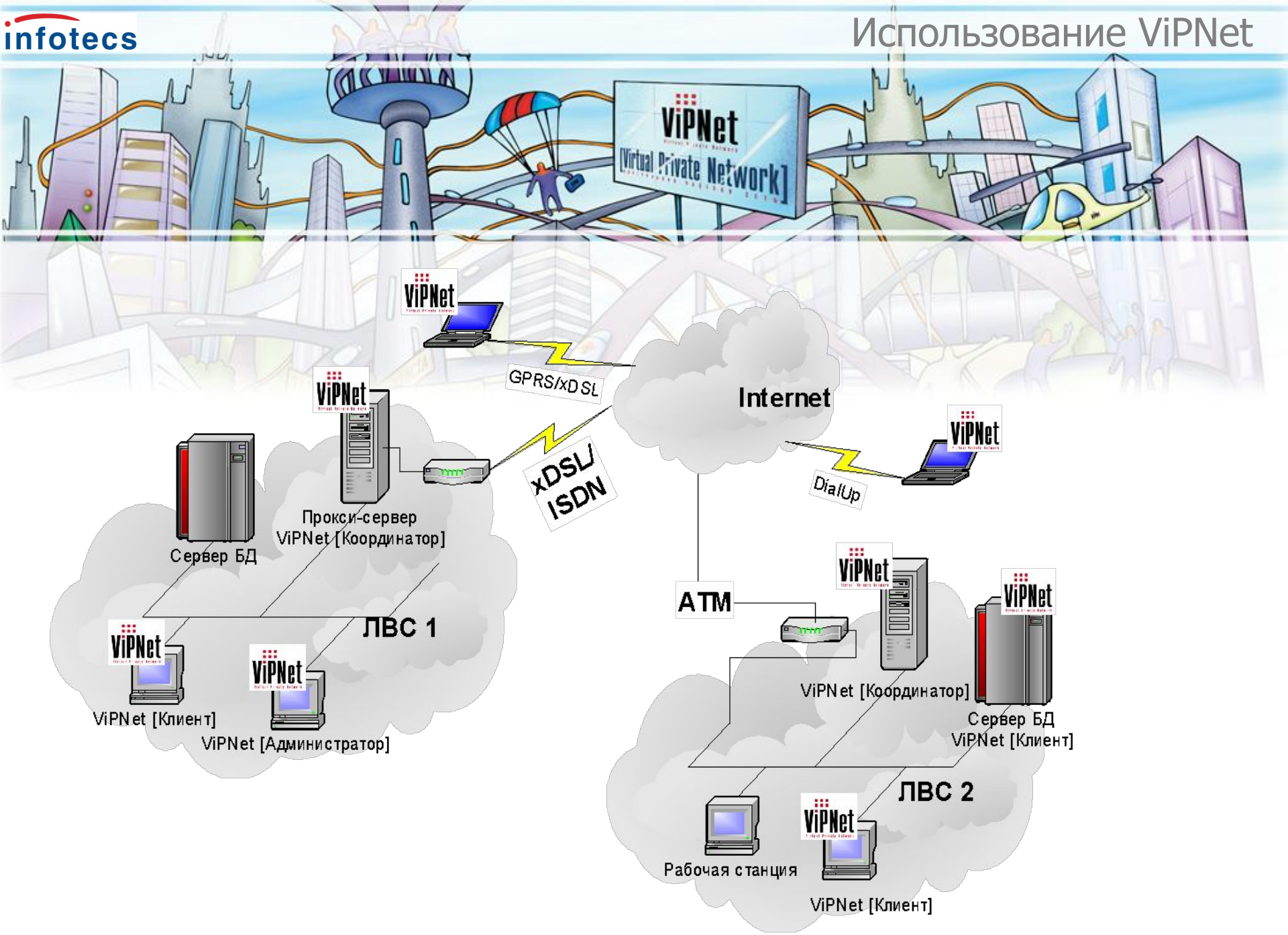
Одной из отличительных особенностей технологии ViPNet является полный контроль над сетевым трафиком во время загрузки операционной системы.

Этот контроль возможен благодаря глубокой интеграции драйвера сетевой защиты ViPNet в стек TCP/IP операционной системы.

Преимущества такого подхода очевидны:

- **во время и после загрузки становятся невозможны любые сетевые атаки, так как ViPNet выполняет функции интегрированного персонального сетевого экрана с элементами IDS**
- **авторизация при входе в операционную систему происходит после активизации драйвера ViPNet, что обеспечивает надежную защиту прикладных и системных сервисов пользователя**

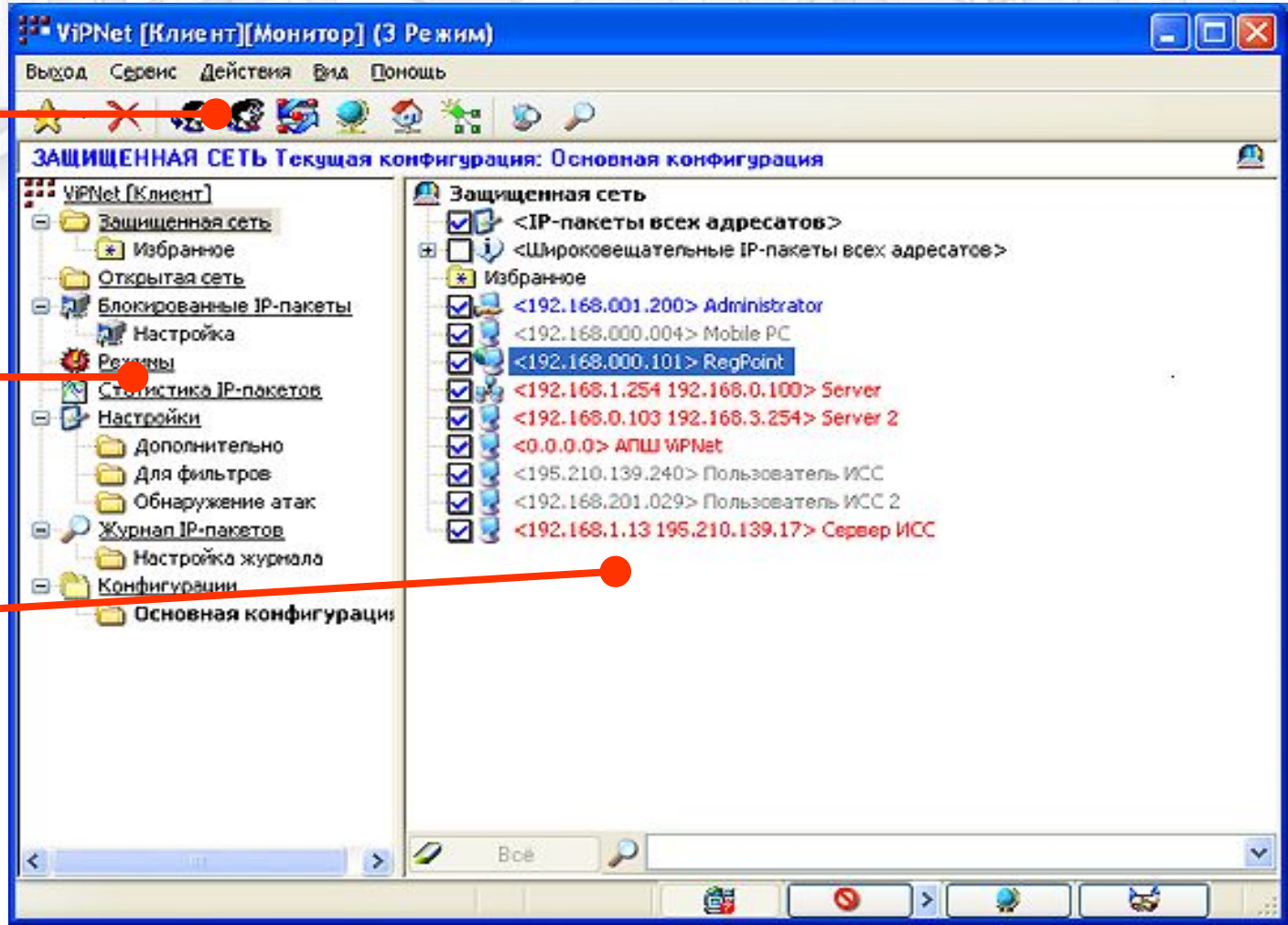
Использование ViPNet



Панель наиболее важных пользовательских приложений

Дерево настроек программы

Лист ViPNet - пользователей и состояние их соединений



Встроенный сетевой экран предлагает 5 уровней защиты.

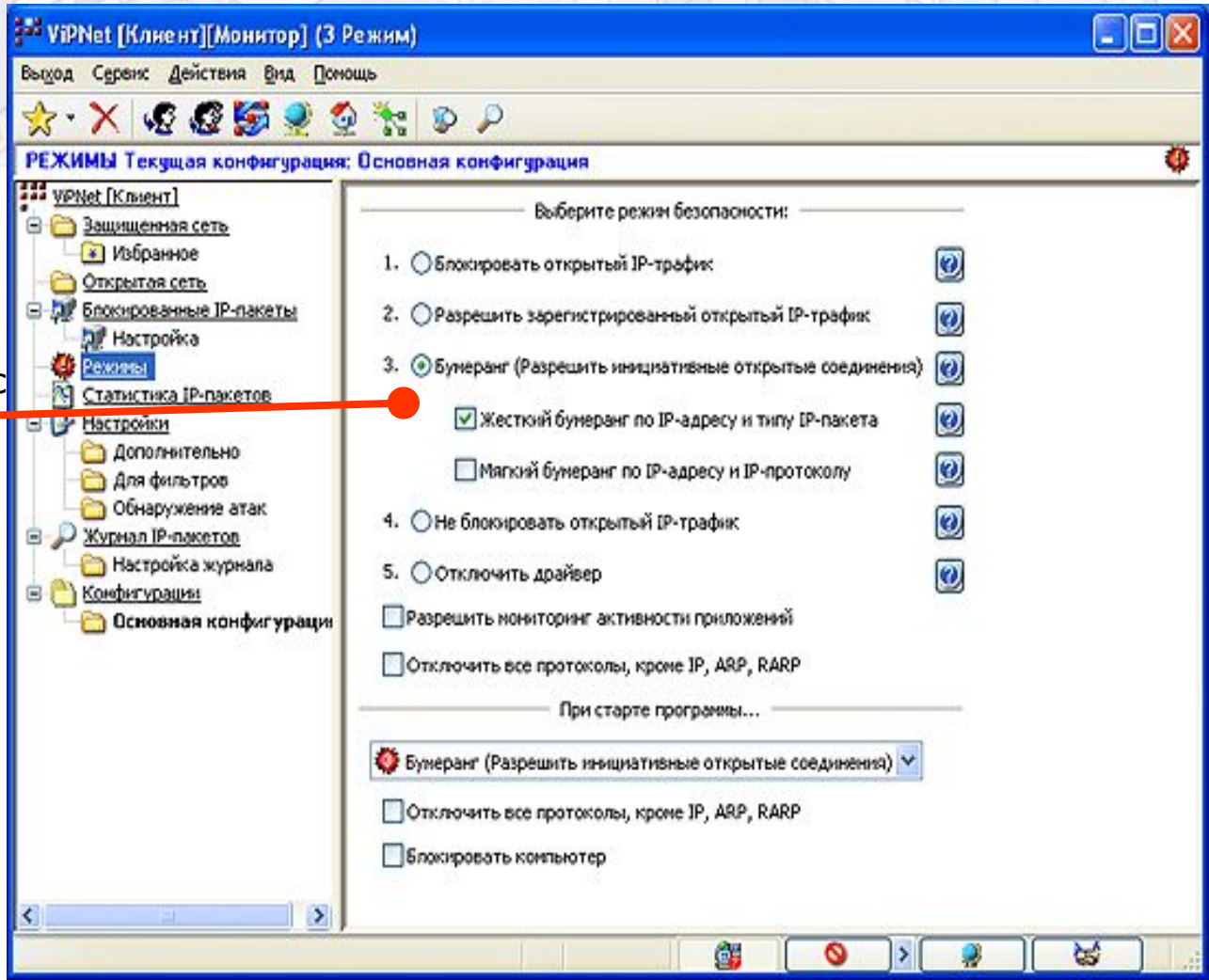
Первый – блокирует весь открытый (незашифрованный) трафик (работа только внутри VPN).

Второй – разрешает работу с зарегистрированными открытыми ресурсами.

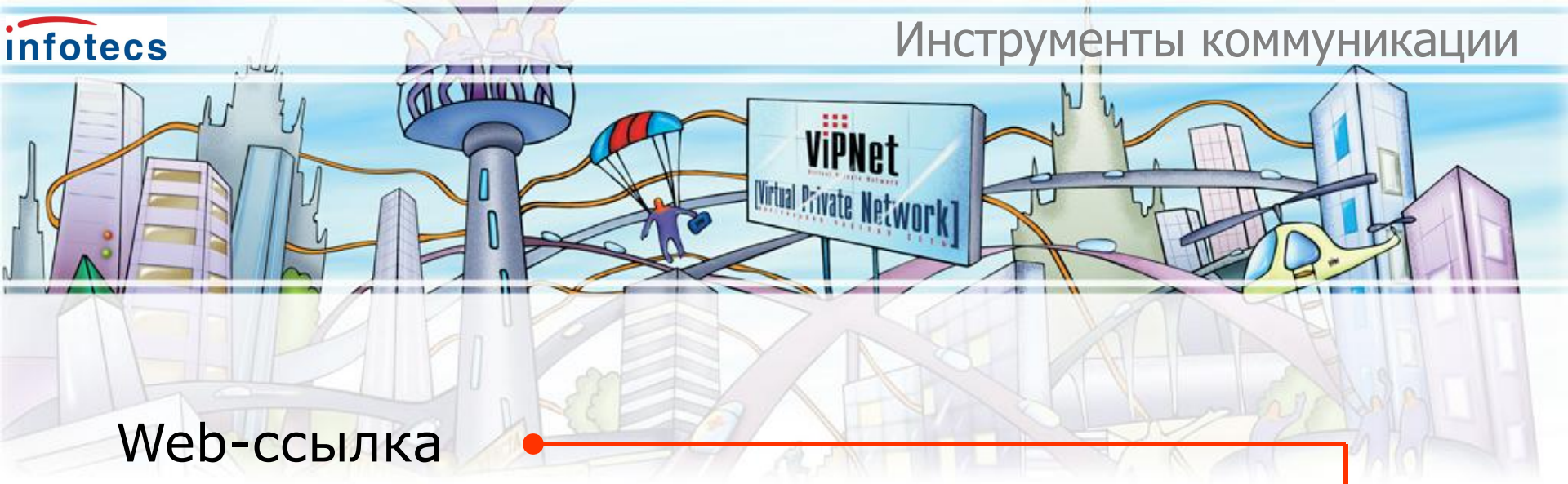
Третий – режим инициативных соединений, оптимален для работы с Интернет.

Четвертый – ничего не блокируется, но все регистрируется.

Пятый – отключение драйвера защиты ViPNet.



Инструменты коммуникации



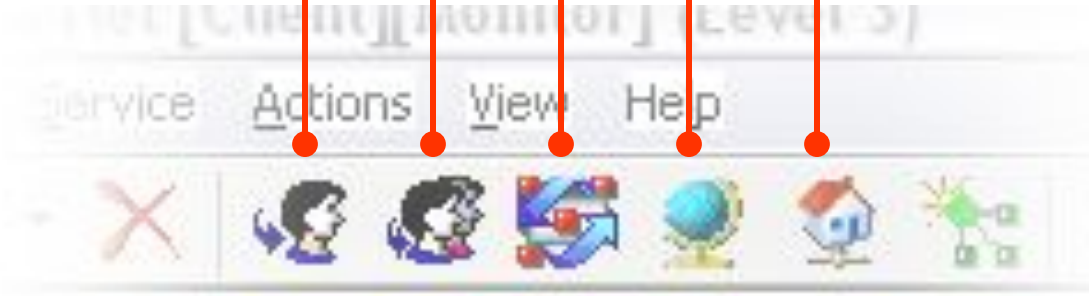
Web-ссылка

Деловая почта

Файловый обмен

Конференция

Чат



Чат/Мгновенная передача сообщений

Отправить сообщение

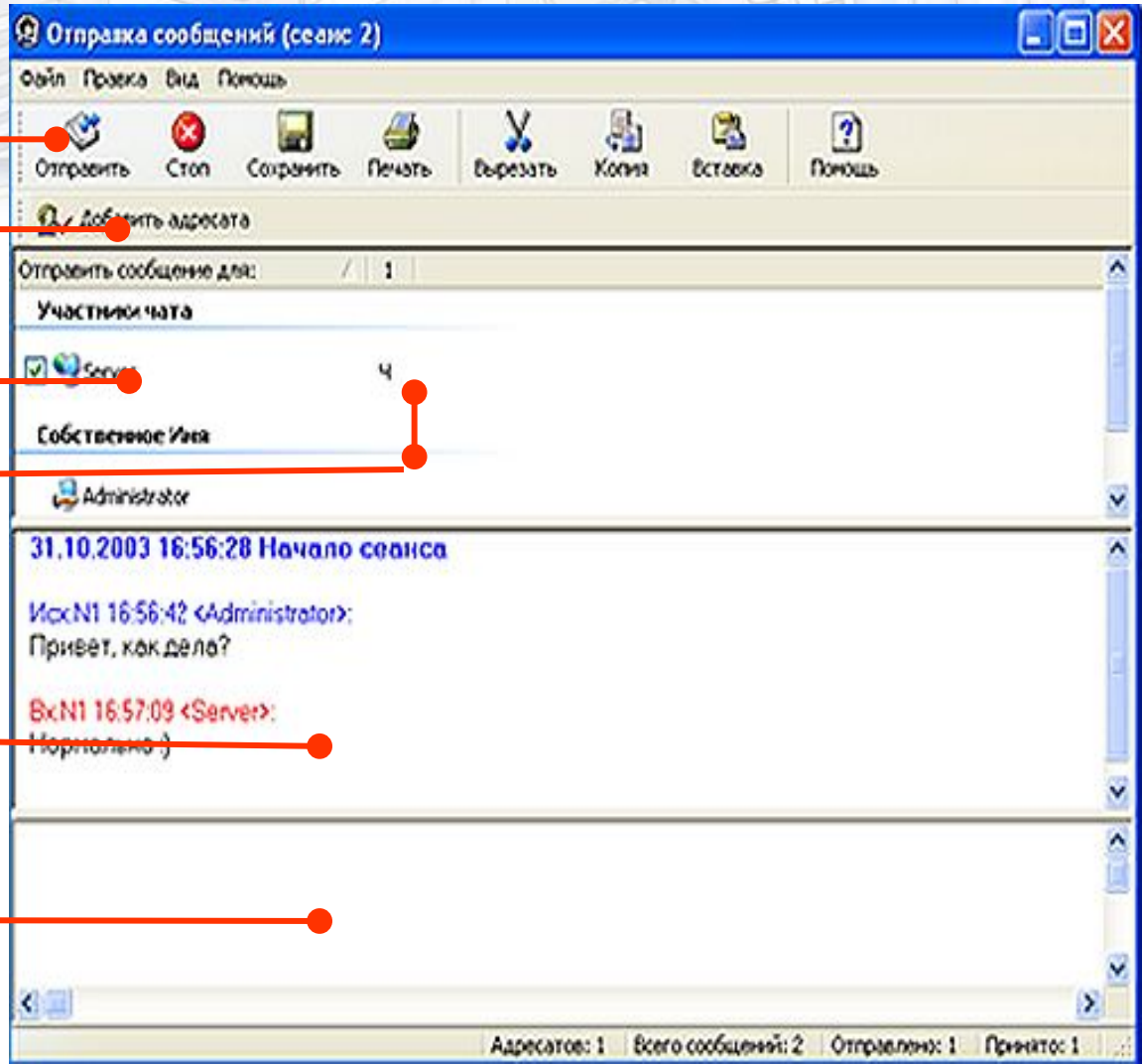
Здесь можно добавить пользователей к чату или организовать конференцию.

Список участников чата

Статус сообщения:
О=Отправлено, Д=Доставлено,
Ч=прочитано

Все сообщения текущей сессии

Область для написания сообщений



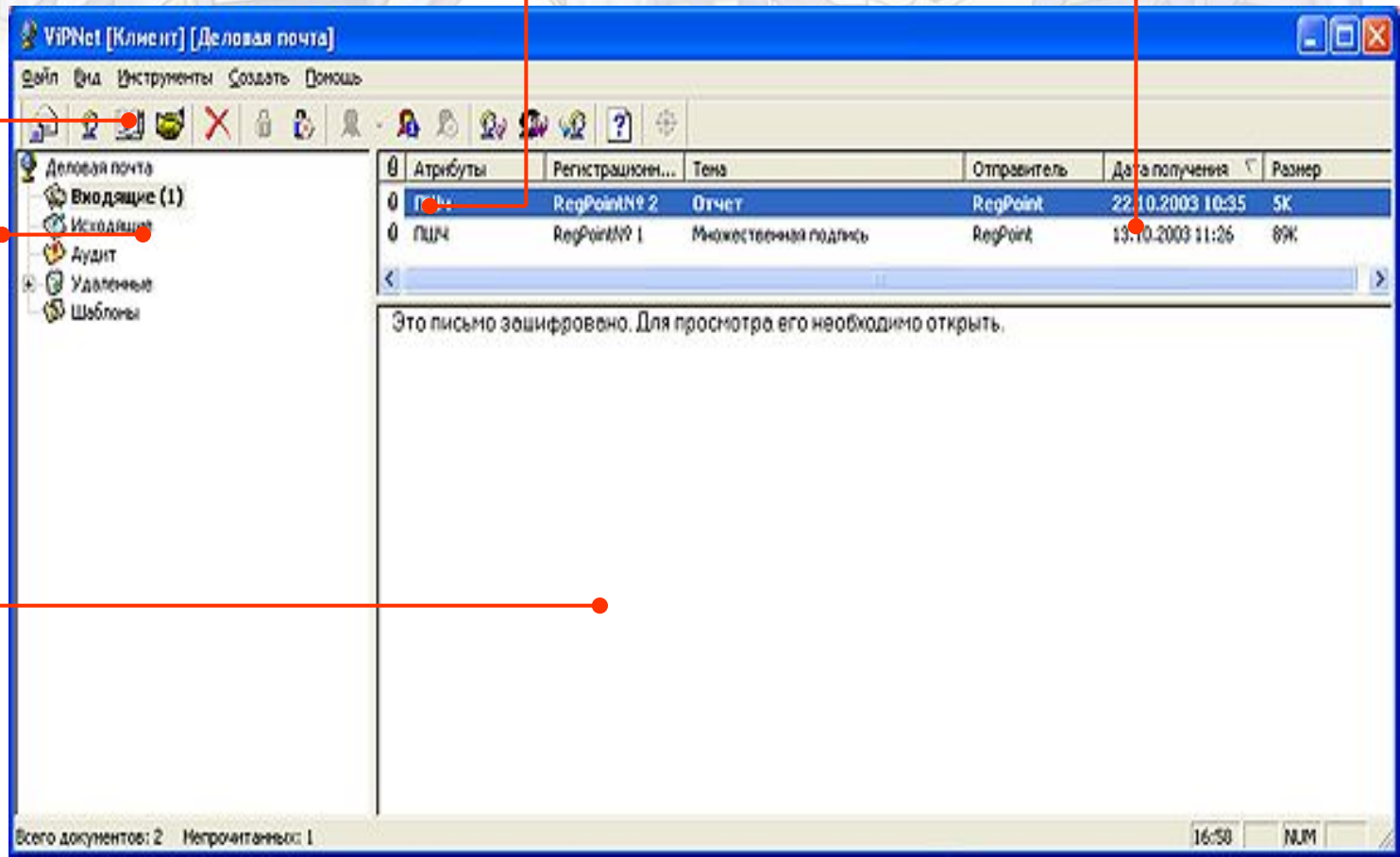
Эти атрибуты сообщают, поступило ли новое сообщение и прочитано ли оно.

Каждое сообщение перечисляется, чтобы облегчить поиск

Адресная книга

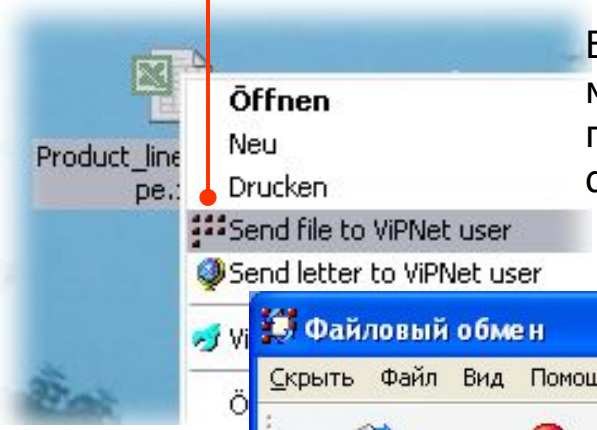
Ящики входящей и исходящей почты,

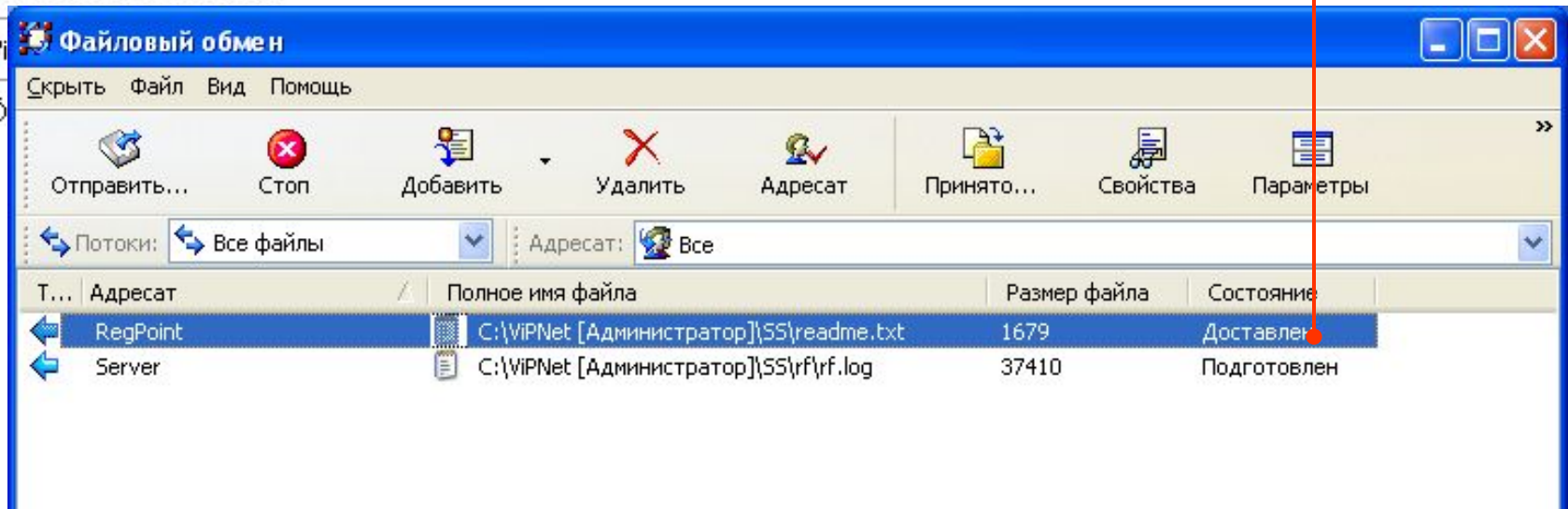
Все сообщения зашифрованы. После декодирования Вы можете читать содержание здесь.



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





Web-ссылка

Технология ViPNet позволяет легко организовывать авторизованный доступ к корпоративным ресурсам.

Если на Web-сервере установлен ViPNet [Клиент] или ViPNet [Координатор], то только ViPNet-пользователь через пункт контекстного меню «Web-ссылка» сможет попасть на этот сервер, например, на корпоративный Web-сайт.

Спецификация аппаратных и программных средств для установки АРМ VipNet Клиент

Для обеспечения работоспособности АРМ VipNet Клиент необходимо:

1.IBM совместимый персональный компьютер:

- Оперативная память -256Мб
- Процессор - 1000МГц
- Жесткий диск -20Гб
- Операционная система - Windows XP Pro Rus SP2

2.Сетевые интерфейсы - Модем (Acorp 56Кб/сек, US-Robotics 56Кб/сек), ADSL-модем

3.Канал доступа - модемный доступ к провайдеру Интернет