ООО «БВ Информационные технологии»

www.bw-it.ru

Тел.: +7 (495) 223-6663, +7 (495) 223-6664

ViPNet CUSTOM

индивидуально конфигурируемые решения

ViPNet™ CUSTOM

Защита сетей (VPN, межсетевые и персональные сетевые экраны)

Удостоверяющий центр (PKI, криптопровайдер)

Что такое ViPNet CUSTOM и зачем он нужен?

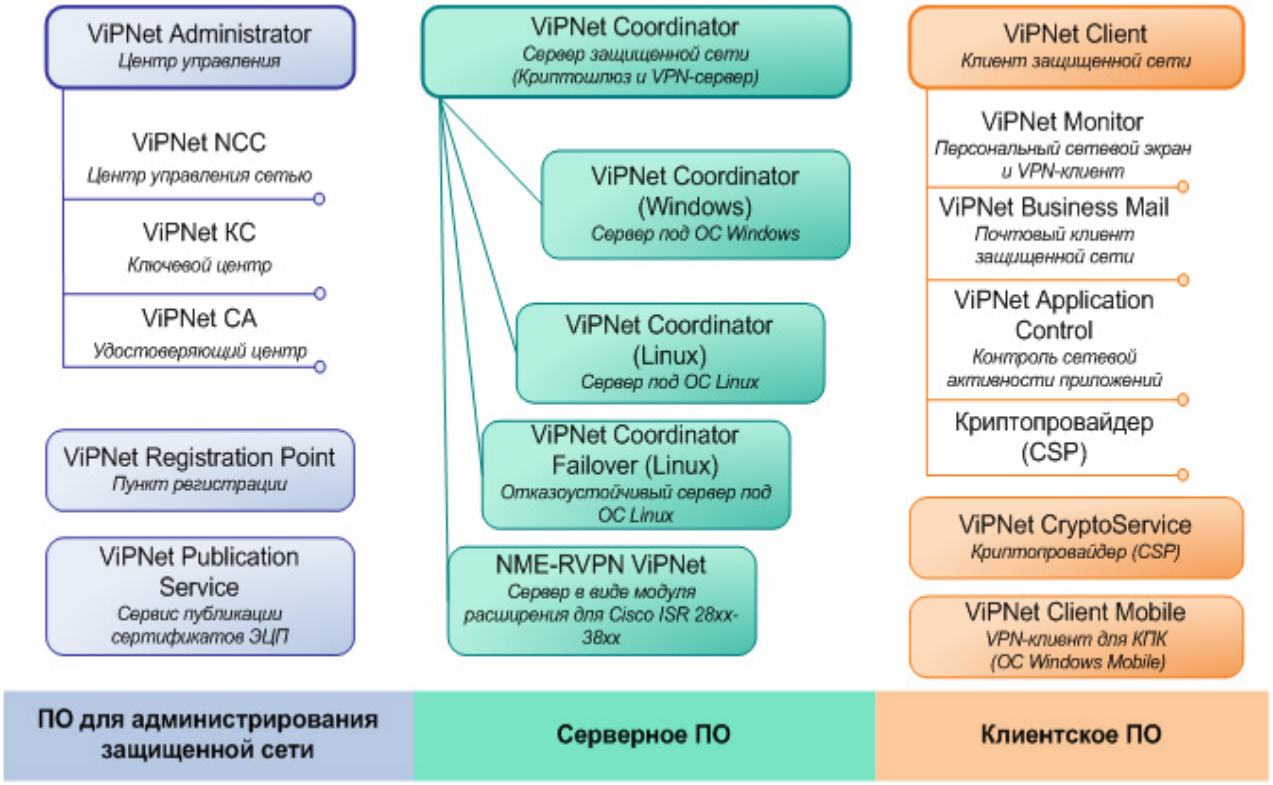
ViPNet CUSTOM – это название комплекса программного и программно-аппаратного обеспечения, разрабатываемого и поставляемого компанией Инфотекс для рынка средств защиты *конфиденциальной* информации.

ViPNet CUSTOM – это более 10 лет развития уникальных технологий защиты информации в корпоративных сетях крупных государственных и коммерческих организаций России, проводимого в соответствии с национальными стандартами по информационной безопасности.

ViPNet CUSTOM предназначен для объединения в единую защищенную виртуальную сеть произвольного числа рабочих станций, мобильных пользователей и локальных сетей; и нацелен на решение двух важных задач информационной безопасности:

- Создание защищенной, доверенной среды передачи конфиденциальной информации с использованием публичных и выделенных каналов связи (Интернет, телефонные и телеграфные линии связи и т.п.), путем организации виртуальной частной сети (VPN).
- Развертывание инфраструктуры открытых ключей (PKI) и организации Удостоверяющего Центра с целью интеграции механизмов электронно-цифровой подписи в прикладное программное обеспечение заказчика (системы документооборота и делопроизводства, электронную почту, банковское программное обеспечение, электронные торговые площадки и витрины). Поддерживается возможность взаимодействия с программным обеспечением PKI других отечественных производителей, например, ЗАО «Сигнал-КОМ» и ООО «Крипто-Про».

В настоящее время в состав комплекса ViPNet CUSTOM входит более 10 различных компонент и модулей, позволяющих реализовать множество сценариев защиты информации в современных мультисервисных сетях связи.



Базовыми компонентами ViPNet CUSTOM является ПО ViPNet Administrator, ViPNet Coordinator (в разных вариантах исполнения) и ViPNet Client. Эти компоненты являются основой для развертывания виртуальной частной сети и инфраструктуры открытых ключей. С целью расширения возможностей базовых компонент могут использоваться дополнительные компоненты ViPNet CUSTOM : ViPNet Registration Point, ViPNet Publication Service и ViPNet CryptoService.

Уникальной особенностью ViPNet CUSTOM является программное обеспечение ViPNet Client Mobile, которое позволяет использовать коммуникатор (КПК) с ОС Windows Mobile 2005/6, как полноценный VPN-клиент для удаленного защищенного подключения к ресурсам корпоративной сети через сеть сотового оператора по GPRS/EDGE или с использованием сетей WiFi.

Криптографические функции во всех компонентах комплекса ViPNet CUSTOM реализуются с помощью семейства средств криптографической защиты информации (СКЗИ) «Домен-К». СКЗИ «Домен-К» является разработкой компании Инфотекс и представляет собой набор программных библиотек, драйверов и средств управления ключами пользователя. В зависимости от выбранного уровня безопасности СКЗИ «Домен-К» может комплектоваться сертифицированными средствами защиты от несанкционированного доступа – электронными замками. В настоящее время доступны следующие версии СКЗИ «Домен-К»:

- СКЗИ «Домен-КС2» - прошло сертификацию в ФСБ России по классам КС1 и КС2;
- СКЗИ «Домен-КМ» - прошло сертификацию в ФСБ России по классу КС3.

С использованием ViPNet CUSTOM могут разрабатываться решения по защите информации, требующие проведения разработки/доработки функционала компонент комплекса по требованиям заказчика. Поэтому ViPNet CUSTOM – это постоянное развитие функциональных возможностей и следование современным требованиям российского рынка средств защиты информации.

Компания Инфотекс особое внимание уделяет вопросам сертификации своих разработок в соответствии с требованиями ФСБ и ФСТЭК России. Компоненты и наборы компонент из комплекса ViPNet CUSTOM регулярно проходят сертификацию по требованиям к СКЗИ, автоматизированным системам и средствам сетевого экранирования (межсетевым и персональным сетевым экранам).

ViPNet CUSTOM – это уникальное предложение на российском рынке средств защиты конфиденциальной информации, объединяющее в себе VPN -технологию и механизмы PKI с развитыми клиент-ориентированными сервисами. Вы думали, как сделать систему безопасности незаметной для пользователя, потому что она приносит только неудобства в работе? Не надо этого делать! Заинтересуйте пользователя возможностями ViPNet CUSTOM : почта, чат, файловый обмен, удаленный доступ к ресурсам корпоративной сети. Сделайте ViPNet CUSTOM частью бизнес-процессов вашей организации.

Технические преимущества ViPNet CUSTOM

- ViPNet CUSTOM ориентирован на организацию защищенного взаимодействия клиент-клиент, в то время как большинство VPN -решений других производителей обеспечивают только соединения уровня сервер-сервер или сервер-клиент. Это дает возможность реализовать любую необходимую политику разграничения доступа в рамках всей защищенной сети, а также снизить нагрузку на VPN - серверы, так как в общем случае при взаимодействии клиент-клиент VPN -сервер не задействован в операциях шифрования трафика между этими клиентами.
- Большое внимание в ViPNet CUSTOM уделено решению проблемы функционирования в условиях наличия разнообразного сетевого оборудования и программного обеспечения, реализующего динамическую или статическую трансляцию адресов/портов (NAT / PAT), что существенно облегчает процесс интеграции системы защиты в существующую инфраструктуру сети. В большинстве случаев ручной настройки клиентского ПО ViPNet Client вообще не потребуется.
- В ViPNet CUSTOM реализована раздельная фильтрация открытого и шифруемого трафиков, что позволяет даже среди доверенных сетевых узлов ограничивать возможность работы через несанкционированные порты, протоколы и еще выше поднимать уровень безопасности защищенной сети.
- Каждый компонент ViPNet CUSTOM содержит встроенный сетевой экран и систему контроля сетевой активности приложений, что позволяет получить надежную распределенную систему межсетевых и персональных сетевых экранов.
- Для разрешения возможных конфликтов IP -адресов в локальных сетях, включаемых в единую защищенную сеть, ViPNet CUSTOM предлагает развитую систему виртуальных адресов. Во многих случаях это позволяет упростить настройку прикладного ПО пользователя, так как наложенная виртуальная сеть со своими виртуальными адресами будет скрывать реальную сложную структуру сети.
- ViPNet CUSTOM поддерживает возможность межсетевого взаимодействия, что позволяет устанавливать необходимые защищенные каналы связи между произвольным числом защищенных сетей, построенных с использованием ViPNet CUSTOM.
- ViPNet CUSTOM обеспечивает защиту информации в современных мультисервисных сетях связи, предоставляющих услуги IP-телефонии и аудио- и видеоконференцсвязи. Поддерживается приоритезация трафика и протоколы H.323, Skinny.

Коммерческие преимущества ViPNet CUSTOM

- По сравнению с обычными VPN -решениями ViPNet CUSTOM предоставляет целый ряд дополнительных возможностей по защищенному обмену информацией: встроенные службы мгновенного обмена сообщениями (чат и конференция), файлами, собственная защищенная почтовая служба с элементами автоматизации обмена письмами и поддержкой механизмов ЭЦП.
- Дополнительные сетевые возможности комплекса ViPNet CUSTOM , такие как контроль сетевой активности приложений, строгий контроль доступа к Интернет, механизмы аварийной перезагрузки и защиты от вторжений на этапе загрузки операционной системы, позволяют защититься от большинства сетевых атак и минимизировать затраты на систему безопасности в целом.
- ViPNet CUSTOM является самодостаточным программным комплексом, поэтому нет необходимости приобретать дополнительные элементы вроде баз данных, почтовых серверов и специализированных серверных платформ. ViPNet CUSTOM не несет скрытых затрат - Вы платите только за те компоненты ViPNet CUSTOM , которые Вам необходимы.
- Так как ViPNet CUSTOM является программным комплексом, то его установка и настройка не требует приобретения специализированного оборудования и может быть произведена на уже существующем компьютерном парке заказчика. В большинстве случаев также не требуется переконфигурация сетевого оборудования.
- Гибкое ценообразование и возможность пополнения лицензии на компоненты ViPNet CUSTOM по необходимости, позволяют формировать оптимальное ценовое решение для каждого конкретного заказчика. Вы платите ровно за то, что Вам нужно сейчас, остальное можно купить позже.
- Компания Инфотекс проводит на регулярной основе учебные курсы по подготовке администраторов защищенной сети, построенной с использованием комплекса ViPNet CUSTOM . Обучив собственных специалистов, можно существенно сэкономить на работах по установке и настройке защищенной сети.

Компоненты ViPNet CUSTOM

Программное обеспечение для администрирования защищенной сети

ViPNet Administrator (Администратор) – это набор программного обеспечения, включающий в себя:

ViPNet NCC (Центр Управления Сетью, ЦУС) - предназначен для конфигурирования и управления виртуальной защищенной сетью ViPNet , решает следующие задачи:

- Определение узлов защищенной сети, пользователей и допустимых связей между ними путем создание необходимых баз данных для работы Удостоверяющего и Ключевого Центров;
- Определение политики безопасности на каждом узле и формирование списка прикладных задач, которые могут быть на данном узле запущены (шифрование трафика, ЭЦП, Деловая Почта и т.д.);
- Поддержание сервиса автоматической рассылки 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.);
- Проведение автоматического централизованного обновления ПО ViPNet на узлах защищенной сети;
- Поддержание удаленного доступа к журналам событий на узлах защищенной сети.

ViPNet KC & CA (Удостоверяющий и Ключевой Центр, УКЦ) – выполняет функции центра выработки ключей шифрования и персональных ключей пользователей, а также Удостоверяющего Центра для организации PKI .

Основными функциями Ключевого Центра являются:

- Выработка и хранение первичной ключевой информации (мастер-ключи шифрования и межсетевые мастер-ключи);
- Выработка ключей шифрования для узлов защищенной сети и ключей шифрования между пользователями защищенной сети (двухуровневая схема);
- Выполнение процедур смены мастер-ключей и компрометации ключей шифрования;
- Выработка персональных ключей защиты пользователей и криптографически надежных парольных фраз (паролей);
- Запись персональных ключей пользователей на аппаратные носители ключей (token ' s , smartcard , touch memory).

Все ключи, вырабатываемые Ключевым Центром - симметричные, длиной 256 бит, используются при шифровании по ГОСТ 28147-89.

Основными функциями Удостоверяющего Центра являются:

- Создание ключей подписи и издание сертификатов Уполномоченных лиц УЦ, формирование запроса на издание сертификата Уполномоченного лица к головному УЦ;
- Импорт сертификатов Уполномоченных лиц УЦ смежных сетей и головного УЦ;
- Создание ключей подписи пользователей и издание соответствующих сертификатов, рассмотрение запросов на издание сертификатов от пользователей сети;
- Взаимодействие с Центрами Регистрации;
- Выполнение операций по отзыву, приостановлению и возобновлению сертификатов, рассылка соответствующих списков отзыва;
- Ведение журналов работы и хранение списков изданных сертификатов;
- Запись сертификатов и секретных ключей пользователей на аппаратные носители ключей;
- Кросс-сертификация с УЦ других производителей (УЦ Крипто-Про, УЦ Сигнал-КОМ, Стандарт УЦ и др.)

УЦ обеспечивает возможность формирования ключей подписи на основе алгоритма ГОСТ Р 34.10-2001. Сертификаты формируются в формате X.509 v3

Программное обеспечение, входящее в состав набора ViPNet Administrator устанавливается на компьютеры вместе с программным обеспечением ViPNet Client . Это делается с целью сетевой защиты составляющих ViPNet Administrator и их включения в единую защищенную сеть ViPNet .

ViPNet Registration Point (Пункт Регистрации) – программное обеспечение, выполняющее функции пункта регистрации пользователей защищенной сети. ViPNet Registration Point состоит из Центра Регистрации, дополненного ПО ViPNet Client . В защищенной сети ViPNet данное программное обеспечение выполняет роль удаленного филиала ViPNet Administrator , что позволяет децентрализовать систему управления защищенной сетью, когда исходная сеть заказчика представляет из себя большую географически распределенную корпоративную сеть.

Пункт Регистрации реализует следующий функционал:

- Регистрация пользователей защищенной сети и внешних пользователей (держателей ЭЦП);
- Формирование секретного ключа подписи пользователя и его запись на аппаратный носитель ключевой информации;
- Формирование и отправку в УЦ запроса на сертификацию подписи от своего имени (Уполномоченного лица Центра Регистрации), прием и ввод в действие;
- Ведение справочника запросов и изданных сертификатов;
- Формирование запросов на отзыв, приостановление и возобновление сертификатов зарегистрированных пользователей;
- Ведение журналов работы и хранение списков изданных сертификатов;
- Ведение журнала событий и действий Уполномоченного лица ЦР;
- Импорт учетных записей пользователей из каталога Active Directory.

Центров Регистрации в одной защищенной сети ViPNet может быть сколь угодно много, что позволяет при грамотно спроектированной топологии защищенной сети существенно снизить трудозатраты администратора защищенной сети, делегировав ряд его функций операторам Центров Регистрации.

ViPNet Publication Service (Сервис Публикации) – выполняет функции сервиса публикации различных списков сертификатов ЭЦП в стандартных хранилищах сертификатов и является расширением к базовой функциональности Удостоверяющего Центра ViPNet . Сервис публикации необходим, если требуется решать задачи взаимодействия со сторонними Удостоверяющими Центрами.

Сервис Публикации выполняет следующие функции:

- Публикация списков отозванных сертификатов;
- Публикация списков изданных сертификатов пользователей и Уполномоченных лиц;
- Обеспечение публикации (экспорта) и импорта сертификатов пользователей через стандартные транспортные протоколы (через LDAP в Active Directory, через FTP на WWW-серверах);
- Формирование отчетов о публикации сертификатов Уполномоченных лиц для УЦ с целью включения этой информации в сертификаты пользователей.

Серверное программное обеспечение для организации защищенной сети

ViPNet Coordinator (Координатор) – это общее название линейки программного обеспечения, выполняющего функции универсального сервера защищенной сети ViPNet . В зависимости от настроек ViPNet Coordinator может выполнять следующие функции:

- Сервера IP-адресов — обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и текущем значении их сетевых настроек (IP- адресов и т.п.);
- Прокси-сервера защищенных соединений — обеспечивает подключение локальной ViPNet сети к другим аналогичным сетям через публичные сети (Интернет);
- Туннельного сервера (криптошлюза) — обеспечивает туннелирование (шифрование) трафика от незащищенных компьютеров и серверов локальной сети для его передачи к другим объектам защищенной сети (в том числе мобильным и удаленным) в зашифрованном виде по открытым

каналам публичных сетей. Для мобильных и удаленных объектов защищенной сети туннельный сервер выступает в роли сервера доступа к ресурсам локальной сети;

- Межсетевого экрана — обеспечивает в соответствии с заданной политикой безопасности фильтрацию трафика по множеству параметров (порты, протоколы, диапазоны адресов и др.) между сегментами защищенной и открытой сетей.
- Сервера защищенной почты — обеспечивает маршрутизацию почтовых сообщений для сервиса ViPNet Business Mail и служебных рассылок в рамках защищенной сети.

ViPNet Coordinator выпускается в виде следующего программного и программно-аппаратного обеспечения:

- ViPNet Coordinator (Windows) – полнофункциональный сервер защищенной сети ViPNet , устанавливаемый на ОС Windows 2000/XP/2003 Server ;
- ViPNet Coordinator (Linux) - полнофункциональный сервер защищенной сети ViPNet , устанавливаемый на ОС Linux с ядрами 2.4.2/31- -2.6.2/18 (дистрибутивы RedHat , Suse и др.)
- ViPNet Coordinator Failover – полнофункциональный сервер защищенной сети ViPNet для ОС Linux, позволяющий реализовать схему отказоустойчивого кластера «горячего резервирования» из 2-х физических серверов. Время автоматического переключения с активного на резервный сервер на аппаратной платформе с P4 3 ГГц составляет 10-15 сек. Сфера применения такого решения – ответственные участки защищенной сети (например, криптошлюзы) с повышенными требованиями к отказоустойчивости.
- NME-RVPN ViPNet - программно-аппаратное решение, выполняет все заявленные функции ViPNet Coordinator за исключением функции сервера защищенной почты. Поставляется предустановленным на аппаратную платформу модуля расширения NME-RVPN для маршрутизаторов Cisco ISR 28xx-38xx. Совместно с данными маршрутизаторами является идеальным решением для организации мультисервисных защищенных сетей связи, например, создания защищенной корпоративной сети IP-телефонии.

Клиентское программное обеспечение для организации защищенной сети

ViPNet Client (Клиент) – это программное обеспечение для ОС Windows 2000/ XP /2003 Server/Vista, реализующее на рабочем месте пользователя или сервере с прикладным ПО функции VPN -клиента, персонального экрана и клиента защищенной почтовой системы. ViPNet Client состоит из набора программных модулей:

1) ViPNet Monitor (Монитор) – отвечает за реализацию функций:

- ***Персонального сетевого экрана*** — надежно защищает рабочую станцию/сервер от возможных сетевых атак, как из глобальной, так и из локальной сети. При этом:
  - Осуществляется фильтрация защищенного и открытого трафиков по множеству параметров («белый» и «черный» списки IP-адресов, порты, протоколы, типы сервисов и приложений);
  - Реализуется режим «stealth» (режим инициативных соединений), позволяющий сделать невидимым компьютер защищенной сети из открытой сети;
  - Имеет встроенную систему обнаружения вторжений (IDS);
  - Обеспечивает мониторинг сетевой активности приложений, позволяющий обнаружить и блокировать несанкционированную активность программ-«троянцев».
- ***Шифратора TCP/IP трафика*** — обеспечивает защиту (конфиденциальность, подлинность и целостность) любого вида трафика (приложений, систем управления и служебного трафика ОС), передаваемого между любыми объектами защищенной сети, будь-то рабочие станции, информационные серверы, серверы приложений, сетевые устройства и узлы. Высокая производительность шифрующего драйвера позволяет в реальном времени защищать трафик служб голосовой и видеосвязи в сетях TCP/IP. Поддерживается прозрачная работа через устройства статической и динамической NAT/PAT маршрутизации.
- ***Чат-клиента*** – позволяет пользоваться услугами сервиса обмена защищенными сообщениями и организации чат-конференций между объектами защищенной сети ViPNet , на которых установлены ViPNet Client или ViPNet Coordinator (Windows).
- ***Клиента службы обмена файлами*** – позволяет обмениваться между объектами защищенной сети ViPNet любыми файлами без установки дополнительного ПО (например, FTP -сервера/клиента) или использования функций ОС по общему доступу к файлам через сеть. Обмен файлами производится через защищенную транспортную сеть ViPNet с гарантированной доставкой и «докачкой» файлов при обрыве связи.

2) ViPNet Application Control (Контроль приложений) – программный модуль – позволяет контролировать сетевую активность приложений и компонент операционной системы. При этом можно формировать «черный» и «белый» списки приложений, которым запрещено или разрешено работать в сети, а также задавать реакцию на сетевую активность неизвестных приложений. В большинстве случаев это позволяет предотвратить несанкционированную сетевую активность вредоносного ПО, например, программ-«троянцев».

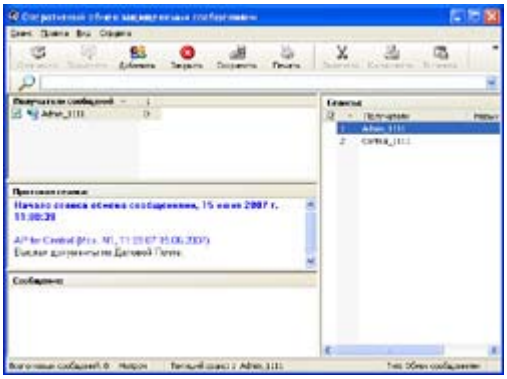
3) ViPNet Business Mail (Деловая Почта) – программный модуль – выполняет функции почтового клиента защищенной почтовой службы, функционирующей в рамках защищенной сети ViPNet , и позволяет:

- Формировать и отсылать письма адресатам защищенной сети через простой графический интерфейс пользователя. Возможна многоадресная рассылка;
- Использовать встроенные механизмы ЭЦП для подписи, в том числе множественной, текста письма и его вложений;
- Контролировать все этапы «жизни» письма благодаря встроенному механизму обязательного квитирования писем. Можно всегда убедиться, что письмо было доставлено, прочитано, открыты вложения. Квитанции об этих событиях могут автоматически подписывать ЭЦП получателя;
- Благодаря встроенной функции аудита иметь доступ к истории удаления писем;
- Вести архивы писем и при необходимости легко переключаться между текущим хранилищем писем и этими архивами;
- Использовать мощный механизм автоматической обработки входящих писем и файлов - задавать правила обработки входящих писем, а также правила по автоматическому формированию и отправке писем с заданными файлами;

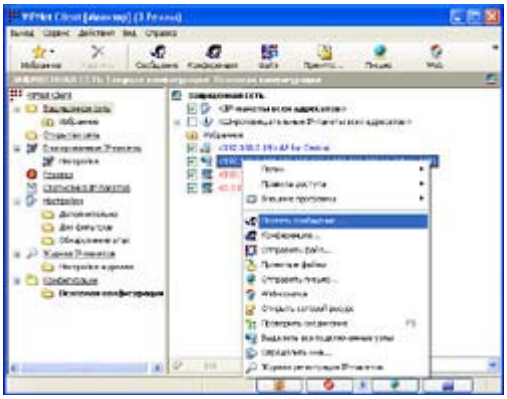
Деловая Почта свободна от спама! Любой отправитель нежелательной корреспон-денции может быть однозначно установлен. Поэтому этот сервис ViPNet является идеальным решением для внутрикорпоративного обмена документами и письмами.

4) Криптопровайдер (CSP) - ViPNet Client содержит встроенный криптопровайдер, реализующий стандартный для разработчиков прикладных систем под ОС Windows интерфейс Microsoft Crypto API 2.0. При этом дополнительно предоставляется COM-интерфейс для вызова криптографических функций и их использования Web приложениями, а также низкоуровневый С-интерфейс к функциям СКЗИ «Домен-К» для встраивания в приложения заказчика.

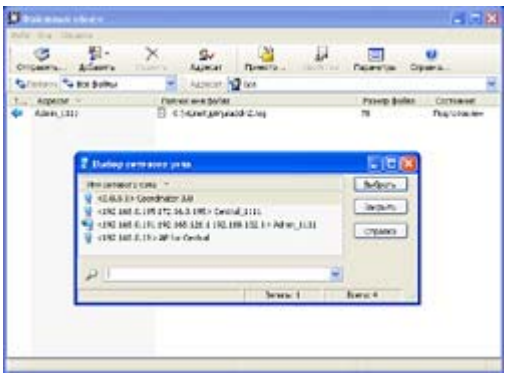
Скриншоты



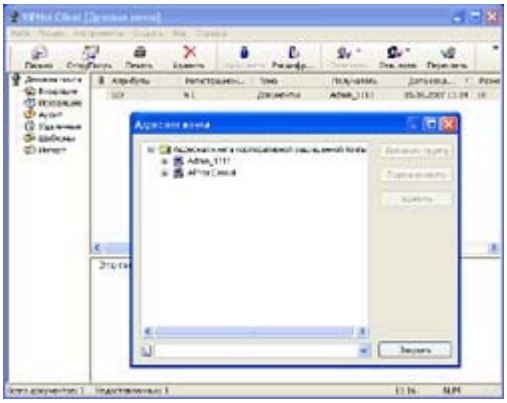
Чат



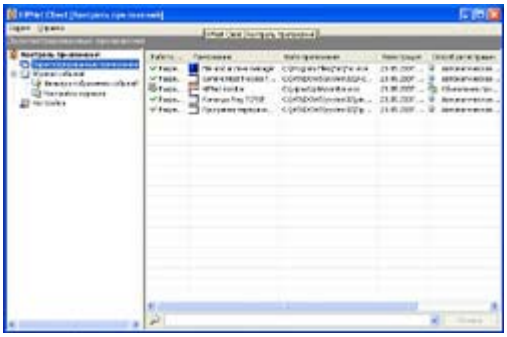
Контекстное меню



Файловый обмен



Деловая почта



Контроль приложений

CryptoService

ViPNet CryptoService

ViPNet CryptoService (КриптоСервис) – самый «легкий» компонент в комплексе ViPNet , предназначен для обеспечения возможности использовать криптографические функции СКЗИ «Домен-К» в прикладном программном обеспечении заказчика, функционирующем под ОС Windows 2000/XP/2003 Server (почтовые и

банковские системы, системы электронного, юридически значимого документооборота, электронные витрины и т.п).

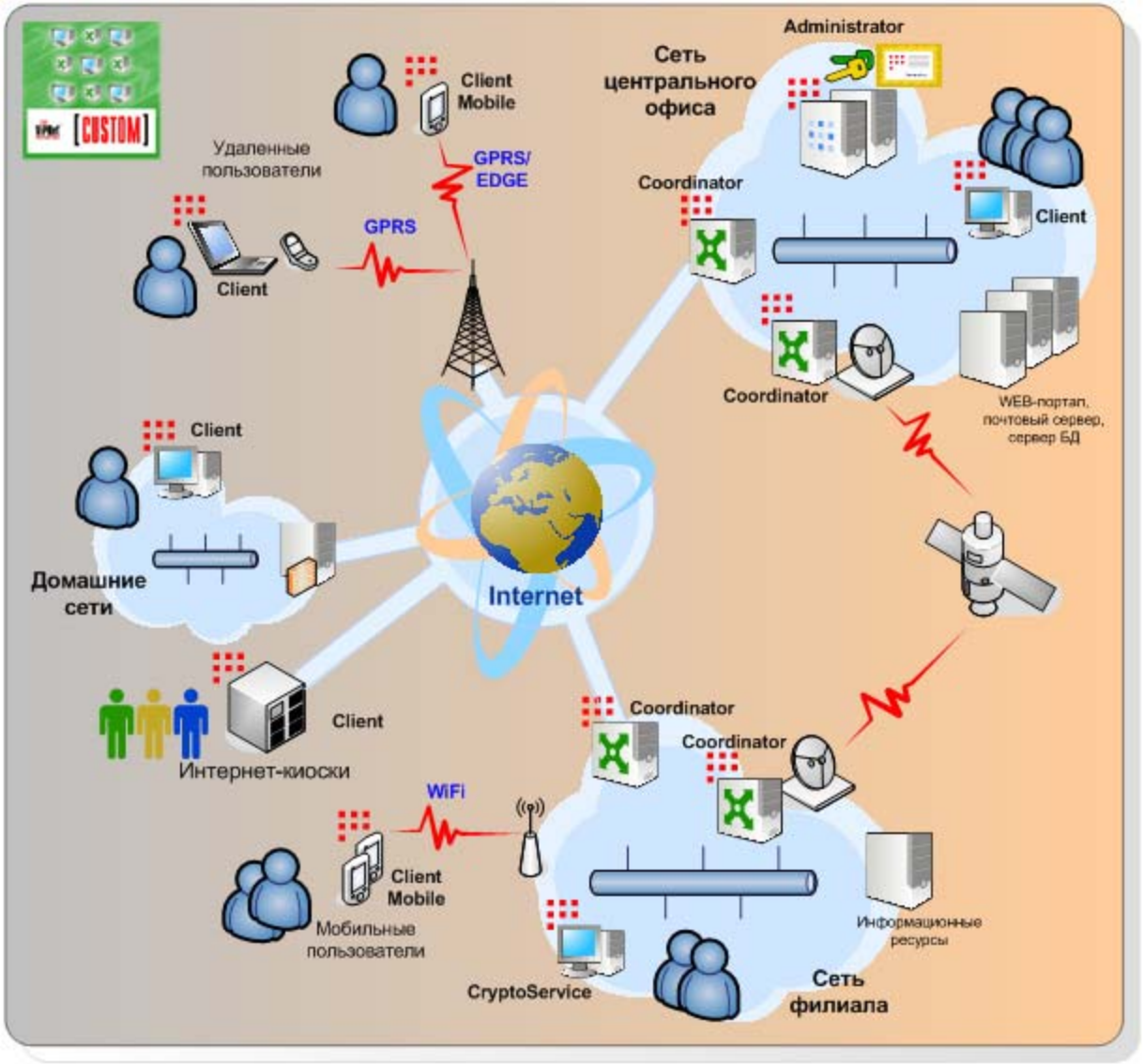
Также как и ViPNet Client ViPNet CryptoService содержит полноценный криптопровайдер, поддерживающий Microsoft Crypto API 2.0., а также высокоуровневый COM - и низкоуровневый C-интерфейсы. Программный модуль «Сервис Безопасности», входящий в состав ViPNet CryptoService обеспечивает все необходимые операции по работе с ключами пользователя: чтение/запись персональных ключей с электронных носителей (token's, smartcard), обновление ключей пользователя, формирование запросов на издание новых сертификатов ЭЦП пользователя и т.п.

Внимание! ViPNet CryptoService, являясь функциональным аналогом криптопровайдеров CryptoPro CSP, SignalCOM CSP и др., также как и они не содержит встроенных средств сетевой защиты. Поэтому применять ViPNet CryptoService следует только на компьютерах, функционирующих в контролируемых сегментах локальных сетей, надежно защищенных от несанкционированного доступа межсетевыми экранами и средствами обнаружения вторжений. Во всех остальных случаях рекомендуется использовать ViPNet Client.

ViPNet Client Mobile

ViPNet Client Mobile (Клиент для КПК) – уникальное программное решение для российского рынка СЗИ – представляет собой программный VPN-клиент и персональный сетевой экран для установки в «наладонники» под управлением ОС Windows Mobile 2005/6. Вместе с ViPNet Client Mobile обычный КПК включается в защищенную сеть ViPNet и превращается в устройство удаленного защищенного доступа к ресурсам корпоративной сети – внутрикорпоративный WEB-портал, почтовые сервисы и т.п. – вся информация будет зашифрована и передана по сетям сотовых операторов и Интернету в закрытом виде. ViPNet Client Mobile поддерживает работу через интерфейсы WiFi и GPRS/EDGE.

Примеры использования ViPNet CUSTOM



Внедрение **ViPNet CUSTOM** позволяет:

- Использовать ViPNet Coordinator как корпоративный межсетевой экран для защиты информационных ресурсов локальных сетей от хакерских атак из Интернета.
- Использовать ViPNet Coordinator как криптошлюз для шифрования конфиденциальной информации, передаваемой через разнообразные каналы связи (Интернет, выделенные линии) независимо от типа подключения к ним (ISDN , xDSL и т.п.) и наличия разнообразного сете- и каналообразующих устройств (межсетевые экраны других производителей, маршрутизаторы с NAT / dNAT , коммутаторы, модемы).
- Подключать к защищенной сети удаленных и мобильных пользователей, в том числе пользователей «наладонников» (КПК), при этом могут использоваться самые различные способы подключения таких пользователей к сети (DialUp , GPRS , WiFi , домашние сети).
- Строить на базе Удостоверяющего Центра ViPNet (ViPNet Administrator) инфраструктуру открытых ключей (PKI) для обеспечения юридически значимого документооборота в рамках компании, а также проводить обмен электронными документами с другими организациями и внешними пользователями (Интернет-киоски, электронные витрины и торговые площадки, системы клиент-банк и т.п.)
- Устанавливая ViPNet Client на компьютеры внутри локальных сетей, реализовывать разграничение доступа между группами пользователей, и обеспечивать тем самым защиту корпоративных ресурсов от злонамеренных действий самих сотрудников компании (проблема внутренней утечки и порчи информации).

- Использовать встроенные сервисные возможности ViPNet CUSTOM (Деловая Почта, чат, конференция, обмен файлами) для повышения доступности пользователя и оперативного обмена информацией, независимо от того, где тот находится в рамках VPN в каждый конкретный период времени (как пример - руководители и сотрудники в командировках).

Сертификаты на продукты

- Сертификат соответствия ФСБ России №СФ/114-1150 от 31 марта 2008 года на средство криптографической защиты информации (СКЗИ) "Домен-КМ" на соответствие требованиям ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к СКЗИ класса КС3 для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.
- Сертификат ФСБ России № СФ/114-1048 от 1 августа 2007 г. на СКЗИ «Домен-КС2» на соответствие ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.11-94, ГОСТ Р34.10-2001 и требованиям ФСБ к СКЗИ класса КС1 и КС2 (в разных комплектациях) для обработки информации, не содержащей сведений, составляющих государственную тайну.
- Сертификат ФСБ России № СФ/124-0984 от 1 марта 2007 г. на аппаратно-программное средство защиты информации ViPNet Клиент (версия 3.0) на соответствие требованиям ФСБ России к СКЗИ класса КС2 и требованиям к межсетевым экранам по 4 классу для защиты информации, не содержащей сведений, составляющих государственную тайну.
- Сертификат ФСБ России № СФ/124-0985 от 1 марта 2007 г. на аппаратно-программное средство защиты информации ViPNet Координатор (версия 3.0) на соответствие требованиям ФСБ России к СКЗИ класса КС2 и требованиям к межсетевым экранам по 4 классу для защиты информации, не содержащей сведений, составляющих государственную тайну.
- Сертификат Федеральной Службы по Техническому и Экспортному контролю России (Гостехкомиссия) №1549 от 17 января 2008 г. на программный комплекс «ViPNet CUSTOM 3.0» – на соответствие оценочному уровню доверия ОУД 4+, требованиям к межсетевым экранам по 3 классу защищенности, 3 уровню контроля НДВ и возможность использования для создания автоматизированных систем до класса 1В включительно.
- Сертификат соответствия № ГО00.RU.1313.Н00014 от 20 ноября 2007 года системы добровольной сертификации ГАЗПРОМСЕРТ на средство криптографической защиты информации (СКЗИ) «Домен-КС2».

Подробнее узнать об использовании VipNet CUSTOM и условиях приобретения можно по телефонам +7 (495) 223-6663 или +7 (495) 223-6664 ООО «БВ Информационные технологии» www.bw-it.ru