

ТРОПАTM ДЖЕТ

Комплекс кодирования межсетевых потоков

Комплекс «Тропа-Джет» обеспечивает защиту информации в процессе ее передачи между территориально разнесенными локальными сетями, связь которых осуществляется по протоколу TCP/IP.

«Тропа-Джет» позволяет объединить локальные сети в виртуальную защищенную сеть (VPN). При этом весь трафик виртуальной защищенной сети, проходящий по сетям общего пользования, защищается при помощи кодирования.

Одной из важнейших задач обеспечения информационной безопасности является защита потоков корпоративных данных, передаваемых по каналам связи общего пользования, в том числе через Интернет. Перспективным и надежным методом защиты передаваемой информации является кодирование данных на выходе из локальной сети и декодирование данных, поступающих в нее.

Программный комплекс кодирования межсетевых потоков (ККМП) «Тропа-Джет» предназначен для обеспечения конфиденциальности и целостности информации, передаваемой по открытым каналам связи.

Комплекс «Тропа-Джет» выполняет следующие функции:

Кодирование межсетевых потоков

Кодирование межсетевых информационных потоков в открытых сетях передачи данных выполняется путем организации виртуальных защищенных сетей (Virtual Private Networks, VPN). Каждая сеть в составе VPN защищена своим кодирующим модулем, устанавливаемым в точке ее соединения с внешними сетями. Защищаемая информация кодируется на передающем модуле и декодируется на принимающем, т.е. передается в открытом виде в пределах локальных сетей и в кодированном – за их пределами. Кодированный трафик передается по протоколу IPsec.

Создание контура безопасности

ККМП «Тропа-Джет» позволяет сформировать контур безопасности, объединяющий IP-адреса всех абонентов, имеющих доступ в виртуальную защищенную сеть. Абонентами VPN могут быть целые сети, подсети и отдельные рабочие станции.

Выборочное кодирование трафика

Формирование контура безопасности служит для разделения трафика на кодируемый и неко-

дируемый потоки. Кодирующий модуль ККМП «Тропа-Джет» производит выделение пакетов, которые необходимо кодировать, на основании IP-адресов отправителя пакета и получателя пакета и, кроме того, проверки интерфейса, через который проходит пакет.

Управление ключевой системой

В ККМП «Тропа-Джет» реализована несимметричная ключевая система, когда потенциальные участники обмена данными используют пары долговременных секретного и открытого ключей кодирования. Кодирование осуществляется на основе сеансовых ключей, автоматически формируемых при помощи долговременных ключей и имеющих ограниченное время жизни. Комплекс «Тропа-Джет» осуществляет все необходимые действия по управлению ключами: генерацию и распределение долговременных ключей, выработку сеансовых ключей абонентов, сертификацию открытых ключей в доверенном центре, плановую и внештатную смену ключей кодирования.

Регистрация событий, мониторинг и управление межсетевыми потоками

ККМП «Тропа-Джет» осуществляет сбор и хранение статистической и служебной информации обо всех штатных и нештатных событиях, возникающих при аутентификации узлов, передаче кодированной информации, ограничении доступа абонентов ЛВС. Средства мониторинга проводят сбор и анализ протоколов регистрации от всех модулей комплекса по кодированному каналу.

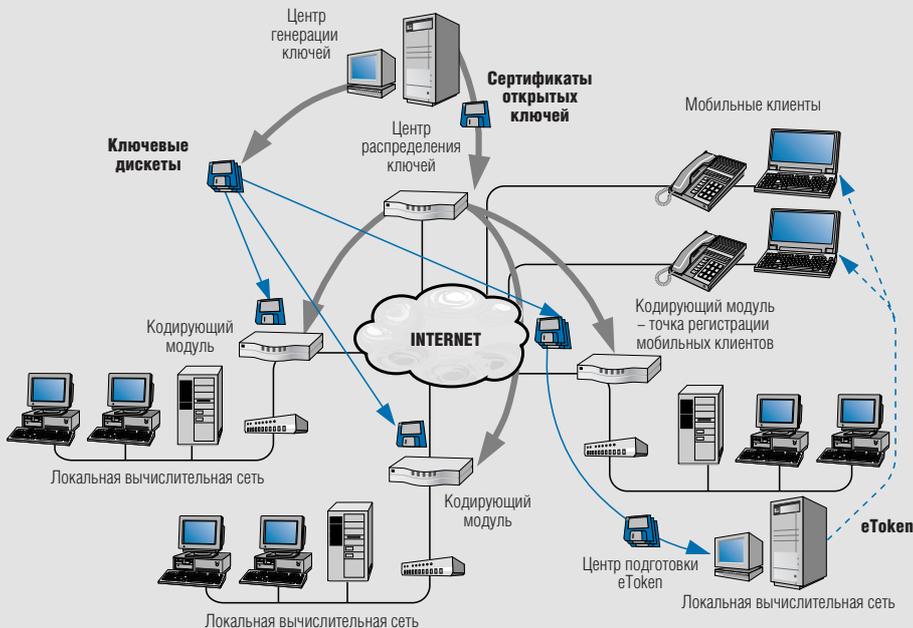
Защита соединений с мобильными клиентами

В состав виртуальной защищенной сети могут входить мобильные клиенты – удаленные компьютеры, подключаемые по выделенным или коммутируемым каналам связи. Носителем ключевой информации для них является электронный ключ eToken.



Основные характеристики ККМП «Тропа–Джет»

Схема организации виртуальной защищенной сети



Надежная защита межсетевого информационного обмена

- весь трафик между абонентами виртуальной защищенной сети кодируется.

Централизованное управление контуром безопасности

- централизованные настройки и администрирование компонентов комплекса с рабочего места администратора;
- удаленное управление по защищенному каналу с помощью графического интерфейса или командной строки.

Полнофункциональная система управления ключами

- динамическое распределение ключей с использованием доверенного центра сертификации;
- проверка подлинности ключевой информации при проведении взаимной аутентификации шлюзов кодирования и выработке сеансового ключа;

- оповещение систем кодирования о компрометации ключей.

Обеспечение собственной защиты

- взаимная аутентификация шлюзов кодирования в момент выработки сеансовых ключей;
- аутентификация администраторов и ограничение доступа к функциям администрирования.

Высокая надежность функционирования

- средства контроля целостности программной и информационной частей комплекса;
- средства определения и уведомления администратора об изменении файлов;
- встроенные средства протоколирования и аудита;
- средства обеспечения устойчивости к сбоям и восстановления работоспособности в случае сбоев и отказов.

Прозрачность

- кодирование передаваемых данных является прозрачным для абонентов и используемого ими программного обеспечения.

Высокая производительность

- работа в сети 100 Мбит/с без существенного влияния на пропускную способность (~86 Мбит/с).

Обеспечение качества сервиса

- поддержка работы с сервисами, предъявляющими высокие требования к величинам временных задержек (IP-телефония, видеоконференцсвязь).

Защита мобильных клиентов

- специальный кодирующий модуль для подключения произвольного количества мобильных клиентов.

Различные варианты выбора платформ

- функционирование под управлением ОС Solaris на аппаратной платформе SPARC или Intel.

Возможность построения комплексных решений по защите

- возможность использования в комплексе с межсетевыми экранами, антивирусными решениями и средствами контекстного анализа.

Использование открытых стандартов

- протокол туннелирования сетевых пакетов соответствует стандартам IETF IPsec;
- формат сертификатов соответствует стандарту X.509.

Сертифицированное решение

- сертификат Гостехкомиссии России № 466 от 14.06.2001 г. на соответствие Техническим условиям и отсутствие недекларированных возможностей;
- возможность использования различных криптографических библиотек, в том числе сертифицированных ФАПСИ.

«Инфосистемы Джет»

Россия, 103006, Москва,
Краснопролетарская 6.
Тел.: (095) 972 11 82, (095) 972 13 32
Факс: (095) 972 07 91
www.jet.msk.su, tropa@jet.msk.su

