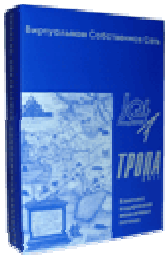


==========

Комплекс кодирования межсетевых потоков «Тропа-Джет»

==========

Одной из важнейших задач обеспечения информационной безопасности является ***защита потоков корпоративных данных***, передаваемых по каналам общего пользования, в том числе и через Internet. Перспективным методом надежной защиты информации является ***метод кодирования данных***.

Для решения этой задачи необходимо осуществить кодирование информации на выходе из локальной сети и декодирование поступающих в нее данных. Эти функции реализуются специальными программными или программно-аппаратными средствами. Если защита сегмента корпоративной сети уже обеспечена межсетевым экраном, естественно возложить на него также выполнение функций ***кодирования и декодирования***.

Для реализации возможностей кодирования/декодирования должно быть выполнено предварительное (начальное) ***распределение ключей***. Современные технологии предлагают для этого целый ряд методов. После распределения ключей появляется возможность осуществления процесса ***выработки совместных секретных ключей***, обслуживающих сеанс общения абонентов.

В результате кодирования весь обмен данными между территориально-удаленными локальными сетями является ***защищенным*** и для пользователей выглядит как обмен внутри одной локальной сети, при этом от пользователей ***не требуется применение каких-либо дополнительных защитных средств***.

Комплекс кодирования межсетевых потоков (ККМП) «Тропа-Джет»

Программный комплекс кодирования межсетевых потоков (ККМП) «Тропа-Джет» реализует функции кодирования межсетевых информационных потоков в сетях передачи данных протокола TCP/IP для обеспечения обмена информацией между территориально-удаленными локальными сетями. Это обеспечивается посредством организации виртуальных защищенных сетей (Virtual Private Networks – VPN).

Комплекс «Тропа-Джет» выполняет следующие функции:

- **Кодирование межсетевых потоков**

  Функции кодирования межсетевых информационных потоков в открытых сетях передачи данных выполняются путем организации 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. Кроме того, кодирующий модуль может быть установлен на отдельную рабочую станцию.

- **Выборочное кодирование трафика**

Формирование контура безопасности служит для разделения трафика на кодируемый и некодируемый 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 несим- метричная 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**

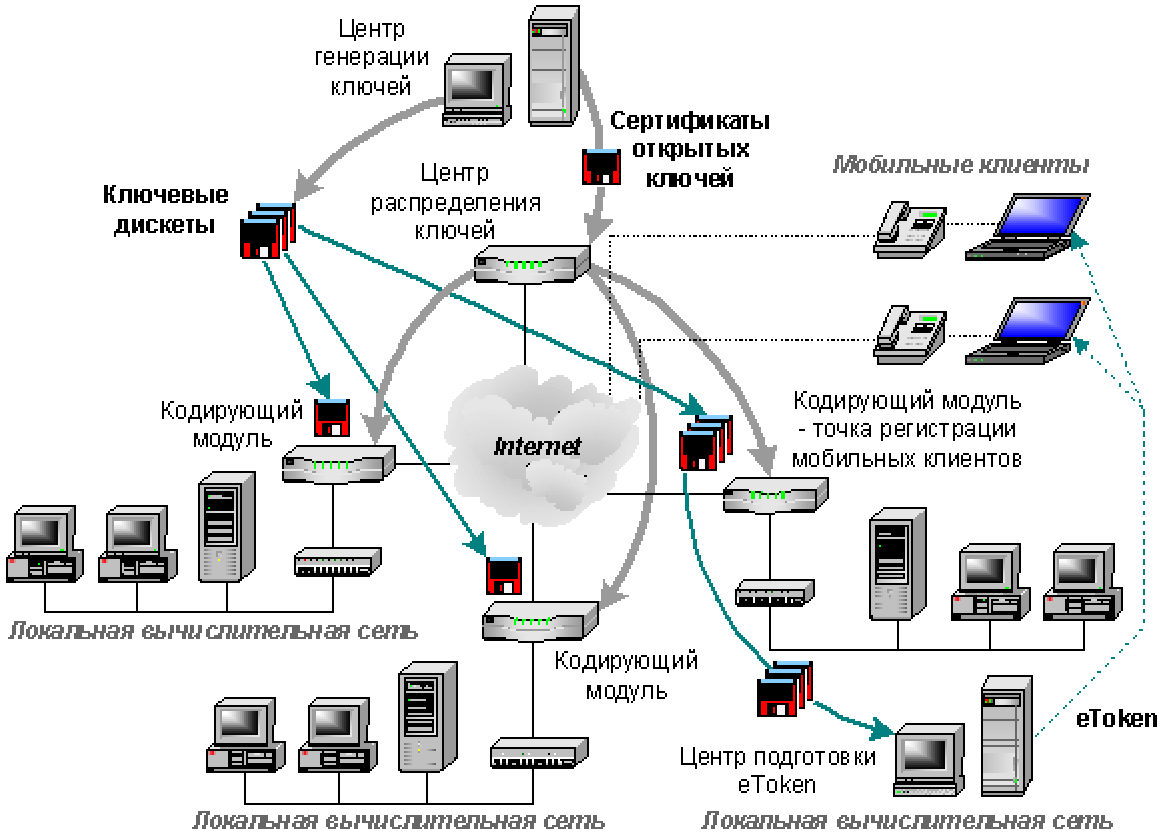
В состав виртуальной защищенной сети могут входить мобильные пользователи – удаленные компьютеры, подключаемые по выделенным или коммутируемым каналам связи. Основным отличием Мобильного клиента является динамически-назначаемый IP-адрес. Носителем ключевой информации для них является электронный ключ eToken.

Состав Комплекса «Тропа-Джет»

Комплекс «Тропа-Джет» состоит из следующих компонентов:

1. Набор шлюзов кодирования;
2. Центр генерации ключей;
3. Центр распределения ключей;
4. Центр регистрации мобильных клиентов;
5. Центр подготовки электронных ключей мобильных клиентов;
6. Мобильный клиент;
7. Центр мониторинга;
8. Программа контроля целостности.

Рисунок 1: Архитектура Комплекса кодирования межсетевых потоков «Тропа-Джет»



Шлюз с кодирующим/декодирующим модулем

Шлюз является основным модулем комплекса, выполняющим функции маршрутизации, фильтрации и кодирования пакетов. Каждый Шлюз предназначен для закрытия определенной группы локальных сетей. На компьютере-шлюзе устанавливается ядерный модуль с функциями кодирования и декодирования и запускается программа аутентификации. Функциями шлюза являются:

- Фильтрация трафика (деление на кодируемый/некодируемый потоки);
- Кодирование трафика (кодируемый поток);
- Аутентификация с другими Шлюзами;
- Регистрация событий в Центре мониторинга;
- Обеспечение собственной защиты.

Центр распределения ключей

Центр распределения ключей осуществляет управление контуром безопасности, а также выполняет следующие функции:

- Получение со сменного носителя открытых ключей Шлюзов;
- Выдача любому Шлюзу открытых ключей любых других Шлюзов и информации о соответствующих сегментах структуры сети;
- Рассылка Шлюзам сообщений об изменениях структуры закрытой сети;
- Выработка и выполнение процедуры смены сеансовых ключей;
- Хранение информации о структуре сети.

Центр реализован в виде программного комплекса, выполняющего функции хранения и выдачи открытых ключей кодирования по сетевому запросу от модулей кодирования. Центр распределения ключей может быть установлен либо на отдельном (выделенном) компьютере, либо совместно с одним из Шлюзов кодирования.

Центр генерации ключей

Данный модуль служит для генерации пар комплементарных ключей, а также является репозитарием всех известных системе ключей. В функции Центра генерации ключей входит:

- генерация пар открытого и секретного ключей Кодирующих модулей;
- генерация пары ключей для сертификации (эталонного заверения) открытых ключей Кодирующих модулей;
- генерация сертификатов открытых ключей, подписанных секретным ключом сертификации;
- помещение подписанных сертификатов открытых ключей на сменные носители;
- хранение эталонных копий сертифицированных открытых ключей в архиве.

Центр генерации ключей – программа, выполняющаяся на изолированном автоматизированном рабочем месте.

Центр регистрации ключей

Центр регистрации ключей служит репозитарием всех известных системе ключей. В его функции входит:

- Ввод со сменного носителя открытого ключа;
- Ввод со сменного носителя закрытого ключа Администратора безопасности;
- Подпись нового ключа ключом Администратора безопасности;
- Помещение подписанного открытого ключа в архив долговременного хранения и на сменный носитель;
- Хранение эталонных копий сертифицированных (зарегистрированных) открытых ключей.

Центр регистрации ключей выполнен в виде программы, выполняющейся на изолированном автоматизированном рабочем месте и предназначенной для сертификации (эталонного заверения) открытых ключей.

Центр регистрации мобильных клиентов и Мобильный клиент

Для обеспечения доступа к защищаемым корпоративным данным мобильных абонентов, не подключенных к защищаемым локальным сетям, используется Центр регистрации мобильных клиентов и программное обеспечение мобильного клиента комплекса «Тропа-Джет».

Центр регистрации мобильных клиентов представляет собой специальный кодирующий модуль для подключения произвольного количества мобильных клиентов.

Мобильный клиент представляет собой программный модуль, работающий под управлением ОС Windows 98/2000 и использующий аппаратные ключи для аутентификации абонента в VPN.

Центр мониторинга

Центр мониторинга представляет собой сетевое автоматизированное рабочее место с установленным на нем набором программ, осуществляющих сбор и анализ протоколов, поступающих от всех модулей комплекса.

Программа контроля целостности

Комплекс «Тропа-Джет» включает в себя средства формирования и проверки контрольных сумм файлов. Эти средства реализованы в виде Программы контроля целостности, которая предназначена для определения и уведомления системного Администратора об изменении, добавлении и удалении файлов.

Администрирование комплекса

Настройка и администрирование компонентов комплекса «Тропа-Джет» осуществляется централизованно с рабочего места Администратора безопасности с помощью графического интерфейса или командной строки. Удаленное управление осуществляется по защищенному каналу.

Комплекс обеспечивает аутентификацию Администраторов и разграничение доступа к функциям администрирования.

Основные особенности комплекса

Основными особенностями ККМП «Тропа-Джет» являются:

- Полнофункциональная схема управления ключами, позволяющая осуществлять динамическое распределение ключей с использованием доверенного центра сертификации, проверку подлинности ключевой информации и оповещение систем кодирования о компрометации ключей;
- Высокая надежность функционирования, обеспечиваемая средствами контроля целостности, протоколирования и аудита, устойчивости к сбоям и восстановления в случае сбоев и отказов;
- Прозрачность кодирования передаваемых данных для абонентов и используемого ими программного обеспечения;
- Высокая производительность (работа в сети 100 Мбит/с без существенного влияния на пропускную способность);
- Обеспечение требуемого качества сервиса (QoS) и поддержка работы с сервисами, предъявляющими высокие требования к величинам временных задержек (IP-телефония, видеоконференцсвязь);
- Различные варианты выбора платформ – функционирование под ОС Solaris на аппаратной платформе SPARC или Intel;
- Возможность использования в комплексе с межсетевыми экранами, антивирусными решениями и средствами контекстного анализа;
- Использование открытых стандартов – протокол туннелирования сетевых пакетов соответствует стандартам IETF IPsec.

Сертификация комплекса

ККМП "Тропа-Джет" имеет Сертификат N 00039743 от 22.12.1999 г. на соответствие требованиям ГОСТ Р ИСО/МЭК 9126-93, ГОСТ Р ИСО/МЭК ТО 9294-93 и Сертификат Гостехкомиссии N 466 от 14.06.2001 г. на соответствие Техническим условиям (создание защищенного информационного обмена между разнесенными локальными сетями) и отсутствие недекларированных возможностей.

Криптографическое ядро комплекса в настоящее время проходит сертификацию ФАПСИ на соответствие ГОСТ Р34.10-94 , ГОСТ Р34.11-94, ГОСТ 28147-89.

========