УДК 681.3

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ И ОРГАНИЗАЦИЯ САНКЦИОНИРОВАННОГО ДОСТУПА К РЕСУРСАМ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Студент гр.113024 С.С. Бойко,
канд. техн. наук В.А. Артамонов

Белорусский национальный технический университет

Опасности при работе в сети. Под подключением к сети понимают любое подключение компьютера к внешней среде для общения с другими ресурсами, когда уже нельзя быть полностью уверенным, что к этому компьютеру и информации в нем имеют доступ только пользователь компьютера или только санкционированные пользователи из сети.

- Если компьютер подключен к локальной сети, то, потенциально, к этому компьютеру и информации в нем можно получить несанкционированный доступ из локальной сети.
- Если локальную сеть соединили с другими локальными сетями, то к возможным несанкционированным пользователям добавляются и пользователи из этих удаленных сетей. Мы не будем говорить о доступности такого компьютера из сети или каналов, через которые соединили локальные сети, потому что наверняка на выходах из локальных сетей стоят устройства, осуществляющие шифрование и контроль трафика, и необходимые меры приняты.
- Если компьютер подключили напрямую через провайдера к внешней сети, например через модем к Интернет, для удаленного взаимодействия со своей локальной сетью, то компьютер и информация в нем потенциально доступны взломщикам из Интернет. А самое неприятное, что через этот компьютер возможен доступ взломщиков и к ресурсам локальной сети.

При всех таких подключениях применяются либо штатные средства разграничения доступа операционной системы, либо специализированные средства защиты от НСД, либо криптографические системы на уровне конкретных приложений, либо и то и другое вместе.

Однако все эти меры, к сожалению, не могут гарантировать желаемой безопасности при проведении сетевых атак, и объясняется это следующими основными причинами:

1. Операционные системы (ОС), особенно WINDOWS относятся к программным продуктам высокой сложности, созданием которых занимается большие коллективы разработчиков. Детальный анализ этих систем провести чрезвычайно трудно. В связи с чем, достоверно обосновать для них отсутствие штатных возможностей, ошибок или недоку-

ментированных возможностей, случайно или умышленно оставленных в ОС, и которыми можно было бы воспользоваться через сетевые атаки, не представляется возможным.

2. В многозадачной ОС, в частности WINDOWS, одновременно может работать много разных приложений, для которых также трудно обосновать отсутствие штатных возможностей, ошибок или недокументированных возможностей, позволяющих воспользоваться информационными ресурсами через сетевые атаки.
3. В современных системах присутствует масса разнообразных механизмов удаленной загрузки и запуска исполняемых программ, проконтролировать работу которых очень сложно.

Контроль трафика компьютеров. Выход здесь только один. Необходимо обеспечить на сетевом уровне тотальный контроль всего входящего и исходящего трафика компьютера, проходящего через все его сетевые интерфейсы. Под контролем мы понимаем:

1. Шифрование и имитозащита трафика между защищаемыми компьютерами. Тем самым одновременно с обеспечением конфиденциальности и достоверности передаваемой информации, ликвидация такой проблемы, как незащищенность IP-протокола от подделок сетевых и физических адресов и протоколов.
2. Фильтрация трафика по различным типам IP-протоколов, портам, сервисам и другим параметрам, протоколирование сеансов, то есть выполнение функций персонального Firewall.

При использовании средства защиты, обеспечивающего такой контроль:

- Уже невозможны сетевые атаки со стороны компьютеров, не владеющих соответствующей ключевой информацией.
- Трафик между парой компьютеров, связанных между собой, автоматически становится защищенным независимо от приложения, его создающего. Никакому третьему компьютеру этот трафик не доступен.
- Любой трафик защищенных компьютеров протоколируется, и любые отклонения в действиях зарегистрированных пользователей от стандартного поведения легко обнаруживаются, что является существенным сдерживающим моментом от проведения атак с их стороны. Кроме того, для зарегистрированных пользователей может также производиться фильтрация трафика, что не позволяет им выйти за пределы разрешенных протоколов.
- Может быть Обеспечена независимость защищенности компьютеров и информации и от сетевых администраторов, от ошибочных или преднамеренных действий которых любая сеть наиболее уязвима.
- Очень легко и быстро можно решить практически любые проблемы сетевой безопасности.

Многие решения VPN, имеющиеся на рынке сегодня, в основном ориентированы на защиту межсетевого трафика и возможность подключения к туннельным серверам удаленных пользователей с использованием некоторого клиента VPN. Такие решения по причинам, указанным выше не безопасны с точки зрения возможности организации несанкционированных доступов из подсоединяемых внешних локальных сетей или через удаленного клиента из внешних глобальных сетей (если нет персонального сетевого экрана). Кроме того, эти решения не рассчитаны на работу в локальных сетях, защиту их фрагментов или отдельных компьютеров, автоматизированное взаимодействие клиентов между собой. Поэтому такие решения мы сейчас рассматривать не будем, а остановимся на решениях обеспечивающих безопасность в предположении, что атаки могут осуществляться не только из внешних сетей, но и из локальных сетей.

По существу, мы говорим о построении виртуальных защищенных сетей (VPN) в более широком понимании, когда в их состав включаются и отдельные компьютеры (рабочие станции и сервера), находящиеся в локальной сети или удаленно подключаемые, фрагменты локальных сетей и локальные сети в целом.

Причем главное преимущество такой наложенной виртуальной сети, что ее развертывание практически не зависит от используемого телекоммуникационного оборудования, сетевого окружения.

Использование распределенной системы персональных и межсетевых экранов, обеспечивающих шифрование трафика, автоматически для любых информационных систем и приложений обеспечивает конфиденциальность и достоверность информации, защиту от сетевых атак, как из глобальных, так и из локальных сетей. Причем, без каких либо специальных проектных работ можно оперативно для любой возникающей проблемы безопасности решить вопрос защиты любого фрагмента сети или отдельного компьютера, не задумываясь при этом об используемых прикладных системах.

Рассмотрим возможные решения построения корпоративной сети с использованием технологии ViPNet, реализующей такие подходы к обеспечению сетевой безопасности.

Виртуальные сети внутри локальной сети. Внутри локальной сети путем установки ПО ViPNet [клиент] на различные рабочие станции и сервера могут быть созданы взаимно – недоступные виртуальные защищенные контура для обеспечения функционирования в единой телекоммуникационной среде различных по конфиденциальности или назначению информационных задач. Любой трафик между двумя компьютерами недоступен никому третьему из любой точки сети. Несанкционированный доступ из сети на защищенные компьютеры невозможен. ПО ViPNet [координатор] обеспечивает организацию работы виртуальной сети.

Внутри распределенной сети путем установки ПО ViPNet [клиент] на различные рабочие станции и сервера могут быть созданы взаимно – недоступные виртуальные защищенные контура для обеспечения функционирования в единой телекоммуникационной среде различных по конфиденциальности или назначению информационных задач (рис.1).

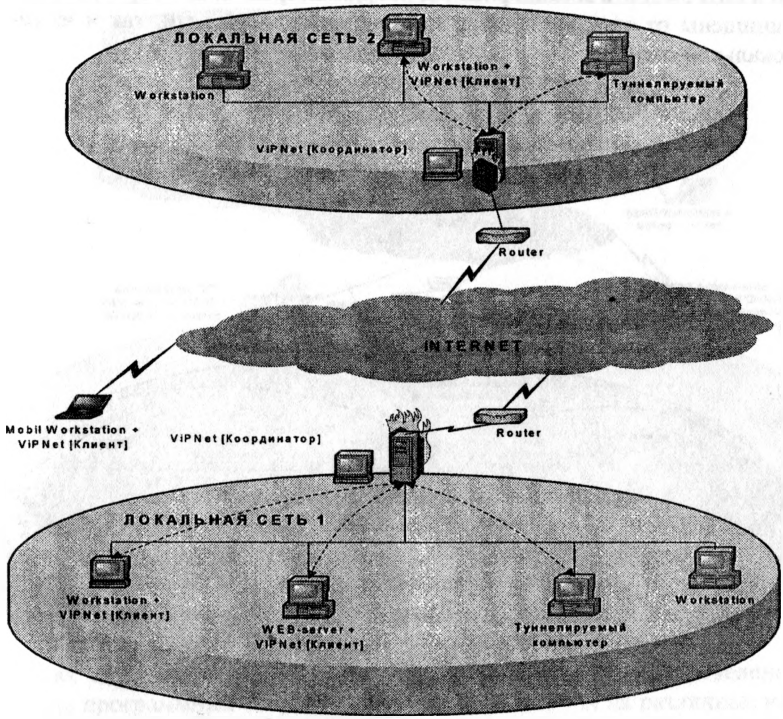

Рис.1. Соединение локальной сети с другой локальной сетью и удаленными пользователями

ViPNet [координаторы], установленные на входах в локальную сеть, обеспечивают как туннелирование (шифрование) трафика заданных адресов открытых компьютеров внутри локальной сети, так и организацию установки защищенного соединения непосредственно между компьютерами с ПО ViPNet[клиент]. Естественно во втором случае можно добиться полной защиты от возможных атак из подсоединяемой локальной сети.

Установка ПО ViPNet [клиент] на мобильный компьютер обеспечивает возможность его работы в корпоративной сети, при этом эффективные атаки на этот компьютер из внешней сети или через этот компьютер на локальные сети невозможны.

При необходимости защиты обращения к доверенным сегментам локальной сети такой сегмент (например, группа серверов) может быть спрятан также за ViPNet [координатор] (рис.2). Тогда обращение к этому сегменту снаружи будет происходить через два координатора, а при необходимости еще и через некоторый внешний Firewall, то есть обеспечивается возможность каскадирования координаторов. Такие обращения будут защищены от атак как снаружи данной локальной сети, так и из самой локальной сети.

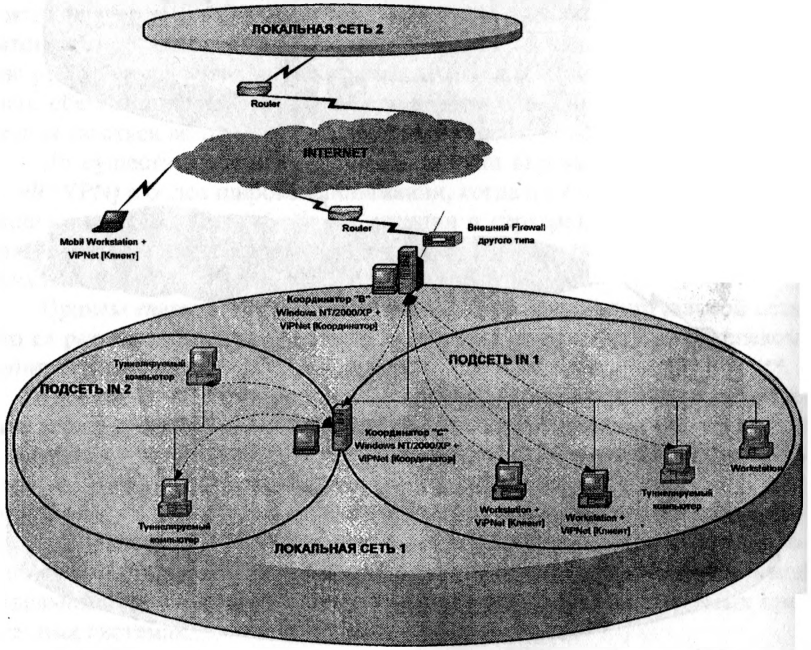

Рис.2. Защита сегментов локальной сети

Произвольная распределенная сеть. В распределенной сети любой конфигурации с любыми каналами связи и сетями может быть легко организована виртуальная защищенная сеть для безопасного и достоверного информационного взаимодействия.

Технология «Открытый Интернет» (рис.3). Путем установки на выходе из локальной сети специального ViPNet [координатора] (Координатор «D») внутри распределенной сети может быть организован виртуальный контур частично или полностью изолированный от остальной сети, компьютеры которого могут получать доступ к открытым ресурсам Интернет. При этом весь потенциально опасный открытый трафик из Ин-

тернет зашифровывается на Координаторе «D» и может быть расшифрован только на компьютерах локальной сети, включенных в этот виртуальный контур. Любые стратегии атак извне не могут нанести вреда остальным ресурсам локальной сети. ПО ViPNet [клиент] при работе станции в Интернет полностью блокирует любой иной трафик данной станции в локальной сети.

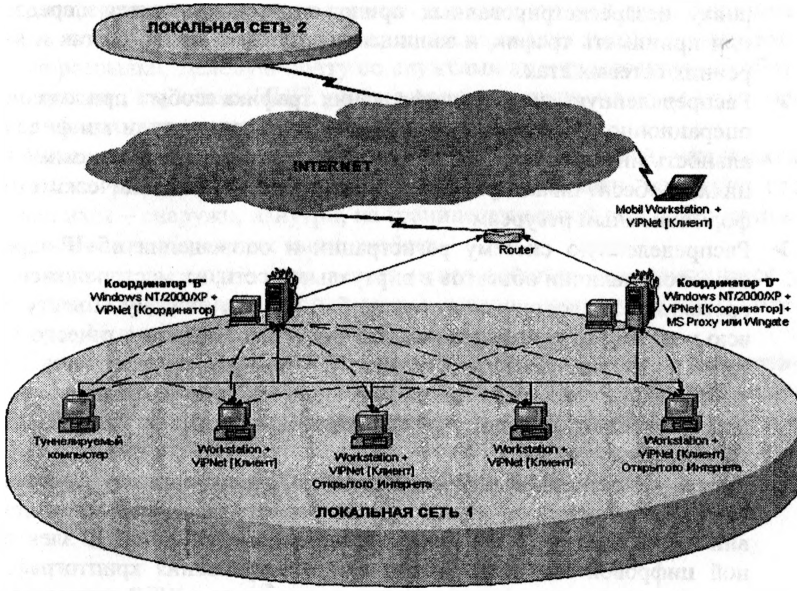

Рис.3. Технология «Открытый Интернет»

Как видно из приведенных примеров, установкой распределенной системы программных сетевых экранов и средств VPN на различные компьютеры можно добиться наиболее оптимальной и эффективной степени защиты ресурсов и информации в корпоративной сети от любых посягательств, исходя из важности информационного объекта и требуемой надежности защиты.

С использованием предлагаемой технологии легко также обеспечивается защита таких служб, как Voice IP, видео конференции, систем удаленного управления различными маршрутизаторами, цифровыми телефонными станциями, других систем удаленного управления и доступа.

Интегрированная виртуальная защищенная среда. Доверительность отношений, безопасность коммуникаций и технических средств, безопасность и достоверность информационных ресурсов в корпоративной сети, взаимодействующей также и с внешними техническими средст-

вами и информационными ресурсами, можно обеспечить только путем создания в телекоммуникационной инфраструктуре корпоративной сети интегрированной виртуальной защищенной среды, что и реализует технология ViPNet. Такая защищенная среда включает:

- Распределенную систему межсетевых и персональных сетевых экранов, обеспечивающих также контроль зарегистрированных и блокировку незарегистрированных приложений, пытающихся передавать или принимать трафик, и защищающую как от внешних, так и внутренних сетевых атак.
- Распределенную систему шифрования трафика любых приложений и операционной системы, гарантирующую целостность и конфиденциальность информации, как на внешних, так и внутренних коммуникациях, и обеспечивающую разграничение доступа к техническим и информационным ресурсам
- Распределенную систему регистрации и оповещения об IP-адресах объектов, наличии объектов в виртуальной сети, их местоположении и состоянии, предоставляющую в любой момент любому объекту сети всю необходимую информацию для возможности автоматического установления защищенных соединений. При этом не требуются какие либо ручные настройки для других объектов при их включении или перезагрузке, изменении у них IP-адресов, IP-адресов Firewall, за которыми установлены.
- Систему электронной цифровой подписи, обеспечивающую достоверность и юридическую значимость документов и совершаемых действий в соответствии с принятым Федеральным законом "Об электронной цифровой подписи". Возможность встраивания криптографических функций в другие приложения, в том числе в WEB-технологии, с поддержкой всей инфраструктуры безопасного ключевого управления обеспечивает возможность в полной мере воспользоваться криптографической подсистемой любым прикладным системам
- Безопасную для локальной сети систему организации виртуальных каналов доступа отдельных компьютеров локальной сети к открытым ресурсам внешних сетей (включая Интернет).
- Систему прозрачного шифрования информации при ее сохранении на сетевых и локальных жестких дисках, других носителях, обеспечивающую целостность и недоступность информации для несанкционированного использования в процессе ее хранения и обмена данными.
- Систему контроля и управления связями, правами и полномочиями объектов виртуальной среды, обеспечивающую автоматизированное управление политиками безопасности в корпоративной сети.
- Систему управления ключами, включающую подсистему распределения симметричных ключей, подсистему асимметричного распределе-

ния ключей (PKI) и управления цифровыми сертификатами.

- Систему межсетевого взаимодействия, обеспечивающую организацию связи между разными виртуальными сетями ViPNet путем взаимного согласования между администрациями сетей допустимых межобъектных связей и политик безопасности.
- Защищенные прикладные службы циркулярного обмена сообщениями и конференций в реальном времени в корпоративной сети. Защищенную, в том числе от вирусных атак, вызывающих несанкционированные рассылки, Деловую почту со службами автопроцессинга обработки файлов, службами ЭЦП, разграничения доступа к документам, поиска и архивирования документов.

Технология ViPNet – это набор программных модулей, установкой которых на различные компьютеры корпоративной сети, не важно где находящихся – снаружи, изнутри, на границе локальной сети, обеспечивается достижение указанных выше свойств.

При этом в полной мере может использоваться уже имеющееся у корпорации оборудование (компьютеры, сервера, маршрутизаторы, коммутаторы, Firewall и т.д.).

Программный комплекс ViPNet и отдельные его компоненты сертифицированы в Гостехкомиссии по классам 1В для автоматизированных систем, 3 классу для межсетевых экранов, 3 классу контроля НДВ и в ФАПСИ (криптоядро «Домен-К») по классам КС1 и КС2.