Защита информации при взаимодействии корпоративных сетей в Internet

***Александр Турский, Сергей Панов**, ОАО" Элвис+"*
"Экономика и производство", №10-12, 1999

Задача защиты информации стала уже неотъемлемым элементом любой автоматизированной системы, работающей с коммерчески значимой информацией. Широкое распространение Internet, intranet и extranet выдвигает решение проблем безопасности в ряд первоочередных и самых актуальных задач.
На опыте внедрения систем сетевой информационной безопасности ОАО ЭЛВИС+ был разработан общий концептуальный подход к задачам построения корпоративных систем. Суть предлагаемого решения заключается в следующих принципах:

- построение жесткого периметра корпоративной части сети на основе технологий виртуальных защищенных сетей (Virtual Private Network, VPN)
- обеспечение небольшого числа контролируемых точек открытого доступа в периметр корпоративной защищенной сети
- построение эшелонированной системы защиты с контролем проникновения в защищенный периметр,
- обеспечение дистанционного администрирования и аудита всех компонент системы защиты с глубокой проработкой вопросов событийного протоколирования и подотчетности пользователей, технического персонала, внешних абонентов.

Эти решения обеспечивают построение виртуальных закрытых сетей (intranet), их безопасную эксплуатацию и интеграцию с открытыми коммуникационными системами.

"Жесткая" защита сетевого уровня

Защита информации на *сетевом уровне* (рис. 1) имеет ряд преимуществ с архитектурной точки зрения. Сетевой уровень управления - это тот уровень, на котором сеть становится полносвязной системой. На более низких уровнях управления защита может быть реализована только как набор двухточечных защищенных звеньев. На сетевом уровне появляются возможность установления защищенного соединения между двумя компьютерами, расположенными в произвольных точках сети и понятие топологии; различаются внешние и внутренние каналы. На этом уровне реализуются такие возможности, как фильтрация трафика между внутренней (корпоративной) сетью и внешней коммуникационной средой, защита от несанкционированного доступа из внешней сети во внутреннюю, маскировка топологий внутренних сетей.
С другой стороны, сетевой уровень является достаточно низким уровнем управления для того, чтобы не оказывать существенного влияния на прикладные системы.

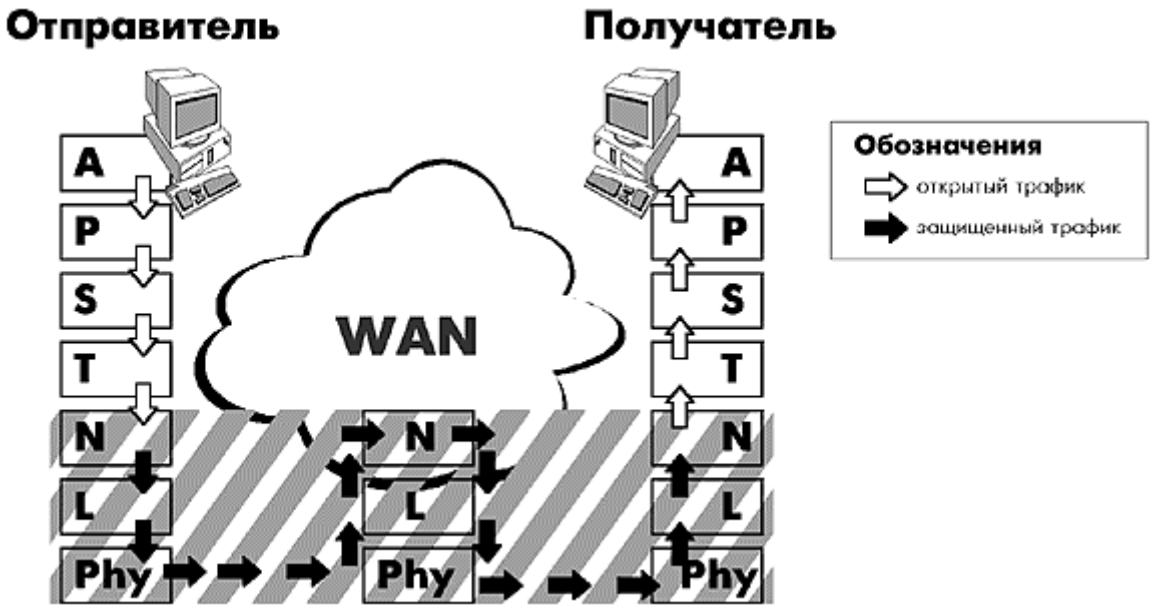

Рис. 1.
Высокая стойкость защиты сетевого уровня объясняется следующими ее характеристиками:

- основной агент системы защиты в виде драйвера операционной системы располагается между нижней частью IP-стека и аппаратно-зависимым драйвером сетевого адаптера; в этой точке существует уникальная возможность полного контроля всего входящего/исходящего трафика
- фильтрация обеспечивается низком уровне, где работает простой и компактный код драйвера, событийное пространство максимально сужено и нет возможности провести атаку через сервисы операционной системы
- автономные средства сетевой защиты могут быть конфигурированы только на транзитный трафик, что исключает прямую атаку непосредственно против средств защиты информации
- в случае применения средств защиты и/или аутентификации данных в защищенную сеть может войти только владелец 1024-битного разделяемого секрета
- обеспечиваются туннелирование и маскирование топологии ведомственной сети.

Безопасное взаимодействие с открытыми коммуникационными сетями

Защищенная корпоративная сеть в ряде случаев практически не может быть изолирована от внешних информационных систем (если только это не сеть специального назначения): людям необходимо обмениваться почтой, новостями, получать данные из внешних информационных источников; при этом не исключена атака на информационные ресурсы корпоративной сети в рамках этого информационного обмена.
Поэтому, наряду с построением виртуальной защищенной сети предприятия, другой важной проблемой защиты корпоративной сети является организация безопасного взаимодействия с открытыми сетями.
Концепция защищенной корпоративной сети ОАО ЭЛВИС+ состоит в том, чтобы закрыть трафик корпоративной сети средствами защиты информации сетевого уровня (построить виртуальную корпоративную сеть) и организовать фильтрацию информации в точках соединения с открытыми сетями. В качестве средств фильтрации информации на

интерфейсах с открытыми сетями применяются традиционные решения - межсетевой экран (firewall), сервисы защиты типа proxy (посредник).
Важным элементом защиты от несанкционированного проникновения в корпоративную сеть из открытой сети является последовательное (каскадное) включение нескольких фильтров-эшелонов защиты. Как правило, между открытой корпоративной сетью устанавливается т.н. зона контролируемого доступа (т.н."демилитаризованная зона", рис. 2).
В качестве внешнего и внутреннего фильтров применяются межсетевые экраны. Демилитаризованная зона представляет собой, как правило, сегмент сети, который характеризуется тем, что в нем представляются информационные ресурсы для доступа из открытой сети. При этом серверы, предоставляющие эти ресурсы для открытого доступа, конфигурируются специальным образом для того, чтобы на них не могли использоваться так называемые "опасные" сервисы (приложения), которые могут дать потенциальному нарушителю возможность реконфигурировать систему, компрометировать ее, и, опираясь на скомпрометированные ресурсы, атаковать корпоративную сеть. В демилитаризованной зоне могут располагаться некоторые серверы служебного обмена между корпоративной и открытой сетью. Кроме того, в демилитаризованной зоне (или в составе внешнего/внутреннего фильтров) часто используют посреднические (proxy) сервисы для усиления фильтрационных характеристик промежуточного сегмента между открытой и корпоративной сетью.

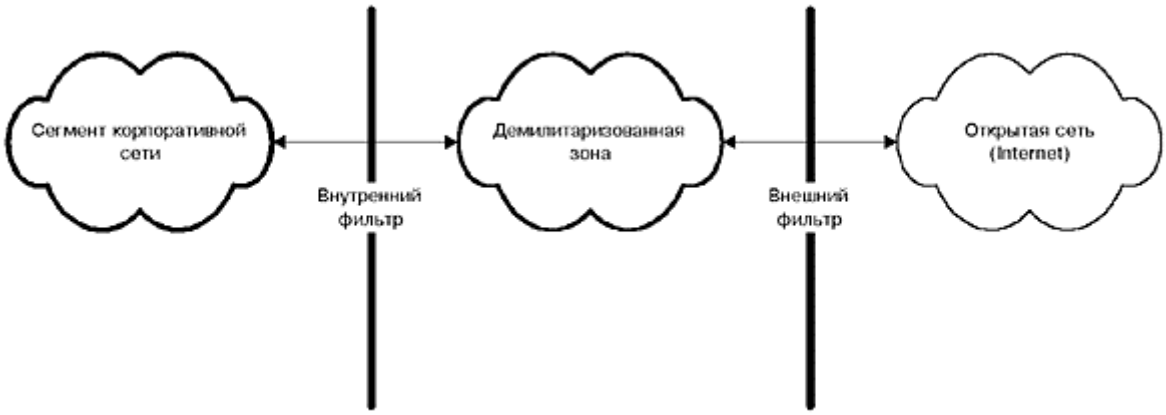

Рис. 2.
Наконец, в среде демилитаризованной зоны (как и в среде корпоративной сети) часто используются т.н. средства обнаружения нарушителя (intrusion detection). Назначение этих средств состоит в том, чтобы по косвенным признакам (таким, например, как аномалии сетевой активности) обеспечить обнаружение компрометации сети, которое может быть произведено в следствие, например, неправильного конфигурирования межсетевого экрана или вследствие ошибки программного обеспечения.
В решениях ОАО ЭЛВИС+ по организации взаимодействия с открытыми сетями (защите Internet-сегмента корпоративной сети) обычно применяются межсетевые экраны, обеспечивающие т.н. расширенную пакетную фильтрацию. . Такие пакетные экраны принимают "решение" о доступе каждого пакета на основе набора правил фильтрации, информации, содержащейся в пакете и на основе некоторой предыстории, которую "помнит" фильтрационная машина, настраиваемая на обмены в рамках конкретных протоколов (протокольный автомат). Перепрограммируемые протокольные автоматы поставляются для большинства распространенных протоколов (как дейтаграммых, так и для протоколов с установлением состояния).
Критерий фильтрации может быть основан на применении одного или нескольких правил фильтрации. Каждое правило формируется на основе применения операций отношения к таким элементам IP пакета, как:

- IP адрес источника/приемника пакета; эти правила позволяют разрешать или запрещать информационный обмен между некоторыми заданными узлами сети
- поле "протокол" (TCP, UDP, ICMP и проч.); правила фильтрации на основе этого поля регламентируют использование инкапсулируемых в IP протоколов
- поле "порт" для источника/приемника пакета; с понятием "порт" в стеке протоколов TCP/IP ассоциируется некоторое приложение, и правила этой группы могут разрешать/запрещать доступ к заданному узлу по заданному прикладному протоколу (зависимость правил фильтрации по IP-адресам для пар источник/приемник позволяет контролировать направление доступа)
- бинарные данные с заданным смещением относительно заголовка IP.

На практике межсетевые экраны часто представляют собой программный продукт, который устанавливается на вычислительную платформу с несколькими сетевыми интерфейсами и обеспечивает сегментирование (рис. 3) и независимую политику безопасности (набор правил фильтрации) для различных компьютеров в различных сегментах сети.
Централизованная архитектура системы, показанная на рис. 3, не противоречит "каскадной" схеме построения защиты. Политика доступа между сегментами настраивается как независимый набор правил фильтрации для каждой пары интерфейсов (сегментов корпоративной сети). В примере на рис. 3 можно предполагать следующую модельную настройку политики безопасности:

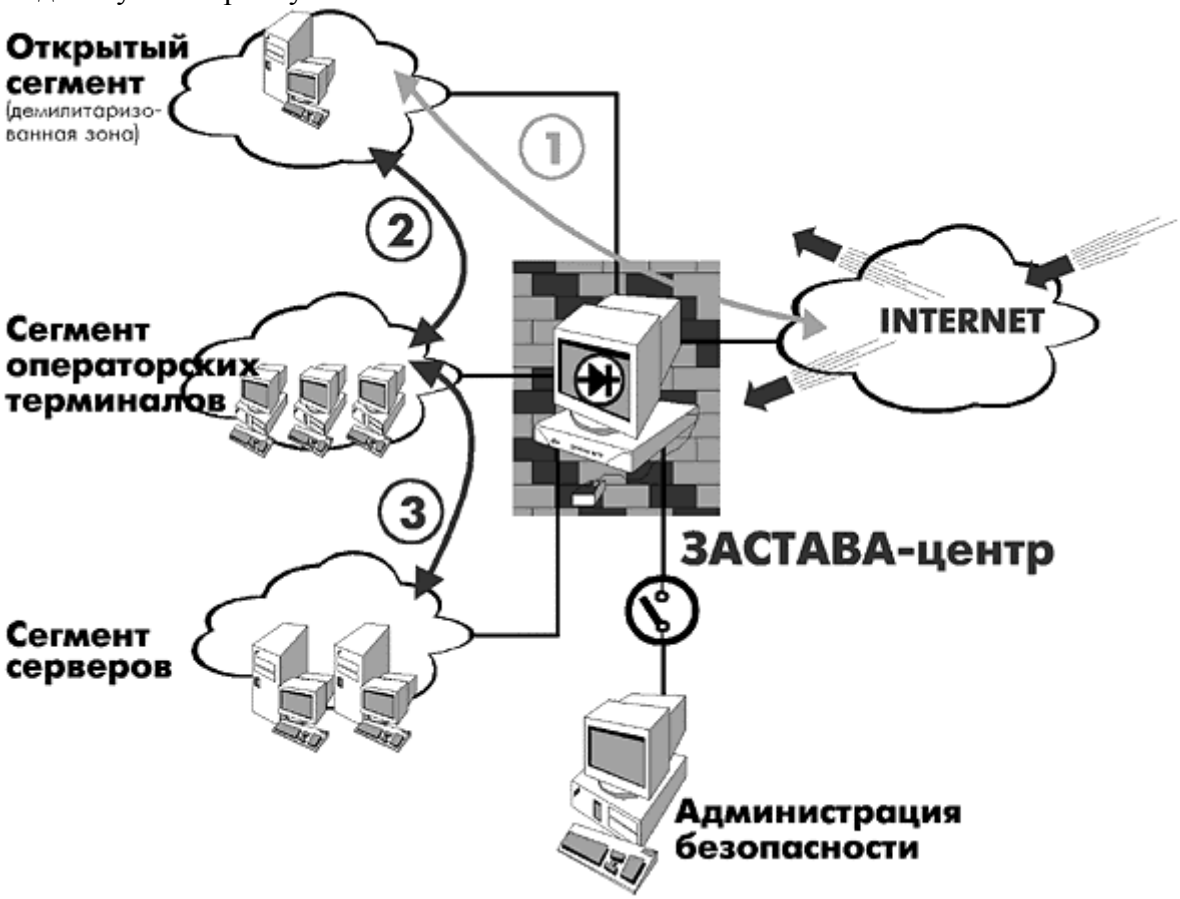

Рис. 3. Сегментирование корпоративной сети

- Внешние абоненты имеют доступ в открытый сегмент, например, на корпоративный Web-сервер, по определенному набору коммуникационных протоколов (фильтр 1).
- Пользователи корпоративной сети имеют доступ к информации высшей критичности, расположенной в сегменте серверов (фильтр 3), а также могут,

используя proxy-сервис в открытом сегменте, выходить в открытые сети (фильтры 2 и 1).
- Администирование безопасности производится дистанционно, обязательно с использованием средств защиты трафика.

В данном примере для атакующей стороны из внешней сети наиболее критичный ресурс (например, в сегменте серверов) может оказаться достижимым только при последовательной компрометации двух эшелонов защиты: демилитаризованной зоны и сегмента рабочих мест пользователей.

Программные продукты Элвис+ для защиты корпоративной сети

К настоящему времени компания ЭЛВИС+ закончила формирование целостного масштабируемого ряда продуктов для построения VPN (защищенных корпоративных сетей) на основанного на стандарте IPSec. Назначение продуктов данной линии заключается в обеспечении гибкого, масштабируемого решения для защиты и аутентификации трафика корпоративной сети и для защиты корпоративной сети от несанкционированного доступа. В состав продуктной линии входят клиентские агенты для защиты отдельных рабочих мест (персональных компьютеров), программные агенты для защиты серверных платформ, шлюзы для защиты входящего и исходящего трафика сегмента корпоративной сети.
Продукты работают на операционных платформах Windows 95, NT, Solaris (SPARC и Intel), кроме того, обеспечена совместимость в платформами, соответствующими стандарту UNIX SVR4.

ЗАСТАВА-Персональный клиент

Продукт является средством защиты рабочей станции, находящейся в персональной эксплуатации. Эта программа содержит все необходимые средства администрирования и конфигурирования, необходимые для взаимодействия этой программы с любыми другими IPSec-совместимыми средствами защиты.
Функции продукта:

- защита и аутентификация трафика, реализация заданной дисциплины работы индивидуально для каждого защищенного соединения, разрешение доступа в заданном режиме только для санкционированных станций; контроль списка партнеров по взаимодействиям, защита от НСД из сети
- настройка политики безопасности при помощи графического интерфейса продукта и/или при помощи внешне определенной конфигурации
- сбор статистики и сигнализация.

ЗАСТАВА-Корпоративный клиент

Продукт является средством защиты рабочей станции корпоративной сети. От предыдущего продукта эта программа отличается тем, что пользователь защищаемой рабочей станции лишен права (и возможности) единолично определять политику безопасности (и, следовательно, структуру сетевых соединений) для своей станции. Политика безопасности полностью контролируется администратором безопасности корпоративной сети и выдается пользователю как целостная структура данных на некотором носителе. Данные, определяющие политику безопасности, могут загружаться с

внешнего носителя (дискета, пластиковая карта) и существуют в защищаемом компьютере только в течение сеанса его работы, разрушаясь после прекращения работы компьютера.

ЗАСТАВА-Сервер

Продукт является функциональным аналогом продуктов семейства ЗАСТАВА-Клиент для серверных платформ, а отличается расширенными ресурсами для поддержания множественных соединений с клиентскими программными агентами.
ЗАСТАВА Сервер поддерживает защищенные соединения с мобильными пользователями, не имеющими фиксированных IP адресов.

ЗАСТАВА-Офис

ЗАСТАВА-Офис программный комплекс для коллективной защиты входящего и исходящего трафика сегмента локальной сети, защиты этого сегмента от несанкционированного доступа из внешний сетей, а также для обеспечения защищенного взаимодействия с другими сегментами локальных сетей путем туннелирования трафика.

Межсетевой экран ЗАСТАВА-Центр

Межсетевой экран ЗАСТАВА - программный комплекс, предназначенный для контроля за входящей и/или выходящей информацией и защиты автоматизированной системы предприятия от несанкционированного доступа с использованием расширенной пакетной фильтрации на сетевом и транспортном уровнях.
Межсетевой экран ЗАСТАВА предназначен для работы в операционных системах Solaris 2.5, 2.5.1, 2.6 или более поздних версий.
Функциональные возможности продукта:

- фильтрация на основе сетевых адресов отправителя и получателя;
- фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов;
- фильтрация запросов на транспортном уровне на установление виртуальных соединений. При этом учитываются транспортные адреса отправителя и получателя;
- фильтрация запросов на прикладном уровне к прикладным сервисам. При этом учитываются прикладные адреса отправителя и получателя;

Межсетевой экран ЗАСТАВА обеспечивает возможность идентификации и аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. Идентификация и аутентификация обеспечивается программными средствами с поддержкой протокола SKIP.
Межсетевой экран ЗАСТАВА обеспечивает:

- возможность регистрации и учета фильтруемых пакетов; в параметры регистрации включаются адрес, время и результат фильтрации;
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- идентификацию и аутентификацию администратора защиты при его локальных запросах на доступ;

В соответствии с Решением N126 Государственной технической комиссией при Президенте РФ от 22 мая 1997 года проведены работы по сертификации программного комплекса - межсетевого экрана "Застава" на соответствие требованиям ТУ и требованиям к третьему классу защищенности МЭ в соответствии с РД "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности". Сертификаты №145 от 9 января 1998 года для Solaris/SPARC и №155 от 24 февраля 1998 для Solaris/Intel.

Применение продуктов семейства ЗАСТАВА для задач защиты корпоративной сети

Продуктная линия ОАО ЭЛВИС+ функционально полна в том смысле, что решение может быть распространено на всю корпоративную сеть предприятия (организации) любого масштаба.

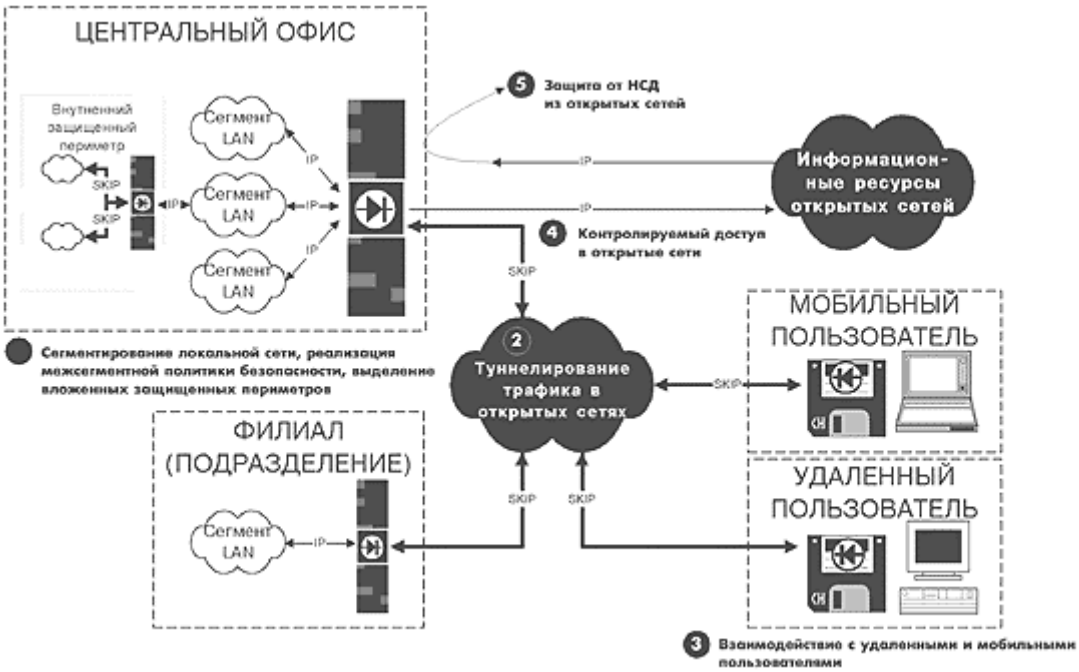

Рис. 5.

При этом может быть обеспечено решение следующих задач (рис. 5):

- построена надежная и прозрачная система защиты трафика от перехвата и фальсификации, как для связи между локальными сетями удаленных подразделений, так и для входа в корпоративную сеть уединенных удаленных (в том числе мобильных) пользователей, построения абонентских сетей
- обеспечен контроль сетевого доступа к информации (вплоть до обеспечения аутентифицированного доступа отдельных пользователей), построена эшелонированная система защиты от атак, осуществляемых методами сетевого доступа
- построены, при необходимости, система вложенных защищенных периметров, ориентированных на работу с информацией различной степени конфиденциальности
- построена система событийного протоколирования и аудита с обеспечением возможности оперативного мониторинга безопасности в масштабах корпоративной сети

- обеспечено централизованное дистанционное управление средствами сетевой защиты.

Развитие продуктной линии ЗАСТАВА предполагает решения по интеграции управления средствами защиты различных уровней, включая прикладной.