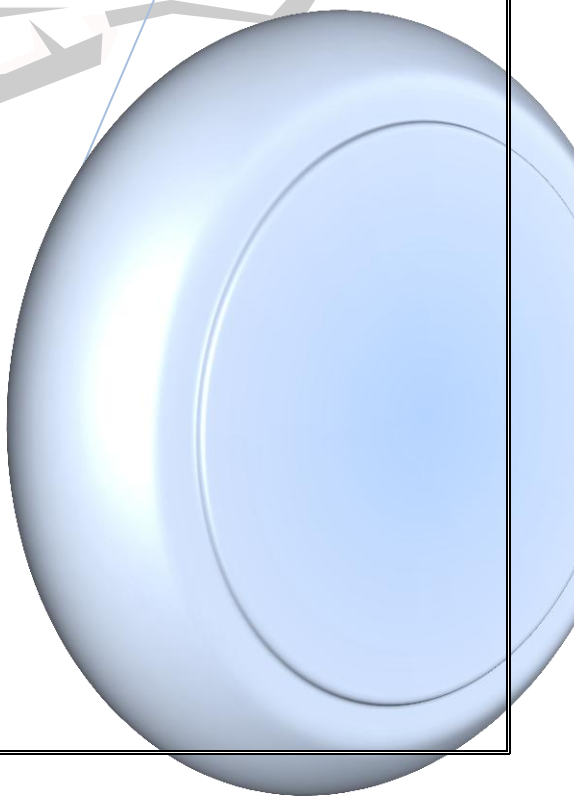
Сетевые атаки

Методы обнаружения сетевых атак

Часовникова Мария 11 «А» класс
2014 год



Оглавление

1. Обнаружение атак

Исторически так сложилось, что технологии, по которым строятся системы обнаружения атак, принято условно делить на две категории: обнаружение аномального поведения (anomaly detection) и обнаружение злоупотреблений (misuse detection). Однако в практической деятельности применяется другая классификация, учитывающая принципы практической реализации таких систем: обнаружение атак на уровне сети (network-based) и на уровне хоста (host-based). Первые системы анализируют сетевой трафик, в то время как вторые — регистрационные журналы операционной системы или приложения. Каждый из классов имеет свои достоинства и недостатки, но об этом чуть позже. Необходимо заметить, что лишь некоторые системы обнаружения атак могут быть однозначно отнесены к одному из названных классов. Как правило, они включают в себя возможности нескольких категорий. Тем не менее эта классификация отражает ключевые возможности, отличающие одну систему обнаружения атак от другой.

В настоящий момент технология обнаружения аномалий не получила широкого распространения, и ни в одной коммерчески распространяемой системе она не используется. Связано это с тем, что данная технология красиво выглядит в теории, но очень трудно реализуется на практике. Сейчас, однако, наметился постепенный возврат к ней (особенно в России), и можно надеяться, что в скором времени пользователи смогут увидеть первые коммерческие системы обнаружения атак, работающие по этой технологии.

Другой подход к обнаружению атак — обнаружение злоупотреблений, которое заключается в описании атаки в виде шаблона (pattern) или сигнатуры (signature) и поиска данного шаблона в контролируемом пространстве (сетевом трафике или журнале регистрации). Антивирусные системы являются ярким примером системы обнаружения атак, работающей по этой технологии.

Как уже было отмечено выше, существует два класса систем, обнаруживающих атаки на сетевом и операционном уровне. Принципиальное преимущество сетевых (network-based) систем обнаружения атак состоит в том, что они идентифицируют нападения прежде, чем те достигнут атакуемого узла. Эти системы более просты для развертывания в крупных сетях, потому что не требуют установки на различные платформы, используемые в организации. В России наибольшее распространение получили операционные системы MS-DOS, Windows 95, NetWare и Windows NT. Различные диалекты UNIX у нас пока не столь широко распространены, как на Западе. Кроме того, системы обнаружения атак на уровне сети практически не снижают производительности сети.

Системы обнаружения атак на уровне хоста создаются для работы под управлением конкретной операционной системы, что накладывает на них определенные ограничения. Например, мне не известна ни одна система этого класса, функционирующая под управлением MS-DOS или Windows for Workgroups (а ведь эти операционные системы еще достаточно распространены в России). Используя знание того, как должна «вести» себя операционная система, средства, построенные с учетом этого подхода, иногда могут обнаружить вторжения, пропускаемые сетевыми средствами обнаружения атак. Однако зачастую это достигается дорогой ценой, потому что постоянная регистрация, необходимая для выполнения подобного рода обнаружения, существенно снижает производительность защищаемого хоста. Такие системы сильно загружают процессор и требуют больших объемов дискового пространства для хранения журналов регистрации и, в принципе, не применимы для высококритичных систем, работающих в режиме реального времени (например, система «Операционный день банка» или система диспетчерского управления). Однако, несмотря ни на что, оба эти подхода могут быть применены для защиты вашей организации. Если вы хотите защитить один или несколько узлов, то системы обнаружения атак на уровне хоста могут стать неплохим выбором. Но если вы хотите защитить большую часть сетевых узлов организации, то системы обнаружения атак на уровне сети, вероятно, будут наилучшим выбором, поскольку увеличение количества узлов в сети никак не скажется на уровне защищенности, достигаемом при помощи системы обнаружения атак. Она сможет без дополнительной настройки защищать дополнительные узлы, в то время как в случае применения системы, функционирующей на уровне хостов, понадобится ее установка и настройка на каждый защищаемый хост. Идеальным решением стала бы система обнаружения атак, объединяющая в себе оба эти подхода. [1]i

Существующие сегодня на рынке коммерческие системы обнаружения атак (Intrusion Detection Systems, IDS) используют для распознавания и отражения атак либо сетевой, либо системный подход. В любом случае эти продукты ищут сигнатуры атак, специфические шаблоны, которые обычно указывают на враждебные или подозрительные действия. В случае поиска этих шаблонов в сетевом трафике, IDS работает на сетевом уровне. Если IDS ищет сигнатуры атак в журналах регистрации операционной системы или приложения, то это системный уровень. Каждый подход имеет свои достоинства и недостатки, но они оба дополняют друг друга. Наиболее

эффективной является система обнаружения атак, которая использует в своей работе обе технологии. В данном материале обсуждаются различия в методах обнаружения атак на сетевом и системном уровнях с целью демонстрации их слабых и сильных сторон. Также описываются варианты применения каждого из способов для наиболее эффективного обнаружения атак.

1.1. Обнаружение атак на сетевом уровне

Системы обнаружения атак сетевого уровня используют в качестве источника данных для анализа необработанные (raw) сетевые пакеты. Как правило, IDS сетевого уровня используют сетевой адаптер, функционирующий в режиме "прослушивания " (promiscuous), и анализируют трафик в реальном масштабе времени по мере его прохождения через сегмент сети. Модуль распознавания атак использует четыре широко известных метода для распознавания сигнатуры атаки:

Соответствие трафика шаблону (сигнатуре), выражению или байткоду, характеризующих об атаке или подозрительном действии;

Контроль частоты событий или превышение пороговой величины;

Корреляция нескольких событий с низким приоритетом;

Обнаружение статистических аномалий.

Как только атака обнаружена, модуль реагирования предоставляет широкий набор вариантов уведомления, выдачи сигнала тревоги и реализации контрмер в ответ на атаку. Эти варианты изменяются от системы к системе, но, как правило, включают в себя: уведомление администратора через консоль или по электронной почте, завершение соединения с атакующим узлом и/или запись сессии для последующего анализа и сбора доказательств.

1.2. Обнаружение атак на системном уровне

В начале 80-х годов, еще до того, как сети получили свое развитие, наиболее распространенная практика обнаружения атак заключалась в просмотре журналов регистрации на предмет наличия в них событий, свидетельствующих о подозрительной активности. Современные системы обнаружения атак системного уровня остаются мощным инструментом для понимания уже осуществленных атак и определения соответствующих методов для устранения возможностей их будущего применения. Современные IDS системного уровня по-прежнему используют журналы регистрации, но они стали более автоматизированными и включают сложнейшие методы обнаружения, основанные на новейших исследованиях в области математики. Как правило, IDS системного уровня контролируют систему, события и журналы регистрации событий безопасности (security log или syslog) в сетях, работающих под управлением Windows NT или Unix. Когда какой-либо из этих файлов изменяется, IDS сравнивает новые записи с сигнатурами атак, чтобы проверить, есть ли соответствие. Если такое соответствие найдено, то система посылает администратору сигнал тревоги или приводит в действие другие заданные механизмы реагирования.

IDS системного уровня постоянно развиваются, постепенно включая все новые и новые методы обнаружения. Один их таких популярных методов заключается в проверке контрольных сумм ключевых системных и исполняемых файлов через регулярные интервалы времени на предмет несанкционированных изменений. Своевременность реагирования непосредственно связана с частотой опроса. Некоторые продукты прослушивают активные порты и уведомляют администратора, когда кто-то пытается получить к ним доступ. Такой тип обнаружения вносит в операционную среду элементарный уровень обнаружения атак на сетевом уровне.

1.3. Достоинства систем обнаружения атак на сетевом уровне

IDS сетевого уровня имеют много достоинств, которые отсутствуют в системах обнаружения атак на системном уровне. В действительности, многие покупатели используют систему обнаружения атак сетевого

уровня из-за ее низкой стоимости и своевременного реагирования. Ниже представлены основные причины, которые делают систему обнаружение атак на сетевом уровне наиболее важным компонентом эффективной реализации политики безопасности.

Низкая стоимость эксплуатации. IDS сетевого уровня необходимо устанавливать в наиболее важных местах сети для контроля трафика, циркулирующего между многочисленных систем. Системы сетевого уровня не требуют, чтобы на каждом хосте устанавливалось программное обеспечение системы обнаружения атак. Поскольку для контроля всей сети число мест, в которых установлены IDS невелико, то стоимость их эксплуатации в сети предприятия ниже, чем стоимость эксплуатации систем обнаружения атак на системном уровне.

Обнаружение атак, которые пропускаются на системном уровне. IDS сетевого уровня изучают заголовки сетевых пакетов на наличие подозрительной или враждебной деятельности. IDS системного уровня не работают с заголовками пакетов, следовательно, они не могут определять эти типы атак. Например, многие сетевые атаки типа "отказ в обслуживании" ("denial-of-service") и "фрагментированный пакет" (TearDrop) могут быть идентифицированы только путем анализа заголовков пакетов, по мере того, как они проходят через сеть. Этот тип атак может быть быстро идентифицирован с помощью IDS сетевого уровня, которая просматривает трафик в реальном масштабе времени. IDS сетевого уровня могут исследовать содержание тела данных пакета, отыскивая команды или определенный синтаксис, используемые в конкретных атаках. Например, когда хакер пытается использовать программу Back Orifice на системах, которые пока еще не поражены ею, то этот факт может быть обнаружен путем исследования именно содержания тела данных пакета. Как говорилось выше, системы системного уровня не работают на сетевом уровне, и поэтому не способны распознавать такие атаки.

Для хакера более трудно удалить следы своего присутствия. IDS сетевого уровня используют "живой" трафик при обнаружении атак в реальном масштабе времени. Таким образом, хакер не может удалить следы своего присутствия. Анализируемые данные включают не только информацию о методе атаки, но и информацию, которая может помочь при идентификации злоумышленника и доказательстве в суде. Поскольку многие хакеры хорошо знакомы с журналами регистрации, они знают, как манипулировать этими файлами для скрытия следов своей деятельности, снижая эффективность систем системного уровня, которым требуется эта информация для того, чтобы обнаружить атаку.

Обнаружение и реагирование в реальном масштабе времени. IDS сетевого уровня обнаруживают подозрительные и враждебные атаки ПО МЕРЕ ТОГО, КАК ОНИ ПРОИСХОДЯТ, и поэтому обеспечивают гораздо более быстрое уведомление и реагирование, чем IDS системного уровня. Например, хакер, инициирующий атаку сетевого уровня типа "отказ в обслуживании" на основе протокола TCP, может быть остановлен IDS сетевого уровня, посылающей установленный флаг Reset в заголовке TCP-пакета для завершения соединения с атакующим узлом, прежде чем атака вызовет разрушения или повреждения атакуемого хоста. IDS системного уровня, как правило, не распознают атаки до момента соответствующей записи в журнал и предпринимают ответные действия уже после того, как была сделана запись. К этому моменту наиболее важные системы или ресурсы уже могут быть скомпрометированы или нарушена работоспособность системы, запускающей IDS системного уровня. Уведомление в реальном масштабе времени позволяет быстро среагировать в соответствии с предварительно определенными параметрами. Диапазон этих реакций изменяется от разрешения проникновения в режиме наблюдения для того, чтобы собрать информацию об атаке и атакующем, до немедленного завершения атаки.

Обнаружение неудавшихся атак или подозрительных намерений. IDS сетевого уровня, установленная с наружной стороны межсетевого экрана (МСЭ), может обнаруживать атаки, нацеленные на ресурсы за МСЭ, даже несмотря на то, что МСЭ, возможно, отразит эти попытки. Системы системного уровня не видят отраженных атак, которые не достигают хоста за МСЭ. Эта потерянная информация может быть наиболее важной при оценке и совершенствовании политики безопасности.

Независимость от ОС. IDS сетевого уровня не зависят от операционных систем, установленных в корпоративной сети. Системы обнаружения атак на системном уровне требуют конкретных ОС для правильного функционирования и генерации необходимых результатов.

1.4. Достоинства систем обнаружения атак системного уровня

И хотя системы обнаружения атак системного уровня не столь быстры, как их аналоги сетевого уровня, они предлагают преимущества, которых не имеют последние. К этим достоинствам можно отнести более строгий анализ, пристальное внимание к данным о событии на конкретном хосте и более низкая стоимость внедрения.

Подтверждают успех или отказ атаки. Поскольку IDS системного уровня используют журналы регистрации, содержащие данные о событиях, которые действительно имели место, то IDS этого класса могут с высокой точностью определять – действительно ли атака была успешной или нет. В этом отношении IDS системного уровня обеспечивают превосходное дополнение к системам обнаружения атак сетевого уровня. Такое объединение обеспечивает раннее предупреждение при помощи сетевого компонента и "успешность" атаки при помощи системного компонента.

Контролирует деятельность конкретного узла. IDS системного уровня контролирует деятельность пользователя, доступ к файлам, изменения прав доступа к файлам, попытки установки новых программ и/или попытки получить доступ к привилегированным сервисам. Например, IDS системного уровня может контролировать всю logon- и logoff-деятельность пользователя, а также действия, выполняемые каждым пользователем при подключении к сети. Для системы сетевого уровня очень трудно обеспечить такой уровень детализации событий. Технология обнаружения атак на системном уровне может также контролировать деятельность, которая обычно ведется только администратором. Операционные системы регистрируют любое событие, при котором добавляются, удаляются или изменяются учетные записи пользователей. IDS системного уровня могут обнаруживать соответствующее изменение сразу, как только оно происходит. IDS системного уровня могут также проводить аудит изменений политики безопасности, которые влияют на то, как системы осуществляют отслеживание в своих журналах регистрации и т.д.

В конечном итоге системы обнаружения атак на системном уровне могут контролировать изменения в ключевых системных файлах или исполняемых файлах. Попытки перезаписать такие файлы или инсталлировать "троянских коней" могут быть обнаружены и пресечены. Системы сетевого уровня иногда упускают такой тип деятельности.

Обнаружение атак, которые упускают системы сетевого уровня. IDS системного уровня могут обнаруживать атаки, которые не могут быть обнаружены средствами сетевого уровня. Например, атаки, осуществляемые с самого атакуемого сервера, не могут быть обнаружены системами обнаружения атак сетевого уровня.

Хорошо подходит для сетей с шифрованием и коммутацией. Поскольку IDS системного уровня устанавливается на различных хостах сети предприятия, она может преодолеть некоторые из проблем, возникающие при эксплуатации систем сетевого уровня в сетях с коммутацией и шифрованием.

Коммутация позволяет управлять крупномасштабными сетями, как несколькими небольшими сетевыми сегментами. В результате бывает трудно определить наилучшее место для установки IDS сетевого уровня. Иногда могут помочь административные порты (managed ports) и порты отражения (mirror ports, span ports) трафика на коммутаторах, но эти методы не всегда применимы. Обнаружение атак на системном уровне обеспечивает более эффективную работу в коммутируемых сетях, т.к. позволяет разместить IDS только на тех узлах, на которых это необходимо.

Определенные типы шифрования также представляют проблемы для систем обнаружения атак сетевого уровня. В зависимости от того, где осуществляется шифрование (канальное или абонентское), IDS сетевого уровня может остаться "слепой" к определенным атакам. IDS системного уровня не имеют этого ограничения. К тому же ОС, и, следовательно, IDS системного уровня, анализирует расшифрованный входящий трафик.

Обнаружение и реагирование почти в реальном масштабе времени. Хотя обнаружение атак на системном уровне не обеспечивает реагирования в действительно реальном масштабе времени, оно, при правильной реализации, может быть осуществлено почти в реальном масштабе. В отличие от устаревших систем, которые проверяют статус и содержания журналов регистрации через заранее определенные интервалы, многие современные IDS системного уровня получают прерывание от ОС, как только появляется новая запись в журнале регистрации. Эта новая запись может быть обработана сразу же, значительно уменьшая время между распознаванием атаки и реагированием на нее. Остается задержка между моментом записи операционной системой события в журнал регистрации и моментом распознавания ее системой обнаружения атак, но во многих случаях злоумышленник может быть обнаружен и остановлен прежде, чем нанесет какой-либо ущерб.

Не требуют дополнительных аппаратных средств. Системы обнаружения атак на системном уровне устанавливаются на существующую сетевую инфраструктуру, включая файловые сервера, Web-сервера и другие используемые ресурсы. Такая возможность может сделать IDS системного уровня очень эффективными по стоимости, потому что они не требуют еще одного узла в сети, которому необходимо уделять внимание, осуществлять техническое обслуживание и управлять им.

Низкая цена. Несмотря на то, что системы обнаружения атак сетевого уровня обеспечивают анализ трафика всей сети, очень часто они являются достаточно дорогими. Стоимость одной системы обнаружения атак может превышать $10000. С другой стороны, системы обнаружения атак на системном уровне стоят сотни долларов за один агент и могут приобретаться покупателем в случае необходимости контролировать лишь некоторые узлы предприятия, без контроля сетевых атак.

1.5. Необходимость в обеих системах обнаружения атак сетевого и системного уровней

Оба решения: IDS и сетевого, и системного уровней имеют свои достоинства и преимущества, которые эффективно дополняют друг друга. Следующее поколение IDS, таким образом, должно включать в себя интегрированные системные и сетевые компоненты. Комбинирование этих двух технологий значительно улучшит сопротивление сети к атакам и злоупотреблениям, позволит ужесточить политику безопасности и внести большую гибкость в процесс эксплуатации сетевых ресурсов.

Рисунок, представленный ниже, иллюстрирует то, как взаимодействуют методы обнаружения атак на системном и сетевом уровнях при создании более эффективной системы сетевой защиты. Одни события обнаруживаются только при помощи сетевых систем. Другие – только с помощью системных. Некоторые требуют применения обоих типов обнаружения атак для надежного обнаружения.

Рис.1. Взаимодействие метотодов обнаружения атак на системном и сетевом уровнях

1.6. Список требования к системам обнаружения атак следующего поколения

Характеристики для систем обнаружения атак следующего поколения:

Возможности обнаружения атак на системном и сетевом уровне, интегрированные в единую систему.

Совместно используемая консоль управления с непротиворечивым интерфейсом для конфигурации продукта, политики управления и отображения отдельных событий, как с системных, так и с сетевых компонентов системы обнаружения атак.

Интегрированная база данных событий.

Интегрированная система генерации отчетов.

Возможности осуществления корреляции событий.

Интегрированная он-лайновая помощь для реагирования на инциденты.

Унифицированные и непротиворечивые процедуры инсталляции.

Добавление возможности контроля за собственными событиями.

В четвертом квартале 1998 года вышла RealSecureT версии 3.0, которая отвечает всем этим требованиям.

Модуль слежения RealSecure - обнаруживает атаки на сетевом уровне в сетях Ethernet, Fast Ethernet, FDDI и Token Ring.

Агент RealSecure - обнаруживает атаки на серверах и других системных устройствах.

Менеджер RealSecure - консоль управления, которая обеспечивает конфигурацию модулей слежения и агентов RealSecure и объединяет анализ сетевого трафика и системных журналов регистрации в реальном масштабе времени. [2][ii]

2. Атаками весь мир полнится

Для защиты от разного рода атак можно применить две стратегии. Первая заключается в приобретении самых расхваливаемых (хотя не всегда самых лучших) систем защиты от всех возможных видов атак. Этот способ очень прост, но требует огромных денежных вложений. Ни один домашний пользователь или даже руководитель организации не пойдет на это. Поэтому обычно используется вторая стратегия, заключающаяся в предварительном анализе вероятных угроз и последующем выборе средств защиты от них.

Анализ угроз, или анализ риска, также может осуществляться двумя путями. Сложный, однако более эффективный способ заключается в том, что прежде, чем выбирать наиболее вероятные угрозы, осуществляется анализ информационный системы, обрабатываемой в ней информации, используемого программно-аппаратного обеспечения и т.д. Это позволит существенно сузить спектр потенциальных атак и тем самым повысить эффективность вложения денег в приобретаемые средства защиты. Однако такой анализ требует времени, средств и, что самое главное, высокой квалификации специалистов, проводящих инвентаризацию анализируемой сети. Немногие компании, не говоря уже о домашних пользователях, могут позволить себе пойти таким путем. Что же делать? Можно сделать выбор средств защиты на основе так называемых стандартных угроз, то есть тех, которые распространены больше всего. Несмотря на то что некоторые присущие защищаемой системе угрозы могут остаться без внимания, большая часть из них все же попадет в очерченные рамки. Какие же виды угроз и атак являются самыми распространенными? Ответу на этот вопрос и посвящена данная статья. Чтобы приводимые данные были более точны, я буду использовать статистику, полученную из различных источников.

Цифры, цифры, цифры…

Кто же чаще всего совершает компьютерные преступления и реализует различные атаки? Какие угрозы самые распространенные? Приведу данные, полученные самым авторитетным в этой области источником — Институтом компьютерной безопасности (CSI) и группой компьютерных нападений отделения ФБР в Сан-Франциско. Эти данные были опубликованы в марте 2000 года в ежегодном отчете «2000 CSI/FBI Computer Crime and Security Survey». Согласно этим данным:

90% респондентов (крупные корпорации и государственные организации) зафиксировали различные атаки на свои информационные ресурсы;

70% респондентов зафиксировали серьезные нарушения политики безопасности, например вирусы, атаки типа «отказ в обслуживании», злоупотребления со стороны сотрудников и т.д.;

74% респондентов понесли немалые финансовые потери вследствие этих нарушений.

За последние несколько лет также возрос объем потерь вследствие нарушений политики безопасности. Если в 1997 году сумма потерь равнялась 100 млн. долл., в 1999-м 124 млн., то в 2000-м эта цифра возросла до 266 млн. долл.. Размер потерь от атак типа «отказ в обслуживании» достиг 8,2 млн. долл. К другим интересным данным можно отнести источники атак, типы распространенных атак и размеры потерь от них .

Другой авторитетный источник — координационный центр CERT — также подтверждает эти данные. Кроме того, согласно собранным им данным, рост числа инцидентов, связанных с безопасностью, совпадает с распространением Internet.

Интерес к электронной коммерции будет способствовать усилению этого роста в последующие годы. Отмечена и другая тенденция. В 80-е — начале 90-х годов внешние злоумышленники атаковали узлы Internet из любопытства или для демонстрации своей квалификации. Сейчас атаки чаще всего преследуют финансовые или политические цели. Как утверждают многие аналитики, число успешных проникновений в информационные системы только в 1999 году возросло вдвое по сравнению с предыдущим годом (с 12 до 23%). И в 2000-м, и 2001-м годах эта тенденция сохраняется.

В данной области существует и российская статистика. И хотя она неполная и, по мнению многих специалистов, представляет собой лишь верхушку айсберга, я все же приведу эти цифры. За 2000 год, согласно

данным МВД, было зарегистрировано 1375 компьютерных преступлений. По сравнению с 1999 годом эта цифра выросла более чем в 1,6 раза. Данные управления по борьбе с преступлениями в сфере высоких технологий МВД РФ (Управление «Р») показывают, что больше всего преступлений — 584 от общего количества — относится к неправомерному доступу к компьютерной информации; 258 случаев — это причинение имущественного ущерба с использованием компьютерных средств; 172 преступления связано с созданием и распространением различных вирусов, а вернее, «вредоносных программ для ЭВМ»; 101 преступление — из серии «незаконное производство или приобретение с целью сбыта технических средств для незаконного получения информации», 210 — мошенничество с применением компьютерных и телекоммуникационных сетей; 44 — нарушение правил эксплуатации ЭВМ и их сетей. [3][iii]

3. Как защититься от удаленных атак в сети Internet?

Особенность сети Internet на сегодняшний день состоит в том, что 99% процентов информационных ресурсов сети являются общедоступными. Удаленный доступ к этим ресурсам может осуществляться анонимно любым неавторизованным пользователем сети. Примером подобного неавторизованного доступа к общедоступным ресурсам является подключение к WWW- или FTP-серверам, в том случае, если подобный доступ разрешен.

Определившись, к каким ресурсам сети Internet пользователь намерен осуществлять доступ, необходимо ответить на следующий вопрос: а собирается ли пользователь разрешать удаленный доступ из сети к своим ресурсам? Если нет, то тогда имеет смысл использовать в качестве сетевой ОС "чисто клиентскую" ОС (например, Windows '95 или NT Workstation), которая не содержит программ-серверов, обеспечивающих удаленный доступ, а, следовательно, удаленный доступ к данной системе в принципе невозможен, так как он просто программно не предусмотрен (например, ОС Windows '95 или NT, правда с одним но: под данные системы действительно нет серверов FTP, TELNET, WWW и т. д., но нельзя забывать про встроенную в них возможность предоставления удаленного доступа к файловой системе, так называемое разделение (share) ресурсов. А вспомнив по меньшей мере странную позицию фирмы Microsoft по отношению к обеспечению безопасности своих систем, нужно серьезно подумать, прежде чем остановить выбор на продуктах данной фирмы. Последний пример: в Internet появилась программа, предоставляющая атакующему несанкционированный удаленный доступ к файловой системе ОС Windows NT 4.0!). Выбор клиентской операционной системы во многом решает проблемы безопасности для данного пользователя (нельзя получить доступ к ресурсу, которого просто нет!). Однако в этом случае ухудшается функциональность системы. Здесь своевременно сформулировать, на наш взгляд, основную аксиому безопасности:

Аксиома безопасности. Принципы доступности, удобства, быстродействия и функциональности вычислительной системы антагонистичны принципам ее безопасности.

Данная аксиома, в принципе, очевидна: чем более доступна, удобна, быстра и многофункциональна ВС, тем она менее безопасна. Примеров можно привести массу. Например, служба DNS: удобно, но опасно.

Вернемся к выбору пользователем клиентской сетевой ОС. Это, кстати, один из весьма здравых шагов, ведущих к сетевой политике изоляционизма. Данная сетевая политика безопасности заключается в осуществлении как можно более полной изоляции своей вычислительной системы от внешнего мира. Также одним из шагов к обеспечению данной политики является, например, использование систем Firewall, позволяющих создать выделенный защищенный сегмент (например, приватную сеть), отделенный от глобальной сети. Конечно, ничто не мешает довести эту политику сетевого изоляционизма до абсурда - просто выдернуть сетевой кабель (полная изоляция от внешнего мира!). Не забывайте, это тоже "решение" всех проблем с удаленными атаками и сетевой безопасностью (в связи с полным отсутствием оных).

Итак, пусть пользователь сети Internet решил использовать для доступа в сеть только клиентскую сетевую ОС и осуществлять с помощью нее только неавторизованный доступ. Проблемы с безопасностью решены? Ничуть! Все было бы хорошо, если бы ни было так плохо. Для атаки "Отказ в обслуживании" абсолютно не имеет значения ни вид доступа, применяемый пользователем, ни тип сетевой ОС (хотя клиентская ОС с точки зрения защиты от атаки несколько предпочтительнее). Эта атака, используя фундаментальные пробелы в безопасности протоколов и инфраструктуры сети Internet, поражает сетевую ОС на хосте пользователя с одной единственной

целью - нарушить его работоспособность. ля атаки, связанной с навязыванием ложного маршрута при помощи протокола ICMP, целью которой является отказ в обслуживании, ОС Windows '95 или Windows NT - наиболее лакомая цель. Пользователю в таком случае остается надеяться на то, что его скромный хост не представляет никакого интереса для атакующего, который может нарушить его работоспособность разве что из желания просто напакостить.

3.1. Административные методы защиты от удаленных атак в сети Internet

Самым правильным шагом в этом направлении будет приглашение специалиста по информационной безопасности, который вместе с вами постарается решить весь комплекс задач по обеспечению требуемого необходимого уровня безопасности для вашей распределенной ВС. Это довольно сложная комплексная задача, для решения которой необходимо определить, что (список контролируемых объектов и ресурсов РВС), от чего (анализ возможных угроз данной РВС) и как (выработка требований, определение политики безопасности и выработка административных и программно-аппаратных мер по обеспечению на практике разработанной политики безопасности) защищать.

Пожалуй, наиболее простыми и дешевыми являются именно административные методы защиты от информационно-разрушающих воздействий.

3.1.1. Как защититься от анализа сетевого трафика?

Существует атака, позволяющая кракеру при помощи программного прослушивания канала передачи сообщений в сети перехватывать любую информацию, которой обмениваются удаленные пользователи, если по каналу передаются только нешифрованные сообщения. Также можно показать, что базовые прикладные протоколы удаленного доступа TELNET и FTP не предусматривают элементарную криптозащиту передаваемых по сети даже идентификаторов (имен) и аутентификаторов (паролей) пользователей. Поэтому администраторам сетей, очевидно, можно порекомендовать не допускать использование этих базовых протоколов для предоставления удаленного авторизованного доступа к ресурсам своих систем и считать анализ сетевого трафика той постоянно присутствующей угрозой, которую невозможно устранить, но можно сделать ее осуществление по сути бессмысленным, применяя стойкие криптоалгоритмы защиты IP-потока.

3.1.2. Как защититься от ложного ARP-сервера?

В том случае, если у сетевой ОС отсутствует информация о соответствии IP- и Ethernet-адресов хостов внутри одного сегмента IP-сети, данный протокол позволяет посылать широковещательный ARP-запрос на поиск необходимого Ethernet-адреса, на который атакующий может прислать ложный ответ, и, в дальнейшем, весь трафик на канальном уровне окажется перехваченным атакующим и пройдет через ложный ARP-сервер. Очевидно, что для ликвидации данной атаки необходимо устранить причину, по которой возможно ее осуществление. Основная причина успеха данной удаленной атаки - отсутствие необходимой информации у ОС каждого хоста о соответствующих IP- и Ethernet-адресах всех остальных хостов внутри данного сегмента сети. Таким образом, самым простым решением будет создание сетевым администратором статической ARP-таблицы в виде файла (в ОС UNIX обычно /etc/ethers), куда необходимо внести соответствую-щую информацию об адресах. Данный файл устанавливается на каждый хост внутри сегмента, и, следовательно, у сетевой ОС отпадает необходимость в использовании удаленного ARP-поиска.

3.1.3. Как защититься от ложного DNS-сервера?

Использование в сети Internet службы DNS в ее нынешнем виде может позволить кракеру получить глобальный контроль над соединениями путем навязывания ложного маршрута через хост кракера - ложный DNS-сервер. Осуществление этой удаленной атаки, основанной на потенциальных уязвимостях службы DNS, может привести к катастрофическим последствиям для огромного числа пользователей Internet и стать причиной массового нарушения информационной безопасности данной глобальной сети. В следующих двух пунктах

предлагаются возможные административные методы по предотвращению или затруднению данной удаленной атаки для администраторов и пользователей сети и для администраторов DNS-серверов.

а) Как администратору сети защититься от ложного DNS-сервера?

Если отвечать на этот вопрос коротко, то никак. Ни административно, ни программно нельзя защититься от атаки на существующую версию службы DNS. Оптимальным с точки зрения безопасности решением будет вообще отказаться от использования службы DNS в вашем защищенном сегменте! Конечно, совсем отказаться от использования имен при обращении к хостам для пользователей будет очень не удобно. Поэтому можно предложить следующее компромиссное решение: использовать имена, но отказаться от механизма удаленного DNS-поиска. Вы правильно догадались, что это возвращение к схеме, использовавшейся до появления службы DNS с выделенными DNS-серверами. Тогда на каждой машине в сети существовал hosts файл, в котором находилась информация о соответствующих именах и IP-адресах всех хостов в сети. Очевидно, что на сегодняшний день администратору можно внести в подобный файл информацию о лишь наиболее часто посещаемых пользователями данного сегмента серверах сети. Поэтому использование на практике данного решения чрезвычайно затруднено и, видимо, нереально (что, например, делать с броузерами, которые используют URL с именами?).

Для затруднения осуществления данной удаленной атаки можно предложить администраторам использовать для службы DNS вместо протокола UDP, который устанавливается по умолчанию, протокол TCP (хотя из документации далеко не очевидно, как его сменить). Это существенно затруднит для атакующего передачу на хост ложного DNS-ответа без приема DNS-запроса.

Общий неутешительный вывод таков: в сети Internet при использовании существующей версии службы DNS не существует приемлемого решения для защиты от ложного DNS-сервера (и не откажешься, как в случае с ARP, и использовать опасно)!

б) Как администратору DNS-сервера защититься от ложного DNS-сервера?

Если отвечать на этот вопрос коротко, то, опять же, никак. Единственным способом затруднить осуществление данной удаленной атаки, это использовать для общения с хостами и с другими DNS-серверами только протокол TCP, а не UDP. Тем не менее, это только затруднит выполнение атаки - не забывайте как про возможный перехват DNS-запроса, так и про возможность математического предсказания начального значения TCP-идентификатора ISN.

В заключение можно порекомендовать для всей сети Internet поскорее перейти либо к новой более защищенной версии службы DNS, либо принять единый стандарт на защищенный протокол. Сделать этот переход, несмотря на все колоссальные расходы, просто необходимо, иначе сеть Internet может быть просто поставлена на колени перед всевозрастающими успешными попытками нарушения ее безопасности при помощи данной службы!

3.1.4. Как защититься от навязывания ложного маршрута при использовании протокола ICMP?

Атака, которая заключалась в передаче на хост ложного ICMP Redirect сообщения о смене исходного маршрута приводила как к перехвату атакующим информации, так и к нарушению работоспособности атакуемого хоста. Для того, чтобы защититься от данной удаленной атаки, необходимо либо фильтровать данное сообщение (используя Firewall или фильтрующий маршрутизатор), не допуская его попадания на конечную систему, либо соответствующим образом выбирать сетевую ОС, которая будет игнорировать это сообщение. Однако обычно не существует административных способов повлиять на сетевую ОС так, чтобы запретить ей изменять маршрут и реагировать на данное сообщение. Единственный способ, например, в случае ОС Linux или FreeBSD заключается в том, чтобы изменить исходные тексты и перекомпилировать ядро ОС. Очевидно, что такой экзотический для многих способ возможен только для свободно распространяемых вместе с исходными текстами операционных систем. Обычно на практике не существует иного способа узнать реакцию используемой у вас ОС на ICMP Redirect сообщение, как послать данное сообщение и посмотреть, каков будет результат. Эксперименты показали, что данное сообщение позволяет изменить маршрутизацию на ОС Linux 1.2.8, Windows '95 и Windows NT 4.0. Следует

отметить, что продукты компании Microsoft не отличаются особой защищенностью от возможных удаленных атак, присущих IP-сетям. Следовательно, использовать данные ОС в защищенном сегменте IP-сети представляется нежелательным. Это и будет тем самым административным решением по защите сегмента сети от данной удаленной атаки.

3.1.5. Как защититься от отказа в обслуживании?

Нет и не может быть приемлемых способов защиты от отказа в обслуживании в существующем стандарте IPv4 сети Internet. Это связано с тем, что в данном стандарте невозможен контроль за маршрутом сообщений. Поэтому невозможно обеспечить надежный контроль за сетевыми соединениями, так как у одного субъекта сетевого взаимодействия существует возможность занять неограниченное число каналов связи с удаленным объектом и при этом остаться анонимным. Из-за этого любой сервер в сети Internet может быть полностью парализован при помощи удаленной атаки.

Единственное, что можно предложить для повышения надежности работы системы, подвергаемой данной атаке, - это использовать как можно более мощные компьютеры. Чем больше число и частота работы процессоров, чем больше объем оперативной памяти, тем более надежной будет работа сетевой ОС, когда на нее обрушится направленный "шторм" ложных запросов на создание соединения. Кроме того, необходимо использование соответствующих вашим вычислительным мощностям операционных систем с внутренней очередью, способной вместить большое число запросов на подключение. Ведь от того, что вы, например, поставите на суперЭВМ операционную систему Linux или Windows NT, у которых длина очереди для одновременно обрабатываемых запросов около 10, а тайм-аут очистки очереди несколько минут, то, несмотря на все вычислительные мощности компьютера, ОС будет полностью парализована атакующим.

3.1.6. Как защититься от подмены одной из сторон при взаимодействии с использованием базовых протоколов семейства TCP/IP

Как отмечалось ранее, единственным базовым протоколом семейства TCP/IP, в котором изначально предусмотрена функция обеспечения безопасности соединения и его абонентов, является протокол транспортного уровня - протокол TCP. Что касается базовых протоколов прикладного уровня: FTP, TELNET, r-служба, NFS, HTTP, DNS, SMTP, то ни один из них не предусматривает дополнительную защиту соединения на своем уровне и оставляет решение всех проблем по обеспечению безопасности соединения протоколу более низкого транспортного уровня - TCP. Однако, вспомнив о возможных атаках на TCP-соединение, рассмотренных в п. 4.5, где было отмечено, что при нахождении атакующего в одном сегменте с целью атаки защититься от подмены одного из абонентов TCP-соединения в принципе невозможно, а в случае нахождения в разных сегментах из-за возможности математического предсказания идентификатора TCP-соединения ISN также реальна подмена одного из абонентов, несложно сделать вывод, что при использовании базовых протоколов семейства TCP/IP обеспечить безопасность соединения практически невозможно! Это происходит из-за того, что, к сожалению, все базовые протоколы сети Internet с точки зрения обеспечения информационной безопасности невероятно устарели.

Единственно, что можно порекомендовать сетевым администраторам для защиты только от межсегментных атак на соединения - в качестве базового "защищенного" протокола использовать протокол TCP и сетевые ОС, в которых начальное значение идентификатора TCP-соединения действительно генерируется случайным образом (неплохой псевдослучайный алгоритм генерации используется в последних версиях ОС FreeBSD).

3.2. Программно-аппаратные методы защиты от удаленных атак в сети Internet

К программно-аппаратным средствам обеспечения информационной безопасности средств связи в вычислительных сетях относятся:

аппаратные шифраторы сетевого трафика;

методика Firewall, реализуемая на базе программно-аппаратных средств;

защищенные сетевые криптопротоколы;

программно-аппаратные анализаторы сетевого трафика;

защищенные сетевые ОС.

Существует огромное количество литературы, посвященной этим средствам защиты, предназначенным для использования в сети Internet (за последние два года практически в каждом номере любого компьютерного журнала можно найти статьи на эту тему).

Далее мы, по возможности кратко, чтобы не повторять всем хорошо известную информацию, опишем данные средства защиты, применяемые в Internet. При этом мы преследуем следующие цели: во-первых, еще раз вернемся к мифу об "абсолютной защите" , которую якобы обеспечивают системы Firewall, очевидно, благодаря стараниям их продавцов; во-вторых, сравним существующие версии криптопротоколов, применяемых в Internet, и дадим оценку, по сути, критическому положению в этой области; и, в-третьих, ознакомим читателей с возможностью защиты с помощью сетевого монитора безопасности, предназначенного для осуществления динамического контроля за возникающими в защищаемом сегменте IP-сети ситуациями, свидетельствующими об осуществлении на данный сегмент одной из описанных в 4 главе удаленных атак.

3.2.1. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети

В общем случае методика Firewall реализует следующие основные три функции:

1. Многоуровневая фильтрация сетевого трафика.

Фильтрация обычно осуществляется на трех уровнях OSI:

сетевом (IP);

транспортном (TCP, UDP);

прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика является основной функцией систем Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте IP-сети, то есть, настроив соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящихся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной ОС, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к Firewall-фильтрации: в качестве субъектов взаимодействия будут выступать IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.

2. Proxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте.

Proxy-схема позволяет, во-первых, при доступе к защищенному Firewall сегменту сети осуществить на нем дополнительную идентификацию и аутентификацию удаленного пользователя и, во-вторых, является основой для создания приватных сетей с виртуальными IP-адресами. Смысл proxy-схемы состоит в создании соединения с конечным адресатом через промежуточный proxy-сервер (proxy от англ. полномочный) на хосте Firewall. На этом proxy-сервере и может осуществляться дополнительная идентификация абонента.

3. Создание приватных сетей (Private Virtual Network - PVN) с "виртуальными" IP-адресами (NAT - Network Address Translation).

В том случае, если администратор безопасности сети считает целесообразным скрыть истинную топологию своей внутренней IP-сети, то ему можно порекомендовать использовать системы Firewall для создания приватной сети (PVN-сеть). Хостам в PVN-сети назначаются любые "виртуальные" IP-адреса. Для адресации во внешнюю сеть (через Firewall) необходимо либо использование на хосте Firewall описанных выше proxy-серверов, либо применение специальных систем роутинга (маршрутизации), только через которые и возможна внешняя адресация. Это происходит из-за того, что используемый во внутренней PVN-сети виртуальный IP-адрес, очевидно, не пригоден для внешней адресации (внешняя адресация - это адресация к абонентам, находящимся за пределами PVN-сети). Поэтому proxy-сервер или средство роутинга должно осуществлять связь с абонентами из внешней сети со своего настоящего IP-адреса. Кстати, эта схема удобна в том случае, если вам для создания IP-сети выделили недостаточное количество IP-адресов (в стандарте IPv4 это случается сплошь и рядом, поэтому для создания полноценной IP-сети с использованием proxy-схемы достаточно только одного выделенного IP-адреса для proxy-сервера).

Итак, любое устройство, реализующее хотя бы одну из этих функций Firewall-методики, и является Firewall-устройством. Например, ничто не мешает вам использовать в качестве Firewall-хоста компьютер с обычной ОС FreeBSD или Linux, у которой соответствующим образом необходимо скомпилировать ядро ОС. Firewall такого типа будет обеспечивать только многоуровневую фильтрацию IP-трафика. Другое дело, предлагаемые на рынке мощные Firewall-комплексы, сделанные на базе ЭВМ или мини-ЭВМ, обычно реализуют все функции Firewall-мето-дики и являются полнофункциональными системами Firewall. На следующем рисунке изображен сегмент сети, отделенный от внешней сети полнофункциональным Firewall-хостом.

Однако администраторам IP-сетей, поддавшись на рекламу систем Firewall, не стоит заблуждаться на тот счет, что Firewall это гарантия абсолютной защиты от удаленных атак в сети Internet. Firewall - не столько средство обеспечения безопасности, сколько возможность централизованно осуществлять сетевую политику разграничения удаленного доступа к доступным ресурсам вашей сети. Да, в том случае, если, например, к данному хосту запрещен удаленный TELNET-доступ, то Firewall однозначно предотвратит возможность данного доступа. Но дело в том, что большинство удаленных атак имеют совершенно другие цели (бессмысленно пытаться получить определенный вид доступа, если он запрещен системой Firewall). Какие из рассмотренных удаленных атак может предотвратить Firewall? Анализ сетевого трафика? Очевидно, нет! Ложный ARP-сервер? И да, и нет (для защиты вовсе не обязательно использовать Firewall). Ложный DNS-сервер? Нет, к сожалению, Firewall вам тут не помощник. Навязывание ложного маршрута при помощи протокола ICMP? Да, эту атаку путем фильтрации ICMP-сообщений Firewall легко отразит (хотя достаточно будет фильтрующего маршрутизатора, например Cisco). Подмена одного из субъектов TCP-соединения? Ответ отрицательный; Firewall тут абсолютно не при чем. Нарушение работоспособности хоста путем создания направленного шторма ложных запросов или переполнения очереди запросов? В этом случае применение Firewall только ухудшит все дело. Атакующему для того, чтобы вывести из строя (отрезать от внешнего мира) все хосты внутри защищенного Firewall-системой сегмента, достаточно атаковать только один Firewall, а не несколько хостов (это легко объясняется тем, что связь внутренних хостов с внешним миром возможна только через Firewall).

Из всего вышесказанного отнюдь не следует, что использование систем Firewall абсолютно бессмысленно. Нет, на данный момент этой методике (именно как методике!) нет альтернативы. Однако надо четко понимать и помнить ее основное назначение. Нам представляется, что применение методики Firewall для обеспечения сетевой безопасности является необходимым, но отнюдь не достаточным условием, и не нужно считать, что, поставив Firewall, вы разом решите все проблемы с сетевой безопасностью и избавитесь от всех возможных удаленных атак из сети Internet. Прогнившую с точки зрения безопасности сеть Internet никаким отдельно взятым Firewall'ом не защитишь!

Из всего вышесказанного отнюдь не следует, что использование систем Firewall абсолютно бессмысленно. Нет, на данный момент этой методике (именно как методике!) нет альтернативы. Однако надо четко понимать и помнить ее основное назначение. Нам представляется, что применение методики Firewall для обеспечения сетевой безопасности является необходимым, но отнюдь не достаточным условием, и не нужно считать, что, поставив Firewall, вы разом решите все проблемы с сетевой безопасностью и избавитесь от всех возможных удаленных атак из сети Internet. Прогнившую с точки зрения безопасности сеть Internet никаким отдельно взятым Firewall'ом не защитишь!

3.2.2. Программные методы защиты, применяемые в сети Internet

К программным методам защиты в сети Internet можно отнести прежде всего защищенные криптопротоколы, с использованием которых появляется возможность надежной защиты соединения. В

следующем пункте пойдет речь о существующих на сегодняшний день в Internet подходах и основных, уже разработанных, криптопротоколах.

К иному классу программных методов защиты от удаленных атак относятся существующие на сегодняшний день программы, основная цель которых - анализ сетевого трафика на предмет наличия одного из известных активных удаленных воздействий.

а) SKIP-технология и криптопротоколы SSL, S-HTTP как основное средство защиты соединения и передаваемых данных в сети Internet

Одна из основных причин успеха удаленных атак на распределенные ВС кроется в использовании сетевых протоколов обмена, которые не могут надежно идентифицировать удаленные объекты, защитить соединение и передаваемые по нему данные. Поэтому совершенно естественно, что в процессе функционирования Internet были созданы различные защищенные сетевые протоколы, использующие криптографию как с закрытым, так и с открытым ключом. Классическая криптография с симметричными криптоалгоритмами предполагает наличие у передающей и принимающей стороны симметричных (одинаковых) ключей для шифрования и дешифрирования сообщений. Эти ключи предполагается распределить заранее между конечным числом абонентов, что в криптографии называется стандартной проблемой статического распределения ключей. Очевидно, что применение классической криптографии с симметричными ключами возможно лишь на ограниченном множестве объектов. В сети Internet для всех ее пользователей решить проблему статического распределения ключей, очевидно, не представляется возможным. Однако одним из первых защищенных протоколов обмена в Internet был протокол Kerberos, основанный именно на статическом распределении ключей для конечного числа абонентов. Таким же путем, используя классическую симметричную криптографию, вынуждены идти наши спецслужбы, разрабатывающие свои защищенные криптопротоколы для сети Internet. Это объясняется тем, что почему-то до сих пор нет гостированного криптоалгоритма с открытым ключом. Везде в мире подобные стандарты шифрования давно приняты и сертифицированы, а мы, видимо, опять идем другим путем!

Итак, понятно, что для того, чтобы дать возможность защититься всему множеству пользователей сети Internet, а не ограниченному его подмножеству, необходимо использовать динамически вырабатываемые в процессе создания виртуального соединения ключи при использовании криптографии с открытым ключом. Далее мы рассмотрим основные на сегодняшний день подходы и протоколы, обеспечивающие защиту соединения.

SKIP (Secure Key Internet Protocol)-технологией называется стандарт инкапсуляции IP-пакетов, позволяющий в существующем стандарте IPv4 на сетевом уровне обеспечить защиту соединения и передаваемых по нему данных. Это достигается следующим образом: SKIP-пакет представляет собой обычный IP-пакет, поле данных которого представляет из себя SKIP-заголовок определенного спецификацией формата и криптограмму (зашифрованные данные). Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хосту в сети Internet (межсетевая адресация происходит по обычному IP-заголовку в SKIP-пакете). Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему обычному модулю (TCP или UDP) ядра операционной системы. В принципе, ничто не мешает разработчику формировать по данной схеме свой оригинальный заголовок, отличный от SKIP-заголовка.

S-HTTP (Secure HTTP) - это разработанный компанией Enterprise Integration Technologies (EIT) специально для Web защищенный HTTP-протокол. Протокол S-HTTP позволяет обеспечить надежную криптозащиту только HTTP-документов Web-севера и функционирует на прикладном уровне модели OSI. Эта особенность протокола S-HTTP делает его абсолютно специализированным средством защиты соединения, и, как следствие, невозможное его применение для защиты всех остальных прикладных протоколов (FTP, TELNET, SMTP и др.). Кроме того, ни один из существующих на сегодняшний день основных Web-броузеров (ни Netscape Navigator 3.0, ни Microsoft Explorer 3.0) не поддерживают данный протокол.

SSL (Secure Socket Layer) - разработка компании Netscape - универсальный протокол защиты соединения, функционирующий на сеансовом уровне OSI. Этот протокол, использующий криптографию с открытым ключом, на сегодняшний день, по нашему мнению, является единственным универсальным средством, позволяющим динамически защитить любое соединение с использованием любого прикладного протокола (DNS, FTP, TELNET, SMTP и т. д.). Это связано с тем, что SSL, в отличие от S-HTTP, функционирует на промежуточном сеансовом уровне OSI (между транспортным - TCP, UDP, - и прикладным - FTP, TELNET и т. д.). При этом процесс создания

виртуального SSL-соединения происходит по схеме Диффи и Хеллмана (п. 6.2), которая позволяет выработать криптостойкий сеансовый ключ, используемый в дальнейшем абонентами SSL-соединения для шифрования передаваемых сообщений. Протокол SSL сегодня уже практически оформился в качестве официального стандарта защиты для HTTP-соединений, то есть для защиты Web-серверов. Его поддерживают, естественно, Netscape Navigator 3.0 и, как ни странно, Microsoft Explorer 3.0 (вспомним ту ожесточенную войну броузеров между компаниями Netscape и Microsoft). Конечно, для установления SSL-соединения с Web-сервером еще необходимо и наличие Web-сервера, поддерживающего SSL. Такие версии Web-серверов уже существуют (SSL-Apache, например). В заключении разговора о протоколе SSL нельзя не отметить следующий факт: законами США до недавнего времени был запрещен экспорт криптосистем с длиной ключа более 40 бит (недавно он был увеличен до 56 бит). Поэтому в существующих версиях броузеров используются именно 40-битные ключи. Криптоаналитиками путем экспериментов было выяснено, что в имеющейся версии протокола SSL шифрование с использованием 40-битного ключа не является надежной защитой для передаваемых по сети сообщений, так как путем простого перебора (240 комбинаций) этот ключ подбирается за время от 1,5 (на суперЭВМ Silicon Graphics) до 7 суток (в процессе вычислений использовалось 120 рабочих станций и несколько мини ЭВМ).

Итак, очевидно, что повсеместное применение этих защищенных протоколов обмена, особенно SSL (конечно, с длиной ключа более 40 бит), поставит надежный барьер на пути всевозможных удаленных атак и серьезно усложнит жизнь кракеров всего мира. Однако весь трагизм сегодняшней ситуации с обеспечением безопасности в Internet состоит в том, что пока ни один из существующих криптопротоколов (а их уже немало) не оформился в качестве единого стандарта защиты соединения, который поддерживался бы всеми производителями сетевых ОС! Протокол SSL, из имеющихся на сегодня, подходит на эту роль наилучшим образом. Если бы его поддерживали все сетевые ОС, то не потребовалось бы создание специальных прикладных SSL-совместимых серверов (DNS, FTP, TELNET, WWW и др.). Если не договориться о принятии единого стандарта на защищенный протокол сеансового уровня, то тогда потребуется принятие многих стандартов на защиту каждой отдельной прикладной службы. Например, уже разработан экспериментальный, никем не поддерживаемый протокол Secure DNS. Также существуют экспериментальные SSL-совместимые Secure FTP- и TELNET-серверы. Но все это без принятия единого поддерживаемого всеми производителями стандарта на защищенный протокол не имеет абсолютно никакого смысла. А на сегодняшний день производители сетевых ОС не могут договориться о единой позиции на эту тему и, тем самым, перекладывают решение этих проблем непосредственно на пользователей Internet и предлагают им решать свои проблемы с информационной безопасностью так, как тем заблагорассудится!

б) Сетевой монитор безопасности IP Alert-1

Практические и теоретические изыскания авторов, по направлению, связанному с исследованием безопасности распределенных ВС, в том числе и сети Internet (два полярных направления исследования: нарушение и обеспечение информационной безопасности), навели на следующую мысль: в сети Internet, как и в других сетях (например, Novell NetWare, Windows NT), ощущается серьезная нехватка программного средства защиты, осуществляющего комплексный контроль (мониторинг) на канальном уровне за всем потоком передаваемой по сети информации с целью обнаружения всех типов удаленных воздействий, описанных в 4 главе. Исследование рынка программного обеспечения сетевых средств защиты для Internet выявило тот факт, что подобных комплексных средств обнаружения удаленных воздействий по нашим сведениям не существует, а те, что имеются, предназначены для обнаружения воздействий одного конкретного типа (например, ICMP Redirect или ARP). Поэтому и была начата разработка средства контроля сегмента IP-сети, предназначенного для использования в сети Internet и получившее следующее название: сетевой монитор безопасности IP Alert-1. Основная задача этого средства, программно анализирующего сетевой трафик в канале передачи, состоит не в отражении осуществляемых по каналу связи удаленных атак, а в их обнаружении, протоколировании (ведении файла аудита с протоколированием в удобной для последующего визуального анализа форме всех событий, связанных с удаленными атаками на данный сегмент сети) и незамедлительным сигнализировании администратору безопасности в случае обнаружения удаленной атаки. Основной задачей сетевого монитора безопасности IP Alert-1 является осуществление контроля за безопасностью соответствующего сегмента сети Internet.

Сетевой монитор безопасности IP Alert-1 обладает следующими функциональными возможностями и позволяет, путем сетевого анализа, обнаружить следующие удаленные атаки на контролируемый им сегмент сети Internet.

Функциональные возможности сетевого монитора безопасности IP Alert-1

1. Контроль за соответствием IP- и Ethernet-адресов в пакетах, передаваемых хостами, находящимися внутри контролируемого сегмента сети.

На хосте IP Alert-1 администратор безопасности создает статическую ARP-таблицу, куда заносит сведения о соответствующих IP- и Ethernet-адресах хостов, находящихся внутри контролируемого сегмента сети.

Данная функция позволяет обнаружить несанкционированное изменение IP-адреса или его подмену (IP Spoofing).

2. Контроль за корректным использованием механизма удаленного ARP-поиска.

Эта функция позволяет, используя статическую ARP-таблицу, определить удаленную атаку "Ложный ARP-сервер".

3. Контроль за корректным использованием механизма удаленного DNS-поиска.

Эта функция позволяет определить все возможные виды удаленных атак на службу DNS.

4. Контроль на наличие ICMP Redirect сообщения.

Данная функция оповещает об обнаружении ICMP Redirect сообщения и соответствующей удаленной атаки.

5. Контроль за корректностью попыток удаленного подключения путем анализа передаваемых запросов.

Эта функция позволяет обнаружить, во-первых, попытку исследования закона изменения начального значения идентификатора TCP-соединения - ISN, во-вторых, удаленную атаку "отказ в обслуживании", осуществляемую путем переполнения очереди запросов на подключение, и, в-третьих, направленный "шторм" ложных запросов на подключение (как TCP, так и UDP), приводящий также к отказу в обслуживании.

Таким образом, сетевой монитор безопасности IP Alert-1 позволяет обнаружить, оповестить и запротоколировать все виды удаленных атак, описанных в 4 главе! При этом данная программа никоим образом не является конкурентом системам Firewall. IP Alert-1, используя описанные и систематизированные в 4 главе особенности удаленных атак на сеть Internet, служит необходимым дополнением - кстати, несравнимо более дешевым, - к системам Firewall. Без монитора безопасности большинство попыток осуществления удаленных атак на ваш сегмент сети останется скрыто от ваших глаз. Ни один из известных авторам файрволов не занимается подобным интеллектуальным анализом проходящих по сети сообщений на предмет выявления различного рода удаленных атак, ограничиваясь, в лучшем случае, ведением журнала, в который заносятся сведения о попытках подбора паролей для TELNET и FTP, о сканировании портов и о сканировании сети с использованием знаменитой программы удаленного поиска известных уязвимостей сетевых ОС - SATAN. Поэтому, если администратор IP-сети не желает оставаться безучастным и довольствоваться ролью простого статиста при удаленных атаках на его сеть, то ему желательно использовать сетевой монитор безопасности IP Alert-1. Кстати, напомним, что Цутому Шимомура смог запротоколировать атаку Кевина Митника, во многом, видимо, благодаря программе tcpdump - простейшему анализатору IP-трафика.

4. Рынок систем безопасности

4.1. Основные тенденции рынка: статистика и прогнозы

Как известно, тот, кто владеет информацией, владеет миром. Однако сегодня все убедительнее звучит и другое, не менее актуальное утверждение: тот, кто владеет информацией, постоянно опасается ее потерять или утратить над ней контроль.

По оценкам многих аналитиков, в 2001 году характер взломов существенно изменился: если раньше хакер действовал в основном один на один с объектом атаки (то есть по сути аполитично), то в настоящее время можно говорить о групповых действиях хакеров, что в быстро изменяющейся обстановке современного мира стало знаковым явлением. Атака — это уже не просто способ самовыражения и не «показательное выступление», а инструмент нанесения удара по цели. Исследования показывают, что Компьютерная Сеть (КС) почти везде весьма

уязвима, поэтому активизация данного вида деятельности несет в себе прямую опасность, особенно в момент напряженности в отношениях между различными политическими группами и государствами. Эксперты отмечают, что большинство крупных ресурсов сети до сих пор уязвимы.

На основании исследований общих тенденций информационной безопасности в IT-секторе можно сделать вывод, что компании достаточно инертно меняют свою информационную политику в области информационной безопасности, что их стратегическое видение постоянно запаздывает в охвате перспективы, а их практику обращения с персональными данными и уровень защищенности инфраструктур с трудом можно назвать удовлетворительными. В качестве аргументов, говорящих в пользу этого утверждения, можно привести впечатляющие цифры. Так, большинство компаний неадекватно соотносят свою деятельность с существующими угрозами: например, только одна компания из 10 удаляет/меняет пароли после увольнения работника, хотя 80% компаний имеют соответствующие регламенты. Результаты исследований свидетельствуют о слабой приверженности организаций к аудиту по вопросам информационной безопасности (35%), о минимальных усилиях по стимулированию легального расследования инцидентов (17%), о недостаточном понимании источников угрозы (79% до сих пор считают, что опасность исходит извне, хотя статистика доказывает обратное). Исследования показали, что 60% топ-менеджеров рассматривает информационную безопасность корпораций как проблему технологий (a technology problem) и только (40%) — как стратегическую проблему для бизнеса корпорации (a strategic business issue).

Однако, несмотря на вышеперечисленные факты, в настоящее время налицо явный рост внимания общества к проблемам информационной безопасности, к тому спектру отношений, которые обычно называют Electronic Security. Подтверждением тому является следующее. По мнению специалистов аналитической компании IDC, спрос на системы Интернет-безопасности в ближайшие годы будет стремительно расти, что превратит данный сектор рынка в один из самых прибыльных. Согласно расчетам IDC, среднегодовой рост на рынке систем Интернет-безопасности в ближайшие пять лет составит 23%, и к 2005 году рынок достигнет объема в 14 млрд. долл. Как считают специалисты IDC, основной потенциал лежит в секторе программных продуктов, предназначенных для безопасной аутентификации, авторизации и администрирования, — в так называемом секторе продуктов группы 3A (Администрирование, Авторизация, Аутентификация). По мнению IDC, программное обеспечение информационной безопасности 3A состоит из реализаций функций администрирования, авторизации и аутентификации, используемых для администрирования безопасности на отдельных компьютерных системах или в корпоративных рамках, и включает в себя процессы определения, создания, изменения, удаления и аудита пользователей. По оценкам того же источника, ежегодный прирост в этом секторе составит 28%, и к 2005 году он займет 67% рынка.

Известно, что одним из факторов, сдерживающих развитие электронной коммерции, является проблема безопасности. Согласно исследованию Конфедерации британской промышленности (CBI), компании больше верят в безопасность B2B -операций. Более половины предприятий, опрошенных CBI, заявили, что они доверяют B2B-коммерции, в то время как о B2C-операциях так высказалось только 32%. Хотя мошенничество с банковскими картами и составляет около 4% от числа серьезных инцидентов, аналитики CBI отмечают, что боязнь мошенничества по-прежнему сдерживает развитие электронного бизнеса, в особенности B2C-сектора.

Среди других важных тенденций рынка следует отметить то, что компании пока еще не готовы защитить себя и представить безопасный сервис, поскольку у них не хватает квалифицированного персонала (70,5%) и они стратегически не в состоянии просчитать, насколько выгодным будет внедрение новых практик безопасности (45,9%). Такие далеко не обнадеживающие результаты были выявлены в ходе исследования по Японии, которая ни в коей мере не является технологически отсталой страной. Специалисты утверждают, что в сфере сетевой безопасности ощущается острая нехватка персонала, способного эффективно решать соответствующие задачи.

Один из последних опросов в прошедшем году зафиксировал растущую озабоченность американцев в связи с проблемами конфиденциальнности и сетевой безопасности. И хотя основной акцент был сделан на оценке безопасности корпоративных и правительственных сетей, в общем контексте ответов прослеживается тревога по отношению ко всему, что окружает людей в этом неопределенном мире: что 71% респондентов заявили, что они озабочены проблемой безопасности в КС, а 78% обеспокоены возможностью кражи или иного несанкционированного использования их персональной информации в КС.

Безопасность беспроводных операций продолжает беспокоить и компании, и пользователей. Те и другие опасаются, что хакеры смогут перехватывать информацию «на лету». Кроме того, потенциальной проблемой представляется потеря пользователями мобильных устройств, содержащих конфиденциальную информацию.

4.2. Структура рынка безопасности

То, что в 60-е годы называлось компьютерной безопасностью, а в 70-е — безопасностью данных, сейчас более точно именуется информационной безопасностью. Информационная безопасность включает меры по защите процессов создания данных, их ввода, обработки и вывода. Главная цель состоит в том, чтобы защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, когда информация создается, модифицируется, когда к ней обеспечивается доступ и когда она распространяется.

Информационная безопасность гарантирует достижение следующих целей:

конфиденциальность критической информации;

целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);

доступность информации в случае необходимости;

учет всех процессов, связанных с информацией.

В общем плане рынок безопасности информационных систем можно условно разделить на два идеологически не связанных направления.

Первое направление ставит своей целью информационную защиту сетей, то есть защиту информации, которая циркулирует внутри информационных сетей. В настоящее время это наиболее востребованно, а потому хорошо развито. Сюда входят различные антивирусы, межсетевые фильтры (firewall), криптографические средства, защитные протоколы, цифровые подписи и т.п. Наиболее надежным средством на сегодняшний день является шифрование с открытым ключом.

Второе направление, стремительно развивающееся в последнее время, связано с непосредственной защитой объектов сети. Это направление представляют в основном механические устройства, предотвращающие доступ к аппаратной части, то есть к серверам, персональным компьютерам и т.д. Основная задача указанных устройств состоит в том, чтобы с помощью различных крепежей, замков, защитных кожухов и пр. не дать нарушителю возможности вскрыть компьютер. В арсенале имеются также программные средства, которые позволяют находить похищенные компьютеры после того, как они хоть раз были подключены к телефонной сети или к Интернету. Эти программы состоят из двух частей: клиента и центра обработки информации. После того как клиент установлен на компьютер, он периодически (каждые 15 минут) связывается с центром и передает доступную информацию о текущем статусе компьютера (IP-адрес, номер телефона, к которому подключен в данный момент компьютер, и т.д.). Клиент инсталлируется таким образом, чтобы быть защищенным от форматирования винчестера, и не быть видным с помощью обычных средств операционной системы (process viewers). Еще один вариант реализации второго направления заключается в том, что компьютеры с помощью дополнительной проводки и специальных датчиков, которые крепятся к задней панели компьютера, объединяются в сеть, отличную от сети передачи данных, и подключаются к аппаратному устройству, способному регистрировать несанкционированный доступ и включать сигнализацию.

Вероятнее всего, в недалеком будущем мы будем свидетелями интеграции этих двух направлений, что является естественным шагом на пути к повышению уровня защиты информации. И в результате такой интеграции сможет появиться некая универсальная система безопасности, а у администратора безопасности будет единое рабочее место, с которого он сможет контролировать порядок обработки данных и целостность объектов. Установка такой системы не потребует дополнительной прокладки кабелей, а ее работа никак не скажется на производительности сети передачи данных.

4.3. Лидеры на рынке систем безопасности

Корпорация Symantec

Корпорация Symantec, один из мировых лидеров в создании систем безопасности для работы в Интернете, является ведущим поставщиком на рынке систем безопасности. Принадлежащее корпорации Symantec торговая марка Norton объединяет линию используемых для обеспечения информационной безопасности продуктов, занимающих ведущие позиции в мире как по числу продаж в розничной торговле, так и по количеству отраслевых наград. Штаб-квартира Symantec расположена в г.Купертино, шт. Калифорния. Корпорация имеет представительства в 37 странах.

В отчете Gartner Dataquest эта компания названа мировым лидером в области поставок программных средств для обеспечения информационной безопасности. Данная оценка основывается на объеме доходов от продажи новых лицензий в 2000 году. Отчет Gartner Dataquest показывает, что рост, продемонстрированный корпорацией Symantec, опережает рост рынка средств безопасности — рост доходов корпорации Symantec составил 40% за год. «В результате слияния с компанией Axent, которое произошло в декабре 2000 года, корпорация Symantec переместилась с 4-го на 1-е место в списке, завладев при этом 14,7% рынка средств безопасности», — отмечается в отчете. Программные средства безопасности Symantec, согласно классификации Gartner Dataquest, включают: антивирусное программное обеспечение, программы шифрования, средства обнаружения попыток несанкционированного проникновения и другие средства информационной защиты — межсетевые экраны, программы фильтрации Web-ресурсов, приложения для управления доступом к внешним сетям. Корпорация Symantec предлагает средства антивирусной защиты, межсетевые экраны, виртуальные частные сети, средства выявления слабых мест системы безопасности и попыток несанкционированного проникновения, программы фильтрации информационных ресурсов Интернета и электронной почты, технологии удаленного управления, а также услуги по обеспечению информационной безопасности.

Компания Network Associates, Inc.

Эта компания, так же как и Symantec, уверенно доминирует на рынке систем безопасности, контролируя около 60% мирового рынка антивирусов. По данным Network Associates, Inc. (NAI) она имеет более 60 млн. пользователей по всему миру. NAI предлагает одно из наиболее укомплектованных в функциональном и потребительском плане семейство программ, которые защищают, управляют и контролируют корпоративные сети. Функциональные возможности и широта решений, предлагаемые Network Associates, дополняются возможностями, приобретенными у Pretty Good Privacy (PGP) и Magic Solutions, а также мощнейшими средствами антивирусных средств Dr.Solomon's, первая версия которой была выпущена в начале 1997 года фирмой Dr.Solomon's Software. По информации McAfee (подразделения Network Associates, Inc.), программный продукт McAfee GroupShield Exchange уже третий год подряд получает награду Best Buy от Secure Computing Magazine, выигрывая в сравнительном тесте антивирусов для MS Exchange. В сравнительном обзоре антивирусов для Microsoft Exchange 2001 McAfee GroupShield получил наивысшие оценки, обойдя продукты других антивирусных производителей, таких как Symantec, «Лаборатория Касперского», Trend Micro, F-Secure, Panda, Computer Associates и др.

Корпорация Computer Associates International, Inc.

Отчет IDC определил Computer Associates International, Inc. (CA) как лидирующего поставщика программного обеспечения в области аутентификации, авторизации и администрирования (ЗА), которому принадлежит 15,5% мирового рынка. В 2001 году отчет IDC под названием «Прогноз и анализ международного рынка программного обеспечения безопасности работы в Интернет на 2001-2005 годы» выделил CA в качестве мирового лидирующего поставщика программного обеспечения защиты данных при работе в Интернете второй год подряд. CA предлагает решения ЗА средствами семейства продуктов eTrust (eTrust PKI, eTrust SSO, eTrust CA-ACF2, eTrust CA-Top Secret, eTrust Admin, eTrust Access Control и eTrust Intrusion Detection). «CA является очевидным мировым лидером в разработке решений по информационной безопасности и по технологической эффективности, и по общему объему на рынке», — отметил вице-президент CA по решениям eTrust, Barry Keyes. — Преимущества нашей новой бизнес-модели лицензирования, всесторонний технический сервис и прозрачное интегрированное решение управления электронным бизнесом позволил и нам сделать не имеющее себе равных по ценности предложение менеджерам по информационной безопасности предприятий и сервис-провайдеров». Семейство продуктов eTrust позволяет команде управления защищать, администрировать доступ и гарантировать управление и безопасность комплексной автоматизированной системы. Решение eTrust совместимо с действующими стандартами защиты данных, гарантирует возможность взаимодействия с существующими механизмами внутренней безопасности и с такими же механизмами партнеров по сетевому взаимодействию.

В заключение хотелось бы еще раз отметить, что проблема информационной безопасности с каждым годом становится все более актуальной. И рынок, откликаясь на массовый спрос наверняка будет предлагать, а впрочем, уже предлагает, надежные и вполне достойные решения по обеспечению безопасности. И главное сейчас — остановить любыми средствами наступление информационного хаоса, который провоцируется любителями заглянуть через плечо или порыться в чужих электронных портфелях. А для этого каждый должен выбрать для себя надежное средство информационной защиты, которое обеспечит ему надлежащую информационную безопасность.[4][iv]

Заключение

Исходно сеть создавалась как незащищенная открытая система, предназначенная для информационного общения все возрастающего числа пользователей.

При этом подключение новых пользователей должно было быть максимально простым, а доступ к информации — наиболее удобным. Все это явно противоречит принципам создания защищенной системы, безопасность которой должна быть описана на всех стадиях ее создания и эксплуатации, а пользователи — наделены четкими полномочиями.

Создатели сети не стремились к этому, да и требования защиты настолько бы усложнили проект, что сделали бы его создание едва ли возможным.

Вывод: Internet создавался как незащищенная система, не предназначенная для хранения и обработки конфиденциальной информации. Более того, защищенный Internet не смог бы стать той системой, которой он сейчас является и не превратился бы в информационный образ мировой культуры, ее прошлого и настоящего. В этом самостоятельная ценность Сети и, возможно, ее небезопасность есть плата за такое высокое назначение.

Следствие: Имеется множество пользователей, заинтересованных в том, чтобы Internet стал системой с категорированной информацией и полномочиями пользователями, подчиненными установленной политике безопасности.

Однако наиболее яркие творения человеческого разума через некоторое время начинают жить самостоятельной жизнью, развиваясь и выходя за первоначальные замыслы создателей. Поэтому слабая защищенность сети с течением времени стала все больше беспокоить ее пользователей.

На наш взгляд, в Сети не должна находиться информация, раскрытия которой приведет к серьезным последствиям. Наоборот, в Сети необходимо размещать информацию, распространение которой желательно ее владельцу. При этом всегда необходимо учитывать тот факт, что в любой момент эта информация может быть перехвачена, искажена или может стать недоступной. Следовательно, речь должна идти не о защищенности Internet, а об обеспечении разумной достаточности информационной безопасности Сети.

Конечно, это не отменяет необходимости ознакомления пользователя с богатым и все время возрастающим арсеналом программных и аппаратных средств обеспечения информационной безопасности сети. Тем не менее отметим, что они не в состоянии превратить Internet в защищенную среду, что означило бы изменение ее природы.

Будет ли Internet защищенным? Развитие средств безопасности Internet может войти в противоречие с ее назначением и исказит саму идею Сети. Более правомерна постановка вопроса о создании специализированной безопасной мировой инфосферы, предназначенной для управления мировым производством, транспортом, геополитикой. Видимо, прогресс приведет к необходимости создания такой единой системы. Такая среда общения будет обладать архитектурой безопасности и гарантировать целостность и конфиденциальность информации. Очевидно, что создатели этой системы должны обеспечить соблюдение политических и экономических интересов мировых субъектов, т. к. многопольное владение этой системой означает контроль над миром.

Ясно, что подобной средой не может быть Internet в сегодняшнем виде. Главное, на наш взгляд, — нужно воздержаться от стремления приблизить сегодняшний Internet к такой среде управления миром. Internet по-своему хорош в том виде, в каком он есть.

В чем перспектива защиты информационных систем в эпоху интеграции среды обработки информации? По нашему мнению, выход из сложившегося положения состоит в четком разграничении информации, представляющей жизненный интерес для субъектов — пользователей — и создания специализированных систем ее обработки. Такие системы должны иметь возможность интегрирования в мировую сеть при обеспечении их односторонней информационной изоляции.

---

[i] КомпьютерПресс 8'1999

[ii] Лукацкий А.В. Системы обнаружения атак//Банковские технологии. 1999. № 2.

[iii] КомпьютерПресс 10'2001

[iv] КомпьютерПресс 3'2002