***Московский государственный институт электроники и математики.***

кафедра ЭВА

**Реферат на тему:**

**“Безопасность сетей на базе TCP/IP”**

Москва 1999

#### Безопасность сетей на базе семейства протоколов TCP/IP

В этой работе безопасность сетей на базе семейства протоколов TCP/IP будет рассмотрена на примере сети Internet, информационная безопасность которой в значительной мере определяется этими протоколами.

Из-за ограниченности объёма этой работы механизмы реализации атак не будут рассмотрены во всех подробностях, так как это довольно большая тема и для этого есть специальная литература, ссылки на которую приведены в конце. Данная работа представляет собой обзор наиболее распространённых атак, основанных на особенностях протоколов, с описанием причин, по которым они возможны, и описанием способов устранения уязвимостей. Также в работе затронуты темы, не имеющие непосредственного отношения к протоколам TCP/IP, но не менее важные с точки зрения безопасности сети Internet.

Далее будут рассмотрены типовые атаки, но сначала надо дать несколько общих определений и рассмотреть классификацию угроз безопасности. Кроме того, следует заметить, что по статистике разрушение данных в вычислительных системах чаще всего происходит не из-за деятельности взломщиков, ошибок в программах или действий вирусов (17%) либо технических отказов (16%), а из-за ошибок и несанкционированных действий пользователей (67%).

Сначала вкратце рассмотрим особенности семейства протоколов TCP/IP и сетей на его основе.

Итак, стек протоколов TCP/IP включает в себя:

* + IP (Internet Protocol) – межсетевой протокол, который обеспечивает транспортировку без дополнительной обработки данных с одной машины на другую;
  + UDP (User Datagram Protocol) – протокол пользовательских датаграмм, обеспечивающий транспортировку отдельных сообщений с помощью IP без проверки ошибок;
  + TCP (Transmission Control Protocol) – протокол управления передачей, обеспечивающий транспортировку с помощью IP с проверкой установления соединения;
  + ICMP (Internet Control Message Protocol) – межсетевой протокол управления сообщениями, который отвечает за различные виды низкоуровневой поддержки протокола IP, включая сообщения об ошибках, содействие в маршрутизации, подтверждение в получении сообщения;
  + ARP (Address Resolution Protocol) – протокол преобразования адресов, выполняющий трансляцию логических сетевых адресов в аппаратные;

Каждый компьютер, подключаемый к Internet, получает свой уникальный IP-адрес.

 Основные понятия компьютерной безопасности

*Угроза* безопасности компьютерной системы - это потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

*Уязвимость* компьютерной системы - это некая ее неудачная характеристика, которая делает возможным возникновение угрозы.

Наконец, *атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

Исследователи обычно выделяют три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании.

Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать. Иногда вместо слова "раскрытие" используются термины "кража" или "утечка".

Угроза *целостности* включает в себя любое умышленное изменение данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие.

Угроза *отказа в обслуживании* возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

В локальных вычислительных системах (ВС) наиболее частыми являются угрозы раскрытия и целостности, а в глобальных на первое место выходит угроза отказа в обслуживании.

#### Особенности безопасности компьютерных сетей

Основной особенностью любой сетевой системы является то, что её компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что, наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или *удалённые*) атаки (remote или network attacks). Они характеризуются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удалённые атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности ВС с точки зрения противостояния удалённым атакам приобретает первостепенное значение.

#### Классификация компьютерных атак

Формы организации атак весьма разнообразны, но в целом все они принадлежат к одной из следующих категорий:

* Удаленное проникновение в компьютер: программы, которые получают неавторизованный доступ к другому компьютеру через Интернет (или локальную сеть);
* Локальное проникновение в компьютер: программы, которые получают неавторизованный доступ к компьютеру, на котором они работают;
* Удаленное блокирование компьютера: программы, которые через Интернет (или сеть) блокируют работу всего удаленного компьютера или отдельной программы на нем;
* Локальное блокирование компьютера: программы, которые блокируют работу компьютера, на котором они работают;
* Сетевые сканеры: программы, которые осуществляют сбор информации о сети, чтобы определить, какие из компьютеров и программ, работающих на них, потенциально уязвимы к атакам;
* Сканеры уязвимых мест программ: программы, проверяют большие группы компьютеров в Интернет в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки;
* Вскрыватели паролей: программы, которые обнаруживают легко угадываемые пароли в зашифрованных файлах паролей;
* Сетевые анализаторы (sniffers): программы, которые слушают сетевой трафик. Часто в них имеются возможности автоматического выделения имен пользователей, паролей и номеров кредитных карт из трафика;
* Модификация передаваемых данных или подмена информации;
* Подмена доверенного объекта распределённой ВС (работа от его имени) или ложный объект распределённой ВС (РВС).
* *Социальная инженерия –* несанкционированный доступ к информации иначе, чем взлом программного обеспечения. Цель – обхитрить людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы;

#### Статистика самых распространенных атак

В 1998 году NIST (http://csrc.nist.gov/) проанализировал 237 компьютерных атак, информация о которых была опубликована в Интернет. Этот анализ дал следующую статистику:

* 29% атак были организованы из-под Windows.

**Вывод:** Не стоит считать опасной только Unix. Сейчас наступило время атак типа "укажи и кликни". Доступность в сети программ для взлома позволяет пользоваться ими даже ничего не знающими людьми. В будущем, вероятно, этот процент будет расти.

* в 20% атак атакующие смогли удаленно проникнуть в сетевые элементы (маршрутизаторы, коммутаторы, хосты, принтеры и межсетевые экраны).

**Вывод:** атаки, в ходе которых атакующий получает неавторизованный доступ к удаленным хостам не так уж редки.

* в 3% атак web-сайты атаковали своих посетителей.

**Вывод:** поиск информации в WWW больше не является полностью безопасным занятием.

* в 4% атак производилось сканирование Интернета на наличие уязвимых хостов.

**Вывод:** Имеется много средств автоматического сканирования, с помощью которых могут быть скомпрометированы хосты. Системные администраторы должны регулярно сканировать свои системы (а не то это сделает кто-то другой).

* 5% атак оказались успешными атаками против маршрутизаторов и межсетевых экранов.

**Урок:** сами компоненты инфраструктуры Интернета уязвимы к атакам (правда, большинством этих атак были атаки удаленного блокирования компьютеров и сканирования, и только небольшая часть из них были удаленным проникновением в компьютеры.)

Согласно опросу за 1999 год Института Компьютерной Безопасности и ФБР о компьютерных преступлениях, 57% опрошенных организаций сообщили, что считают соединения их сетей с Интернет "местом, откуда часто организуются атаки". 30% опрошенных сообщило, что имели место случаи проникновения в их сети, а 26% сказали, что в ходе атак происходила кража конфиденциальной информации. Федеральный центр по борьбе с компьютерными преступлениями в США – FedCIRC (http://www.fedcirc.gov) сообщил, что в 1998 году атакам подверглось около 130000 государственных сетей с 1100000 компьютерами.

#### Анализ сетевого трафика сети *Internet*

Одним из способов получения паролей и идентификаторов пользователей в сети Internet является анализ сетевого трафика. Сетевой анализ осуществляется с помощью специальной пpогpаммы-анализатоpа пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

Во многих протоколах данные передаются в открытом, незашифрованном виде. Анализ сетевого трафика позволяет перехватывать данные, передаваемые по протоколам FTP и TELNET (пароли и идентификаторы пользователей), HTTP (передача гипертекста между WEB-сервером и браузером, в том числе и вводимые пользователем в формы на web-страницах данные), SMTP, POP3, IMAP, NNTP (электронная почта и конференции) и IRC (online-разговоры, chat). Так могут быть перехвачены пароли для доступа к почтовым системам с web-интерфейсом, номера кредитных карт при работе с системами электронной коммерции и различная информация личного характера, разглашение которой нежелательно.

В настоящее время разработаны различные протоколы обмена, позволяющие защитить сетевое соединение и зашифровать трафик (например, протоколы SSL и TLS, SKIP, S-HTTP и т.п.). К сожалению, они ещё не сменили старые протоколы и не стали стандартом для каждого пользователя. В определённой степени их распространению помешали существующие в ряде стран ограничения на экспорт средств сильной криптографии. Из-за этого реализации данных протоколов либо не встраивались в программное обеспечение, либо значительно ослаблялись (ограничивалась максимальная длина ключа), что приводило к практической бесполезности их, так как шифры могли быть вскрыты за приемлемое время.

#### Ложный ARP-сервер в сети *Internet*

Для адресации IP-пакетов в сети Internet кроме IP-адреса хоста необходим еще либо Ethernet-адрес его сетевого адаптера (в случае адресации внутри одной подсети), либо Ethernet-адрес маршрутизатора (в случае межсетевой адресации). Первоначально хост может не иметь информации о Ethernet-адресах других хостов, находящихся с ним в одном сегменте, в том числе и о Ethernet-адресе маршрутизатора. Следовательно, перед хостом встает стандартная проблема, решаемая с помощью алгоритма удаленного поиска.

В сети Internet для решения этой проблемы используется протокол ARP (Address Resolution Protocol). Протокол ARP позволяет получить взаимно однозначное соответствие IP- и Ethernet-адресов для хостов, находящихся внутри одного сегмента. Этот протокол работает следующим образом: при первом обращении к сетевому ресурсу хост отправляет широковещательный ARP-запрос, в котором указывает IP-адрес нужного ресурса (маршрутизатора или хоста) и просит сообщить его Ethernet-адрес. Этот запрос получают все станции в данном сегменте сети, в том числе и та, адрес которой ищется. Получив этот запрос, хост вносит запись о запросившей станции в свою ARP-таблицу, а затем отправляет на запросивший хост ARP-ответ со своим Ethernet-адресом. Полученный в ARP-ответе Ethernet-адрес заносится в ARP-таблицу, находящуюся в памяти ОС на запросившем хосте.

Из-за использования в РВС алгоритмов удаленного поиска, существует возможность осуществления в такой сети типовой удаленной атаки "Ложный объект РВС"

Общая схема этой атаки такова:

* ожидание ARP-запроса;
* при получении ARP-запроса передача по сети на запросивший хост ложного ARP-ответа, в котором указывается адрес сетевого адаптера атакующей станции (ложного ARP-сервера) или тот Ethernet-адрес, на котором будет принимать пакеты ложный ARP-сервер;
* прием, анализ, воздействие и передача пакетов обмена между взаимодействующими хостами (воздействие на перехваченную информацию);

Самое простое решение по ликвидации данной атаки – создание сетевым администратором статической ARP-таблицы в виде файла, куда вносится информация об адресах, и установка этого файла на каждый хост внутри сегмента.

 Ложный DNS-сервер в сети *Internet*

Как известно, для обращения к хостам в сети Internet используются 32-разрядные IP-адреса, уникально идентифицирующие каждый сетевой компьютер. Но для пользователей применение IP-адресов при обращении к хостам является не слишком удобным и далеко не самым наглядным. Поэтому для их удобства было принято решение присвоить всем компьютерам в Сети имена, что в свою очередь потребовало преобразования этих имён в IP-адреса, так как на сетевом уровне адресация пакетов идёт не по именам, а по IP-адресам.

Первоначально, когда в сети Internet было мало компьютеров, для решения проблемы преобразования имён в адреса существовал специальный файл (так называемый hosts-файл), в котором именам в соответствие ставились IP-адреса. Файл регулярно обновлялся и рассылался по Сети. По мере развития Internet, число объединённых в Сеть хостов увеличивалось, и такая схема становилась всё менее работоспособной. Поэтому ей на смену пришла новая система преобразования имён, позволяющая пользователю получить IP-адрес, соответствующий определённому имени, от ближайшего информационно-поискового сервера (DNS-сервера). Этот способ решения проблемы получил название Domain Name System (DNS – доменная система имён). Для реализации этой системы был разработан протокол DNS.

Алгоритм работы DNS-службы такой:

1. Хост посылает на IP-адрес ближайшего DNS-сервера DNS-запрос, в котором указывается имя сервера, IP-адрес которого требуется найти.
2. DNS-сервер при получении такого запроса ищет указанное имя в своей базе имён. Если оно и соответствующий ему IP-адрес найдены, то DNS-сервер отправляет на хост DNS-ответ, в котором указывает этот адрес. Если имя не найдено в своей базе имён, то DNS-сервер пересылает DNS-запрос на один из ответственных за домены верхнего уровня DNS-серверов. Эта процедура повторяется, пока имя не будет найдено или будет не найдено.

Как видно из приведённого алгоритма, в сети, использующей протокол DNS, возможно внедрение ложного объекта – ложного DNS-сервера

Так как по умолчанию служба DNS функционирует на базе протокола UDP, не предусматривающего, в отличие от TCP, средств идентификации сообщений, это делает её менее защищённой.

Возможна такая схема работы ложного DNS-сервера:

1. Ожидание DNS-запроса.
2. Извлечение из полученного сообщения необходимых сведений и передача за запросивший хост ложного DNS-ответа от имени (с IP-адреса) настоящего DNS-сервера и с указанием в этом ответе IP-адреса ложного DNS-сервера.
3. При получении пакета от хоста – изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на сервер. Ложный DNS-сервер ведёт работу с сервером от своего имени.
4. При получении пакета от сервера – изменение в IP-заголовке пакета его IP-адреса на адрес ложного DNS-сервера и передача пакета на хост. Ложный DNS-сервер для хоста является настоящим сервером.

Возможны два варианта реализации этой атаки. В первом случае необходимым условием является перехват DNS-запроса, что требует нахождения атакующего либо на пути основного трафика, либо в одном сегменте с DNS-сервером. Во втором случае создаётся направленный шторм ложных заранее подготовленных DNS-ответов на атакуемый хост.

В Internet при использовании существующей версии службы DNS нет приемлемого решения для защиты от ложного DNS-сервера. Можно отказаться от механизма удалённого поиска и вернуться к методу с файлом *hosts,* как это было до появления службы DNS, но на сегодняшний день в этот файл можно лишь внести информацию о наиболее часто посещаемых адресах.

Также для затруднения данной атаки можно предложить использовать протокол TCP вместо UDP, хотя из документации не всегда известно, как это сделать, да и использование TCP всё равно не обеспечивает полную безопасность.

#### Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети *Internet* ложного маршрутизатора

Это ещё одна атака, связанная с внедрением в РВС ложного объекта. Маршрутизация в Internet осуществляется на сетевом уровне (IP-уровень). Для её обеспечения в памяти сетевой ОС каждого хоста существуют таблицы маршрутизации, содержащие данные о возможных маршрутах. Каждый сегмент сети подключен к глобальной сети Internet как минимум через один маршрутизатор. Все сообщения, адресованные в другие сегменты сети, направляются на маршрутизатор, который, в свою очередь, перенаправляет их далее по указанному в пакете IP-адресу, выбирая при этом оптимальный маршрут.

Как говорилось ранее, в сети Internet существует управляющий протокол ICMP, одно из назначений которого состоит в динамическом изменении таблицы маршрутизации оконечных сетевых систем. Удалённое управление маршрутизацией реализовано в виде передачи на хост управляющего ICMP-сообщения *Redirect Message*.

Для осуществления данной атаки необходимо подготовить ложное ICMP-сообщение *Redirect Datagrams for the Host*, где указать адрес хоста, маршрут к которому будет изменён, и IP-адрес ложного маршрутизатора. Затем это сообщение передаётся на атакуемый хост от имени маршрутизатора. Эта атака позволяет получить контроль над трафиком между этим хостом и интересующим взломщика сервером, если хост и взломщик находятся в одном сегменте, или нарушить работоспособность хоста, если они располагаются в разных сегментах.

Защититься от этого воздействия можно фильтрацией проходящих ICMP-сообщений при помощи систем Firewall. Другой способ заключается в изменении сетевого ядра ОС, чтобы запретить реакцию на ICMP-сообщение Redirect.

#### Подмена одного из субъектов TCP-соединения в сети *Internet* (hijacking)

Протокол TCP (Transmission Control Protocol) является одним из базовых протоколов транспортного уровня сети Internet. Он позволяет исправлять ошибки, которые могут возникнуть в процессе передачи пакетов, устанавливая логическое соединение – виртуальный канал. По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление информационным потоком, организовывается повторная передача искаженных пакетов, а в конце сеанса канал разрывается. При этом протокол TCP является единственным базовым протоколом из семейства TCP/IP, имеющим дополнительную систему идентификации сообщений и соединения.

Для идентификации TCP-пакета в TCP-заголовке существуют два 32-разрядных идентификатора, которые также играют роль счетчика пакетов. Их названия - **Sequence Number** (номер последовательности) и **Acknowledgment Number** (номер подтверждения).

Для формирования ложного TCP-пакета атакующему необходимо знать текущие идентификаторы для данного соединения. Это значит, что ему достаточно, подобрав соответствующие текущие значения идентификаторов TCP-пакета для данного TCP-соединения послать пакет с любого хоста в Сети от имени одного из участников данного соединения, и данный пакет будет воспринят как верный.

При нахождении взломщика и объекта атаки в одном сегменте, задача получения значений идентификаторов решается анализом сетевого трафика. Если же они находятся в разных сегментах, приходится пользоваться математическим предсказанием начального значения идентификатора экстраполяцией его предыдущих значений.

Для защиты от таких атак необходимо использовать ОС, в которых начальное значение идентификатора генерируется действительно случайным образом. Также необходимо использовать защищённые протоколы типа SSL, S-HTTP, Kerberos и т.д.

#### Направленный шторм ложных TCP-запросов на создание соединения

На каждый полученный TCP-запрос на создание соединения операционная система должна сгенерировать начальное значение идентификатора ISN и отослать его в ответ на запросивший хост. При этом, так как в сети Internet (стандарта IPv4) не предусмотрен контроль за IP-адресом отправителя сообщения, то невозможно отследить истинный маршрут, пройденный IP-пакетом, и, следовательно, у конечных абонентов сети нет возможности ограничить число возможных запросов, принимаемых в единицу времени от одного хоста. Поэтому возможно осуществление типовой атаки "Отказ в обслуживании", которая будет заключаться в передаче на атакуемый хост как можно большего числа ложных TCP-запросов на создание соединения от имени любого хоста в сети. При этом атакуемая сетевая ОС в зависимости от вычислительной мощности компьютера либо – в худшем случае – практически зависает, либо – в лучшем случае – перестает реагировать на легальные запросы на подключение (отказ в обслуживании).

Это происходит из-за того, что для всей массы полученных ложных запросов система должна, во-первых, сохранить в памяти полученную в каждом запросе информацию и, во-вторых, выработать и отослать ответ на каждый запрос. Таким образом, все ресурсы системы "съедаются" ложными запросами: переполняется очередь запросов, и система занимается только их обработкой.

Недавно в Сети был отмечен новый тип атак. Вместо типичных атак Denial of Service хакеры переполняют буфер пакетов корпоративных роутеров не с единичных машин, а с целых тысяч компьютеров-зомби.

Такие атаки способны блокировать каналы мощностью вплоть до Т3 (44.736 Мбит/c) и уже отмечено несколько таких случаев. Опасность атаки становится тем важнее, чем больше бизнесов используют частные сети типа VPN и другие Интернет-технологии. Ведь отказ канала у публичного провайдера приведет в этом случае не просто к отключению отдельных пользователей, а к остановке работы огромных корпораций.

В этом случае существуют трудности в определении источника атаки - ложные пакеты идут с различных неповторяющихся IP-адресов. "Зомби-атаку" называют самой сложной из известных. На одинокую жертву нападает целая армия, и каждый зомби бьет только один раз.

Приемлемых способов защиты от подобных атак в сети стандарта IPv4 нет, так как невозможен контроль за маршрутом сообщений. Для повышения надёжности работы системы можно использовать по возможности более мощные компьютеры, способные выдержать направленный шторм ложных запросов на создание соединения.

#### Атаки, использующие ошибки реализации сетевых служб

Помимо перечисленных атак существуют и различные атаки, направленные против конкретных платформ. Например:

* **Атака Land –** формируется IP-пакет, в котором адрес отправителя совпадает с адресом получателя. Этой уязвимости подвержены все версии ОС семейства Windows до Windows NT 4.0 Service Pack 4 включительно. При поступлении таких запросов доступ к системе становится невозможным.
* **Атаки teardrop и bonk –** основаны на ошибках разработчиков ОС в модуле, отвечающем за сборку фрагментированных IP-пакетов. При этом происходит копирование блока отрицательной длины либо после сборки фрагментов в пакете остаются “дырки” – пустые, не заполненные данными места, что также может привести к сбою ядра ОС. Обе эти уязвимости присутствовали в ОС Windows95/NT до Service Pack 4 включительно и в ранних версиях ОС Linux (2.0.0).
* **WinNuke –** атака Windows-систем передачей пакетов TCP/IP с флагом Out Of Band (OOB) на открытый (обычно 139-й) TCP-порт. На сегодняшний день эта атака устарела. Ранние версии Windows95/NT зависали.

Существуют и различные другие атаки, характерные лишь для определённых ОС.

#### Атака через WWW

В последние несколько лет с бурным развитием World Wide Web сильно увеличилось и число атак через Web. В целом все типы атак через Web можно разделить на две большие группы:

1. Атака на клиента
2. Атака на сервер

В своём развитии браузеры ушли очень далеко от первоначальных версий, предназначенных лишь для просмотра гипертекста. Функциональность браузеров постоянно увеличивается, сейчас это уже полноценный компонент ОС. Параллельно с этим возникают и многочисленные проблемы с безопасностью используемых технологий, таких как подключаемые модули (plug-ins), элементы ActiveX, приложения Java, средства подготовки сценариев JavaScript, VBScript, PerlScript, Dynamic HTML.

Благодаря поддержке этих технологий не только браузерами, но и почтовыми клиентами и наличию ошибок в них в последние год-два появилось большое количество почтовых вирусов, а также вирусов, заражающих html-файлы (реализованные на VBScript с использованием ActiveX-объектов). Сильно распространены троянцы. Событием года стал выпуск хакерской группой Cult of the Dead Cow программы BackOrifice 2000, которая в отличие от предыдущей версии работает под WindowsNT да ещё и распространяется в исходных текстах, что даёт возможность всем желающим создать клон этой программы под свои конкретные нужды, к тому же, наверняка, не улавливаемый антивирусными программами.

Безопасность серверного ПО в основном определяется отсутствием следующих типов ошибок:

* Ошибки в серверах: ошибки, приводящие к утрате конфиденциальности; ошибки, приводящие к атакам типа “отказ в обслуживании” и ошибки, приводящие к выполнению на сервере неавторизованного кода.
* Ошибки во вспомогательных программах
* Ошибки администрирования

#### Проблема 2000 года применительно к сети *Internet*

Несмотря на то, что наступление 2000 года никак не повлияет на работу протоколов семейства TCP/IP, существуют программно-аппаратные средства, потенциально уязвимые по отношению к проблеме Y2K – это средства, обрабатывающие данные, связанные с системной датой.

Кратко рассмотрим возможные проблемы:

* + Проблемы с системами шифрования и цифровой подписи – возможна некорректная обработка даты создания обрабатываемых сообщений.
  + Ошибки в работе систем электронной коммерции, систем электронных торгов и резервирования заказов – неправильная обработка даты.
  + Проблемы с модулями автоматизированного контроля безопасности системы и протоколирования событий – неправильное ведение журнала и его анализ.
  + Проблемы с модулями реализации авторизованного доступа к ресурсам системы – невозможность доступа к системе в определённые даты.
  + Проблемы с запуском в определённое время модулей автоматического анализа безопасности системы и поиска вирусов.
  + Проблемы с системами защиты от нелегального копирования, основанными на временных лицензиях.
  + Проблемы с работой операционных систем.
  + Неправильная обработка даты аппаратными средствами защиты.

Для устранения возможных проблем при наступлении 2000 года необходимо всесторонне протестировать существующие системы и исправить обнаруженные ошибки. Обязательно нужно ознакомиться с информацией по данной системе от фирмы-производителя и обновить программное обеспечение, если доступны исправленные версии.

#### Методы защиты от удалённых атак в сети *Internet*

Наиболее простыми и дешёвыми являются административные методы защиты, как то использование в сети стойкой криптографии, статических ARP-таблиц, hosts файлов вместо выделенных DNS-серверов, использование или неиспользование определённых операционных систем и другие методы.

Следующая группа методов защиты от удалённых атак – программно-аппаратные. К ним относятся:

* программно-аппаратные шифраторы сетевого трафика;
* методика Firewall;
* защищённые сетевые криптопротоколы;
* программные средства обнаружения атак (IDS – Intrusion Detection Systems или ICE – Intrusion Countermeasures Electronics);
* программные средства анализа защищённости (SATAN – Security Analysis Network Tool for Administrator, SAINT, SAFEsuite, RealSecure и др.);
* защищённые сетевые ОС.

В общем случае методика Firewall реализует следующие основные функции:

1. Многоуровневая фильтрация сетевого трафика;
2. Proxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте. Смысл proxy-схемы заключается в создании соединения с конечным адресатом через промежуточный proxy-сервер на хосте Firewall;
3. Создание приватных сетей с “виртуальными” IP-адресами. Используется для скрытия истинной топологии внутренней IP-сети.

Здесь можно выделить подгруппу методов защиты – программные методы. К ним относятся прежде всего защищённые криптопротоколы, используя которые можно повысить надёжность защиты соединения.

 Список использованных информационных ресурсов:

1. И.Д.Медведовский, П.В.Семьянов, Д.Г.Леонов *Атака на Internet 2-е изд., перераб. и доп. –*М.: ДМК, 1999.
2. Э.Немет, Г.Снайдер, С.Сибасс, Т.Р.Хейн *UNIX: руководство системного администратора:* Пер. с англ. –К.: BHV, 1996
3. В.Жельников *Криптография от папируса до компьютера.* –M.: ABF, 1996
4. Материалы журнала “Компьютерра” (http://www.computerra.ru)
5. Server/Workstation Expert, August 1999, Vol. 10, No. 8.
6. Глобальные сети и телекоммуникации, №№ 01/1998, 06/1998
7. Материалы конференций сети FidoNet: *RU.NETHACK*, *RU.INTERNET.SECURITY*
8. Список рассылки BugTraq (BUGTRAQ@SECURITYFOCUS.COM)
9. HackZone – территория взлома (http://www.hackzone.ru)
10. Библиотека Сетевой Безопасности (http://security.tsu.ru)
11. Сайт компании Internet Security Systems (http://www.iss.net)
12. У.Гибсон *Нейромант* –М.: ТКО АСТ; 1997