**Содержание**

[Введение 3](#_Toc197083425)

[1. Проблемы защиты информации 4](#_Toc197083426)

[2. Средства защиты информации 6](#_Toc197083427)

[3. Информационная безопасность в Internet 6](#_Toc197083428)

[Заключение 7](#_Toc197083429)

[Список литературы 9](#_Toc197083430)

# Введение

Internet - глобальная компьютерная сеть, охватывающая весь мир. Сегодня Internet имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь раз­личных информационных сетей, принадлежащих различным учреждениям во всем мире, одна с другой.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи распреде­ленного доступа к ресурсам. Около двух лет назад были созданы оболочки, поддержи­вающие функции сетевого поиска и доступа к распределенным информационным ресур­сам, электронным архивам.

Internet, служившая когда-то исключительно исследовательским и учебным груп­пам, чьи интересы простирались вплоть до доступа к суперкомпьютерам, становится все более популярной в деловом мире. Компании соблазняют быстрота, дешевая глобальная связь, удобство для проведения совместных работ, доступные программы, уникальная база данных сети Internet. Они рассматривают глобальную сеть как дополнение к своим собственным локальным сетям.

 Фактически Internet состоит из множества локальных и глобальных сетей, принад­лежащих различным компаниям и предприятиям, связанных между собой различными линиями связи. Internet можно представить себе в виде мозаики сложенной из небольших сетей разной величины, которые активно взаимодействуют одна с другой, пересылая файлы, сообщения и т.п.

В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до про­гноза погоды на завтра. Кроме того Internet предоставляет уникальные возможности де­шевой, надежной и конфиденциальной глобальной связи по всему миру. Это оказывается очень удобным для фирм имеющих свои филиалы по всему миру, транснациональных корпораций и структур управления. Обычно, использование инфраструктуры Internet для международной связи обходится значительно дешевле прямой компьютерной связи через спутниковый канал или через телефон.

Электронная почта - самая распространенная услуга сети Internet. В настоящее время свой адрес по электронной почте имеют приблизительно 20 миллионов человек. Посылка письма по электронной почте обходится значительно дешевле посылки обыч­ного письма. Кроме того сообщение, посланное по электронной почте дойдет до адресата за несколько часов, в то время как обычное письмо может добираться до адресата не­сколько дней, а то и недель.

# 1. Проблемы защиты информации

Internet и информационная безопасность несовместны по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet - хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы - файлы и программы, не говоря уже о возможности их порчи и корректировки.

Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ прост -“халява”, то есть дешевизна программного обеспечения (TCP/IP), легкость доступа в Internet.

Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты 10Base-T и кабельного модема обеспечивают высокоскоростной доступ (10 Мбит/с) к локальному Web-серверу через сеть кабельного телевидения.

Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

1. ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web;
2. заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Internet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов;
3. перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Безопасность данных является одной из главных проблем в Internet. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Дилемма безопасности такова: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

Это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена на сто процентов.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

# 2. Средства защиты информации

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску безопасность Вашей локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT Coordination Center в 1999 году было зарегистрировано 2421 инцидентов - взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1995 число незаконных вторжений возросло на 48.9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов - “хакеров” является применение межсетевых экранов - брэндмауэров (firewalls).

Стоит отметить, что в следствии непрофессионализма администраторов и недостатков некоторых типов брэндмауэров порядка 30% взломов совершается после установки защитных систем.

Не следует думать, что все изложенное выше - “заморские диковины”. Всем, кто еще не уверен, что Россия уверенно догоняет другие страны по числу взломов серверов и локальных сетей и принесенному ими ущербу, следует познакомиться с тематической подборкой материалов российской прессы и материалами Hack Zone (Zhurnal.Ru).

Не смотря на кажущийся правовой хаос в рассматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и нормативных документов, а все используемые системы подлежат обязательной сертификации Государственной Технической Комиссией при президенте России.

# 3. Информационная безопасность в Internet

Архитектура Internet подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов вовне, что предъявляет повышенные требования к защите информации.

В Internet-системах используется подход клиент-сервер, а главная роль на сегодняшний день отводится Web-сервису. Web-серверы должны поддерживать традиционные защитные средства, такие как аутентификация и разграничение доступа; кроме того, необходимо обеспечение новых свойств, в особенности безопасности программной среды и на серверной, и на клиентской сторонах.

Таковы, если говорить совсем кратко, задачи в области информационной безопасности, возникающие в связи с переходом на технологию Inernet. Далее мы рассмотрим возможные подходы к их решению.

Формирование режима информационной безопасности - проблема комплексная.

Меры по ее решению можно разделить на четыре уровня:

* законодательный (законы, нормативные акты, стандарты и т.п.);
* административный (действия общего характера, предпринимаемые руководством организации);
* процедурный (конкретные меры безопасности, имеющие дело с людьми);
* программно-технический (конкретные технические меры).

# Заключение

Проблема защиты информации в Internet ставится и, с той или иной степенью эффективности, решается с момента появления сетей на основе протоколов семейства TCP/IP.

В эволюциях технологий защиты можно выделить три основных направления. Первое — разработка стандартов, имплиментирующих в сеть определенные средства защиты, прежде всего административной. Примером являются IP security option и варианты протоколов семейства TCP/IP, используемые в Министерстве обороны США. Второе направление — это культура межсетевых экранов (firewalls), давно применяемых для регулирования доступа к подсетям. Третье, наиболее молодое и активно развивающееся, направление — это так называемые технологии виртуальных защищенных сетей (VPN, virtual private network, или intranet).

Наблюдаемый в последние годы взрывной рост популярности Internet и связанных с ней коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в TCP/IP-сетях. Причем если ранее, вплоть до начала 90-х, основной задачей защиты в Internet было сохранение ресурсов преимущественно от хакерских атак, то в настоящее время актуальной становится задача защиты коммерческой информации.

Выбор технологии защиты информации для большой открытой системы — сети масштаба Internet, крупной корпоративной сети, сети коммуникационного провайдера, должен удовлетворять ряду специфических требований:

* наличие *открытой* спецификации, отсутствие монополизма в части технологических решений
* *широкая масштабируемость* решений по техническим и ценовым параметрам
* *универсальность технологии, переносимость, многоплатформенность*
* *совместимость* аппаратных, программных, коммуникационных решений
* обеспечение, при необходимости, *комплексной* защиты информации
* простота управления ключами и организации защищенных коммуникаций для вновь подключенных пользователей.

# Список литературы

* 1. Браун С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. c англ. - М.: Мир: Малип: СК Пресс, 1996. - 167c.
	2. Гилстер П. Новый навигатор Internet: Пер с англ. -Киев: Диалектика, 1996. - 495 c.
	3. Игер Б. Работа в Internet / Под ред. А. Тихонова; Пер. c англ. - М.: БИНОМ, 1996. - 313 c.
	4. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windiws Sockets. - Диалог - МИФИ, 1996. - 283 c.