

*Калугина М.В.,  
студентка 4 курса очного обучения,  
кафедра «Информационные системы и технологии»,  
Поволжский государственный университет  
телекоммуникаций и информатики,  
г. Самара, Россия*

*Научный руководитель: Бедняк С.Г.,  
к.п.н., доцент,  
кафедра «Информационные системы и технологии»  
Поволжский государственный университет  
телекоммуникаций и информатики,  
г. Самара, Россия*

## **ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В INTERNET**

**Аннотация:** В работе рассматриваются основные способы защиты информации, а также методы по обеспечению информационной безопасности в Internet.

**Ключевые слов:** Защита информации, глобальная компьютерная сеть, электронная почта, межсетевые экраны, безопасность данных, корпоративная сеть.

**Annotation:** The paper discusses the main ways of protecting information, as well as methods to ensure information security in Internet.

**Keywords:** information security, global computer network, email, firewalls, data security, corporate network.

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.

### 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 обосновательны, 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.

#### 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.

### 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 Internet. 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).

## Список литературы

1. Браун С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. с англ. - М.: Мир: Малип: СК Пресс, 1996. - 167с.
2. Гилстер П. Новый навигатор Internet: Пер с англ. -Киев: Диалектика, 1996. - 495 с.
3. Игер Б. Работа в Internet / Под ред. А. Тихонова; Пер. с англ. - М.: БИНОМ, 1996. - 313 с.
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 с.