В.К. СТЕПАНОВ,
профессор Московского государственного университета культуры и искусств

Меры безопасности при работе в Интернете

Приступая к работе в Интернете, стоит сразу же серьезно отнестись к вопросам безопасности.

Возрастание роли Сети в жизни цивилизации неминуемо привлекает в нее большое число отдельных лиц и целые организации, стремящиеся использовать Интернет-технологии для решения различного рода неблаговидных задач.

Лица, занимающиеся в Сети противозаконными действиями, традиционно именуются «хакерами». Первоначально это слово обозначало высококвалифицированных программистов, которые могли добиться оптимальной работы компьютерной программы при минимальном объеме программного кода. Однако с течением времени этот термин закрепился именно за компьютерными взломщиками и приобрел негативное значение. Хакерское сообщество весьма разнородно и имеет множество «специализаций» (фрикеры, кардеры, фишеры, спамеры, фармеры и др.), которые описаны в соответствующей литературе.

Сообщество это, являющееся в социальном смысле ярчайшей иллюстрацией сетевой субкультуры, имеет не только свои сайты, но и издаваемые на глянцевой бумаге периодические издания и регулярно проводимые в реальной жизни съезды и симпозиумы.

Одним из основных инструментов хакерских атак являются систематически распространяемые компьютерные вирусы (вредоносные компьютерные программы). Появление первых компьютерных вирусов, распространяемых через Интернет, датируется 1991 годом. Прошедшее с той поры время было потрачено вирусописателями отнюдь не впустую. Сегодня именно Интернет является основным каналом распространения вредоносных программ. Ситуация отягощается тем, что если в 90-х годах прошлого века хакерами двигал в значительной степени спортивный интерес, то в настоящее время сетевые злоумышленники в точном соответствии со своими реальными прототипами целенаправленно стремятся прежде всего к личному обогащению. **Это заставляет уделять все большее внимание мерам безопасности при работе в Интернете.**

Варианты злонамеренного использования Сети весьма и весьма разнообразны, но в самом обобщенном виде могут быть сведены к следующим разновидностям:

- **проникновение извне на компьютер пользователя (в компьютерную сеть организации) с целью кражи или порчи хранящихся там данных или выведения из строя оборудования;**
- **кража пересылаемой через Интернет конфиденциальной информации;**
- **рассылка по электронной почте спама (незапрашиваемой, нежелательной корреспонденции, носящей, прежде всего, рекламный характер).**

Первый вариант наиболее опасен, поскольку, при умелых действиях электронных взломщиков, приводит к получению ими полного контроля над компьютером пользователя или всей локальной сетью учреждения. Пагубные последствия этого очевидны: любая хранящаяся в компьютере информация может быть безвозвратно уничтожена, похищена или

изменена без ведома владельца компьютера. Это в полной мере относится не только к текстовым документам, но и к базам данных, которые составляют основную ценность для информационных учреждений. Для библиотек реальна угроза утраты электронного каталога, сведений о читателях, данных об оплате услуг, а также получения хакерами несанкционированного доступа к ресурсам, предоставляемым на платной основе.

Второй вариант крайне опасен при осуществлении через Сеть платежей и передаче конфиденциальных сведений персонального характера. Применительно к работе информационных учреждений эта угроза связана, прежде всего, с утратой сведений о паролях для доступа к удаленным коммерческим информационным ресурсам. Перехватив передаваемый по сетевым каналам пароль, злоумышленник может неограниченно пользоваться закрытым ресурсом или каким-либо сервисом за счет библиотеки (например, приобретать литературу в электронных книжных магазинах).

Рассылка спама на первый взгляд наименее опасная угроза. Однако необходимо знать, что **именно посредством спама распространяется большая часть вирусов, скрытая активация которых может создать базу для начала хакерской атаки на конкретный компьютер или компьютерную сеть всего учреждения.**

Несмотря на то, что основные заботы по обеспечению информационной безопасности лежат на системном администраторе организации, всем пользователям также стоит знать и применять меры предосторожности, обеспечивающие безопасную работу в Интернете.

Прежде всего, в обязательном порядке на компьютер должна быть установлена **антивирусная программа**. Задача таких программ — обеспечить комплексное предохранение компьютера от угроз различного вида. Помимо контроля содержания входящих писем и загружаемых web-страниц, программы блокируют работу занесенных вирусов, а зачастую обеспечивают и защиту от несанкционированного проникновения на компьютер извне. Арсенал антивирусных программ весьма разнообразен. Наибольшее распространение во всем мире, включая Россию, получили такие программы, как Dr.Web, Kaspersky AVP, McAfee VirusScan, Norton AntiVirus, Panda AntiVirus.

Свидетельствовать о заражения компьютера могут в совокупности или по отдельности следующие признаки:

- **значительное замедление работы компьютера при запуске программ, частые зависания и сбои в работе;**
- **исчезновение отдельных файлов или целых каталогов, а также искажение их содержимого;**
- **самопроизвольный запуск программ;**
- **сообщения корреспондентов, с которыми ведется переписка, о большом количестве писем, пришедших с вашего адреса, которые явно не отправлялись;**
- **неоправданно частое обращение к жесткому диску компьютера.**

При проявлении подобных признаков необходимо отсоединить компьютер от сети (для этого достаточно просто выдернуть из системного блока сетевой кабель) и произвести полное обследование компьютера с помощью антивирусной программы. Как правило, с помощью такой проверки удается выявить и обезвредить прокравшиеся вредоносные программы, после чего можно продолжать работу.

Рекомендуется периодически (примерно раз в месяц) производить полную антивирусную проверку компьютера, даже если машина ведет себя внешне нормально. Это усилит защиту и позволит устранить потенциальную угрозу до момента, когда вирус начтет активные разрушительные действия. Следует помнить, что антивирусное программное обеспечение должно систематически обновляться, иначе эффективность его работы снижается во много раз — новые вирусы появляются ежедневно, и старая антивирусная программа может просто не распознать недавно написанный вирус, что поставит компьютер под угрозу.

Соединение с Интернетом рекомендуется защищать с помощью специальной функции, именуемой «брандмауэр». Стоит периодически визуально проверять активное состояние брандмауэра: об этом свидетельствует маленькая пиктограмма в виде замочка или щита, дополняющая традиционную иконку сетевого подключения.

В ходе работы в Интернете следует избегать посещения сайтов сомнительного содержания.

Исключения существуют всегда, но общее правило таково, что наиболее вирусонасыщены сайты эротико-порнографического характера и сайты, содержащие якобы бесплатное программное обеспечение или ключи (пароли, серийные номера, «крэки») для активации условно бесплатных программных продуктов. Попытка выгрузки из Сети пиратского программного обеспечения или программ активации, скорее всего, приведет к заражению компьютера, которое происходит «под прикрытием» установки желаемой программы. При этом пользователь, скорее всего, не заметит, что компьютер заражен, а вредоносная программа только и ждет соединения с Интернетом, чтобы начать выполнять свою неблаговидную задачу.

Работа с электронной почтой также требует большой осторожности. К сожалению, начинающие пользователи обычно пренебрегают требованиями безопасности. Беспечность, как правило, обычно проходит после первого заражения, которое зачастую приводит к необходимости переустановки операционной системы и потере результатов длительной работы.

Главную опасность, как уже было отмечено, представляет спам. Проблему нежелательной почты лучше решать с самого начала, а именно — стараться не афишировать адрес почтового ящика, не регистрируясь на общедоступных форумах и листах рассылки форумов без серьезной на то необходимости. Однако рано или поздно почтовые адреса становятся достоянием спамеров. Это происходит разными путями — от кропотливого сбора визитных карточек на разного рода выставках и конференциях, до изощренной хакерской атаки на почтовые серверы организаций с целью кражи адресных книг, содержащих сведения о всех внутренних и внешних корреспондентах.

Нежелательная почта сама по себе весьма разнородна. Наименее опасны «правдивые» сообщения, в которых действительно предлагаются различные товары и услуги. Вред от такого рода сообщений ограничивается потерей времени на их сортировку, удаление и затраченный на них трафик. Заголовки писем («Профессионально оцифруем ваши кино/видео/фото/аудиоархивы», «Таможенное оформление грузов», «Сложные вопросы признания “прочих расходов”» и т.д.), как правило, точно выражают суть предложения, и, что крайне важно, сами письма подобного рода не содержат приложений.

Гораздо большую опасность представляют письма, содержащие приложения, поскольку именно в них и скрываются вирусы. Темы их заголовков могут быть самыми различными, а в теле писем помещается текст, который на первый взгляд выглядит вполне невинно. Заголовки таких сообщений могут быть эмоционально-игривыми («Когда ты ко мне приедешь», «Привет, напиши мне!!!», «Когда ты мне ответишь?»), интригующими («Я тебя сегодня видела», «За вами следят и подсматривают») или поделовому сухими («Исходный документ в приложении»). Содержание писем может быть сколь угодно различным, но направленным на реализацию одной задачи — **в результате прочтения пользователь должен открыть вирусосодержащее приложение.**

Ниже приводятся примеры реальных писем, содержавших в приложении опасные вирусы:

«Привет! Давно от тебя никаких новостей не слышно что-то... Ты где вообще пропадаешь? Я тут файл приложил, давно хотел отправить, но всё забывал. Там всё просто, откроешь, сразу разберешься. Удачи!!!».

«Привет! Ты сегодня мне позвонишь???? Я уже не могу ждать! Пока думаешь, посмотри программку, которую тебе прислала, ну как? Правда, здорово?».

«Привет, в Интернете появился новый вирус, высылаю тебе заплатку... Установи, пока ещё твой компьютер не заразился. Пока! Напиши мне!».

Следует иметь в виду, что фантазия у спамеров чрезвычайно развита, поскольку от нее на-

прямую зависит степень успеха и, следовательно, уровень доходов. Каждый день рождаются все новые ухищрения, призванные привлечь внимание доверчивых пользователей и одновременно усыпить бдительность владельцев атакуемых почтовых ящиков.

Разновидностью вирусоопасного спама является рассылка, имитирующая сообщения о присланных пользователю открытках. Сообщение о пришедшей открытке в таких письмах сопровождается ссылкой, которая ведет на сайт, оформлением напоминающий стандартный «открыточный» сервис (например, postcards.ru или e-cards.com), но не содержащий ничего, кроме вирусов. **Расчет делается на то, что обделенный вниманием пользователь, обрадовавшись неожиданному знаку внимания, кликнет на ссылку и будет инфицирован при заходе на сайт.**

Меры предосторожности при работе с электронной почтой целиком и полностью лежат на пользователе. Практика показывает, что любые антиспамовые модули несовершенны, а антивирусные программы не всегда в состоянии корректно распознать угрозу.

Поэтому каждый пользователь обязан внимательно относиться к пришедшей корреспонденции и соблюдать следующие несложные меры предосторожности.

Прежде всего, необходимо обращать внимание на обратные адреса полученных писем. Опытный глаз всегда может распознать спам уже по одному наименованию почтового ящика, с которого они пришли. Как правило, имена почтовых ящиков состоят из бессмысленного набора букв и цифр (wes00sinclair@autotown.com, thu-ji6537@bayou.com, tuan67574@barbary.com, bqsilva@wish.nl, servants5talking@saic.com, a_@porta.net, getting9understand@ey.com). Темы сообщений, в которых предлагаются какие-то товары или услуги, также красноречиво говорят о том, что данное сообщение относится к спаму. **Все эти письма можно удалять не читая, не беспокоясь о потере действительно важной корреспонденции.**

Столь же безжалостно удаляются письма от неизвестных корреспондентов с любыми приложениями, если в них нет конкретного обращения по имени владельца почтового ящика и связанного текста, адекватно поясняющего причину обращения и содержание приложения. Использование в качестве имени для обращения названия почтового ящика (например, «Уважаемый vstepanov!») также свидетельствует о том, что данное сообщение является спамом и, скорее всего, содержит вирус.

При получении письма с приложением от знакомых адресатов, если оно не является ожидаемым и в нем не поясняется содержание приложения, также следует быть осторожным.

Бдительность не должна быть усыплена наличием некоего приветственного текста, наподобие «Посмотри, это весело!», «Это то, что Вы просили». В данном случае настоятельно рекомендуется запросить корреспондента, с адреса которого получено письмо, посылалось ли данное сообщение и не является ли приложение вирусом. С большой долей вероятности можно утверждать, что в данном случае имел место взлом используемого корреспондентом почтового сервера, в результате которого хакеры получили в свое распоряжение базу адресов, с которыми велась переписка, и спешат использовать открывшуюся возможность в своих неблаговидных целях. Такого рода атаки являются наиболее опасными в силу того, что письма с привычных адресов вызывает намного меньше подозрений и вероятность открытия приложений к ним, равнозначная инфицированию компьютера, гораздо выше.

С помощью специальных опций почтовых клиентских программ можно значительно уменьшить риск заражения. Так, например, опция «Диспетчер почты» в The Bat позволяет все подозрительные письма удалять непосредственно на почтовом сервере, что дает возможность не только в некоторых случаях сэкономить трафик, но и не подвергать непосредственной опасности почтовый ящик, расположенный на пользовательском компьютере. В то же время необходимо помнить, что при открытии зараженного приложения к письму, пришедшему на бесплатный почтовый ящик (например на mail.ru, freemail.ru и т.п.), угрозе подвергается именно тот компьютер, на котором открывается приложение.

Все требования по безопасности должны неукоснительно выполняться каждым пользователем с первого дня работы в Сети. Это застрахует и его самого, и всех клиентов локальной сети от проникновения вредоносных программ, которые могут нанести огромный ущерб всей компьютерной сети библиотеки. И, наоборот, пренебрежение мерами безопасности рано или поздно гарантированно приведет к возникновению проблем в работе программного, а возможно, и аппаратного обеспечения. **Гораздо лучше соблюдать описанные требования, нежели на собственном опыте убедиться, что Интернет является ареной невидимых битв, а серверы библиотек, как наименее защищенные, часто используются хакерами для тренировок.**