Интернет: техника безопасности

Илья Рюмин, *преподаватель информатики, Москва*

Одни называют Интернет современным проклятием, другие — последним островом свободы, третьи — всего лишь усовершенствованным телефоном. Здесь мы рассмотрим одну интересную сторону Сети: словесные поединки.

Вы спросите: так речь идёт о риторике? И да, и нет. С одной стороны, речь действительно пойдёт о риторике, как искусстве словесного поединка. Но есть одно маленькое отличие. Слово «риторика» ассоциируется у нас с древними греками или средневековыми схоластами. Возможно также — с современными теледебатами, с дискуссией реальных людей лицом к лицу. Но у споров в Интернете есть своя замечательная специфика. Так что речь пойдёт о риторике, но в новых, необычных условиях.

Главная отличительная черта дискуссий в Интернете — это полнейшая безнаказанность. Будем называть вещи своими именами. Причём «безнаказанность» не только в смысле Уголовного кодекса, а гораздо шире. Когда вы разговариваете в реале, то вас с собеседником связывает куча взаимных ограничений. Если вы встретились с этим человеком на работе, это — ваш коллега, с которым потом придётся иметь дело. Или, хуже того, начальник. Если дома — ваш родственник. Если он на вас обидится, то потом «отомстит». Сделает гадость или не окажет привычной услуги, или окажет, но не в привычном размере…

Даже если вы едете в поезде и говорите с вашим попутчиком, то вы не вполне безнаказанны. Если он обидится, то вам придётся какое-то время терпеть его присутствие рядом со всеми вытекающими последствиями. Наконец, дело может дойти до мордобоя или нанесения ущерба вашей собственности.

В Интернете — не так. Единственный метод воздействия на вас — слова. Единственный ваш метод воздействия на других — тоже слова. При желании можно сохранять полную анонимность, так что добраться до вас в реале будет невозможно. Если не делать совсем уж больших глупостей, то также невозможно и «взломать» ваш компьютер. Вероятность столкновения с хакерами экстра-класса пренебрежимо мала.

Тут может возникнуть одно возражение. А именно: кто-нибудь вспомнит о модераторах. Но что может сделать вам модератор? Максимум — заблокировать вам доступ в одно только это место. Неприятно — всё-таки теряется интересный круг общения. Но не более того. Вообще, тема модераторства стоит отдельного разговора немного позднее.

С другой стороны, полная безнаказанность распространяется не только на вас, но и на вашего собеседника. Вы остаётесь перед лицом человека, на которого можете влиять словом и только словом. Голый разум против голого разума. Подкуп, угрозы, шантаж, насилие, обольщение — все эти традиционные методы реала оказываются не у дел, если хотя бы одна из сторон отказывается предоставить достаточно сведений о себе. Даже если такие сведения обнародованы, они вполне могут оказаться ложными.

Для начала немного о технике безопасности. Как уже говорилось, анонимность может сделать вас неуязвимым ко всему, кроме чужих слов. Это удобно. Однако есть в этом и минус.

Что если вы пришли на этот форум или в этот чат не только для ругани? Что если вы хотите рассказать о своей работе или увлечениях? Оставить ссылку на свой сайт или место работы? Сохранить за собой авторство материалов, опубликованных на этом форуме? В такой ситуации вам придётся раскрыть своё инкогнито.

Вот только ни к чему раскрывать его полностью. Явно не следует называть домашний адрес и телефон. Лучше не уточнять место работы или учёбы. Стоит ли раскрывать настоящее имя? Спорный вопрос. Те люди, которые готовы перейти от ссоры в Сети к ссоре в реале, как правило, весьма тупы. Они не смогут найти вас по вашему имени и городу проживания.

И наоборот: те люди, которые действительно способны вас найти, обычно ограничиваются

угрозами. Но всегда можно наткнуться на исключение. Решайте сами, насколько велик риск в вашем случае. Хорошим компромиссом является постоянный и достаточно запоминающийся псевдоним. По нему вас можно легко узнать, но трудно найти.

Не применяйте для доступа к форуму или чату тот же пароль, что и для вашей почты, ICQ и так далее. Этот пароль обычно известен только модераторам форума. Однако, во-первых, вы можете когда-нибудь с ними поссориться. А во-вторых, форум могут когда-нибудь взломать.

Не применяйте пароль, который легко подобрать. А легко подобрать пароли, которые являются обычным словом русского или английского языка, русским или английским именем, иногда в комбинации с цифрами. Или то же самое, но в обратном порядке. Плохи пароли из соседних букв типа qwerty или qaz. Плохи очень короткие пароли. Постарайтесь составить пароль из случайного набора символов. Или, если вы не способны запомнить такой пароль, то составьте его как комбинацию из нескольких слов с намеренными ошибками.

При регистрации на форуме или в чате часто требуется указать e-mail. Никогда не указывайте домашний или рабочий e-mail. Даже если администрация чата клятвенно гарантирует его неразглашение, этим клятвам не надо верить. Чат могут взломать или вы рассоритесь с администрацией. Заведите «мусорный» бесплатный почтовый ящик на любой почте, укажите его.

Никогда не указывайте свой домашний или рабочий e-mail при общении. Это грозит вам следующими неприятностями:

- Вы начнёте регулярно получать по почте спам.
- Ваш почтовый ящик могут намеренно переполнить мусором, за скачивание которого вам же и придётся платить.
- Вам начнут присылать вирусы и трояны.

При некоторых видах общения в Сети вашему собеседнику становится известен ваш IP адрес. Вопреки распространённому мнению, это само по себе ещё не несёт опасности. Опасность несут дыры в операционной системе вашего компьютера и, особенно, в почте.

А если злоумышленнику неизвестен ваш IP, то он не знает даже кого атаковать. Поэтому, не стоит всем говорить свой IP, но если он стал известен, не стоит и паниковать. Нужно напороться на действительно могучего хакера, чтобы он смог взломать ваш компьютер, зная лишь IP-адрес.

Если хозяин компьютера соблюдает все стандартные меры безопасности, то для его взлома требуется хакер экстра-класса. Таких специалистов в Сети — раз, два и обчёлся. И слишком маловероятно, что он захочет тратить время на вас.

Хорошо защищённый домашний компьютер взломать гораздо труднее, чем столь же защищённый сервер общего пользования (например, тот, на котором находится форум или чат). Просто потому, что сервер гораздо более «открыт» для внешнего мира. Но это только при соблюдении мер безопасности: увы, в этом отношении владельцы домашних компьютеров гораздо беспечнее, чем владельцы серверов.

Хакеры обычного среднего уровня действуют двумя основными способами. Первый — это применение известных ошибок в операционной системе (которые до них нашли хакеры экстра-класса). Но об этих ошибках становится быстро известно и создателям операционных систем. Поэтому, чтобы избежать подобных атак, надо просто вовремя обновлять программное обеспечение и ставить «заплаты».

С появлением Windows XP это стало совсем просто (технология Windows Update). Про своевременное обновление баз антивирусов я не говорю: обычно антивирусы об этом автоматически напоминают.

Необходимо вовремя ставить «заплаты» и на другие программы, особенно, если эта программа широко популярна и использует файлы, скачанные из Сети. Это относится, например, к такой программе, как проигрыватель WinAmp. Файл музыки в формате MP3, даже если он содержит вирус, ещё не опасен. Но вот если его запустить WinAmp-ом, который содержит «дыру» в защите, тогда вирус активизируется. Если же вы своевременно ставите «заплаты», тогда эта проблема решается. Причём, я имею в виду именно заплаты, а не скачивание новых версий. Сырые свежие версии программ как раз могут иметь много «дыр».

Ещё один способ обойти эту проблему — использовать не самые популярные программы, а сравнительно редкие. Очень часто самая распространённая программа — ещё не самая лучшая. Есть и другие, которые ничем не хуже. Например, можно использовать бра-

узер Firefox вместо Internet Explorer, проигрыватель DivX вместо стандартного проигрывателя Windows, пейджер Miranda вместо ICQ, и т.д. Разумеется, «редкие» программы тоже содержат «дыры», но злоумышленники гораздо реже их «ломают».

Второй путь взлома вашего компьютера средним хакером — это ваша собственная глупость. Чтобы избежать такого рода проблем, достаточно соблюдать несколько простых правил «компьютерной гигиены»:

• Не ленитесь придумывать трудно отгадываемые пароли. Подробности см. выше.
• Не ленитесь придумывать разные пароли для разных случаев. Подробности см. выше.
• Если при регистрации вам предлагается ввести ключевой вопрос-ответ для восстановления забытого пароля, помните, что этой возможностью с удовольствием воспользуется хакер. Откажитесь от этой «услуги» или же придумайте ответ такой же трудно отгадываемый, как и пароль.

Никогда не скачивайте из Сети программы с сомнительных сайтов. Особенно с порнографических и хакерских. Вообще не копируйте себе на компьютер программы, взятые из сомнительных источников. В программе может быть вирус или троян.

Если берёте программу у знакомого, то учтите, что он может и не знать о её заражённости. Флэшки, скачиваемые в виде exe-файлов, могут быть и заражены — аккуратнее с ними. Также заражёнными могут быть doc-файлы для Microsoft Word. Вполне безопасно качать музыку, картинки, фильмы, потому, что всё перечисленное — это не программы.

Если по почте пришло письмо с вложением (attachment) и вы не знаете, от кого оно, стирайте его, не читая. Не пытайтесь открыть и изучить прикреплённый файл. Именно такие попытки обычно активизируют вредоносную программу, спрятанную в письме. Если всё же распирает любопытство, обратитесь к специалисту (не к пацану соседскому!), он это сделает с соблюдением всех мер предосторожности.

Если по почте пришло письмо с вложением (attachment) и вы знаете, от кого оно, но этот ваш знакомый не собирался вам ничего присылать, стирайте его, не читая. Помните, что обратный адрес под силу подделать даже совсем слабенькому хакеру.

Если вам пришёл спам, не отвечайте на него. Если в нём предлагается отказаться от этой рассылки, не поддавайтесь на уловку и не отказывайтесь. Любой ваш ответ подтвердит спамеру, что вы читаете его мусор, и вам пришлют потом в 10 раз больше спама. Вообще не кликайте на ссылки в подозрительных письмах.

Не принимайте за чистую монету письма, пришедшие якобы от администратора сети или чата или форума или от антивирусной системы или от какого-нибудь автоматической системы. В большинстве случаев это будет сетевой червь или троян. Если есть шанс, что письмо от администратора, не поленитесь ему позвонить, прежде чем выполнять какие-либо действия, которые рекомендуются в письме.

Не поддавайтесь на провокации типа «прочти и пошли другу». Это — тот же червь, но рассчитанный не на ошибки системы, а на человеческую глупость. То есть психологический червь. Самые известные черви такого рода — это «письма счастья», «поздравления» от малознакомых личностей и «голосования в защиту чего-нибудь». Подобные черви перегружают Сеть и тормозят её работу.

В общем, «кто предупреждён, тот вооружён». Соблюдайте элементарные правила безопасности — как правила дорожного движения — и ваша работа (и развлечения) в Интернете будут вполне безопасны.

Проверено неоднократно, и не только на собственном опыте.

❑