В постоянной рубрике «Эксперт» редакция «Сгущёнки» продолжает публиковать самые интересные лекции лучших преподавателей университета. Материал лекций носит научно-популярный характер и наверняка будет интересен широкому кругу читателей.

Вирусология

Сегодня основная масса студентов является активными пользователями ПК. Между тем, Интернет и носители информации таят в себе множество опасностей для наших компьютеров. Среди таких неприятностей – компьютерные вирусы, вредоносные программы и спам-сообщения. Что представляют из себя эти угрозы, каких разновидностей они бывают и каковы меры борьбы с ними? Об этом рассказал в своей лекции старший преподаватель кафедры прикладной информатики механико-математического факультета СГУ Леонид Валентинович Бессонов.

ФОТО НАТАЛИ КАЛИНИНОЙ

Интернет прочно вошёл в жизнь современного человека и занимает всё больше времени. Всё больше повседневных задач решается с помощью Всемирной паутины.

С усилением роли Интернета в нашей жизни растёт и обеспокоенность опасностями, которые он в себе таит. Так ли всё страшно? Многие преподаватели говорят, что «из-за Интернета» студенты стали меньше читать. Психологи теоретизируют об изменениях мышления, связанных со спецификой веб-информации, и добавляют про формирование так называемого «клипового мышления». Среди многообразия сетевых опасностей выберем и попробуем разобраться по существу с наиболее ощутимыми угрозами для студента.

Осторожно, вирусы!

Первое, что многим приходит в голову при упоминании интернет-угроз – компьютерный вирус. Зачастую непонимание природы вирусов позволяет свободно распространяться мифам, способствует нагнетанию обстановки и поощряет разного рода спекуляции.

Компьютерным вирусом называется программа, способная к саморазмножению. Такая программа, будучи запущенной, может создавать свои копии (точные или модифицированные). Зачастую механизм распространений устроен так, чтобы вирус переходил с одного компьютера на другой. Своё название компьютерные вирусы получили по аналогии с биологическими как раз за способность распространяться самостоятельно. Другой отличительной особенностью этих программ является скрытность их работы: как правило, проникновение вируса в компьютерную систему и прочие действия вируса происходят без ведома пользователя и совершенно незаметно для него.

Анатомия компьютерного вируса может быть простой или сложной, но условно его можно разделить на две части: механизм размножения и начинка. Механизм размножения определяет способ распространения и запуска вируса. Начинка вируса – это те действия, которые он будет выполнять, проникнув в компьютерную систему.

Вирусы: от милых до опасных

Бывают безобидные и даже милые вирусы. Например, экспертам-вирусологам известна программа, поздравляющая с днём рождения любимую маму автора. Вирус, периодически переворачивающий изображение на экране монитора «вверх ногами», тоже может быть расценен как шутка. Но бывают и весьма опасные вирусы.

Вирусы-разрушители уничтожают данные. Типичным примером такого злодея является «Чернобыль» (Win95.CIH), массовое распространение которого случилось в 1999 году. Этот вирус проверял при включении компьютера дату и если на календаре стояло 26 апреля уничтожал все данные на жёстком диске.

Также встречаются вирусы-шпионы. Их основная цель – сбор и отправка злоумышленнику важной конфиденциальной информации, например, номеров кредитных карт, паролей от почтовых ящиков и тому подобное. В настоящее время большое распространение получили вирусы-зомби. Их задача – внедриться в компьютер жертвы и ждать специальную команду от своего автора. Множество заражённых этим вирусом компьютеров называют «зомби-сетью». В 2003 году мир познакомился с одним таким «зомби» – вирус MsBlast был предназначен для атаки на сайт автоматической системы обновлений Windows. 16 августа 2003 года со всех заражённых вирусом компьютеров непрерывным потоком шли запросы к этому сайту, в результате чего сервер был перегружен и вышел из строя. Не о каждом таком вирусе становится известно общественности. «Зомби-сети» часто используются для того, чтобы «подмочить» репутацию какого-нибудь банка или государственной структуры. Действительно, как же доверять банку, если он с вирусом справиться не может?.. Поэтому жертвы таких атак не спешат рассказывать миру о приключившемся с ними. К слову, продажа «зомби-сетей» уже давно превратилась в серьёзный бизнес.

Охотники за вирусами

Как же защититься от вирусов? Самой защищённой считается изолированная система, доступ к которой осуществляется под строгим контролем специалистов. Но что делать обычному пользователю? Без паники! Для начала убедимся, что компьютер «чист»: установим антивирус. Можно взять бесплатный, например, Avast или Avira, а можно и купить. Благо, сейчас неплохой «антивирус на год» стоит столько же, сколько средний студент тратит в месяц на проезд в автобусах. Установленный антивирус сам скачает свежие антивирусные базы и проверит компьютер. Вирусов нет? Отлично! Теперь нужно только следить за тем, чтобы вирусы не внедрились в нашу чистенькую систему. Для этого проверяй все носители данных, подключаемые к компьютеру (флешки, цифровые плееры, цифровые фотоаппараты, сотовые телефоны и так далее).

Простым, но действенным способом не «заразиться» является отказ от «автозапуска» при подсоединении носителя данных. Лучше открывать «проводник» и, выбрав флешку в дереве дисков и папок (левая часть окошка), сделать все необходимые операции с файлами. Также вирусы могут содержаться во вложениях к письмам электронной почты и на некоторых вебстраницах. От большей части таких угроз пользователя защищают «гиганты» Интернета. Например, поисковики Google и Яндекс будут предупреждать пользователя при переходе на сайт, с которого было замечено распространение вирусов. Также и с почтовыми системами: они автоматически проверяют подшитые к письмам файлы и уничтожают их, если находят вирус.

Надёжный пароль состоит из цифр, букв и знаков препинания.

Справедливости ради, нужно сказать, что не всякая вредоносная программа является вирусом. Специалисты по компьютерной безопасности называют вредоносной любую программу, которая устанавливается в компьютерной системе без ведома её владельца и осуществляет нежелательные действия. Так, например, есть так называемые троянские программы, которые часто относят к вирусам. Но в отличие от них трояны не имеют механизма распространения. Для попадания в компьютерную систему кто-то должен «приделать ноги» трояну. Внедрить троян может недоброжелатель, получивший доступ к компьютеру. С другой стороны, пользователь может попасться на какую-либо уловку при просмотре сайта или получении электронной почты, и, сам того не ведая, установить троян в систему. Программа может действовать так же, как вирусы-«шутники» или «разрушители», но бывают и более неприятные последствия. Например, некоторые трояны предоставляют злоумышленнику возможность управления компьютером жертвы. Чтобы «вредители» не подбросили троян, не оставляй компьютер без присмотра, когда рядом есть кто-то посторонний, и держи в тайне свой надёжный пароль (он ведь надёжный?;)).

Надёжный пароль состоит из цифр, букв и знаков препинания. Пароль не должен быть ожидаемым: в нём не должно быть имён и дат рождений.

Игры разума

Средства защиты от вирусов становятся всё надёжнее. Что же придумывают недремлющие злоумышленники? В XXI веке «расцвели» атаки, основанные на «социальных технологиях». Многие слышали такие слова, как «социальная инженерия», «фишинг». В основе таких угроз лежит человеческий фактор. Ничего не подозревающий пользователь получает письмо, подписанное тем, кому он готов доверять. Например: «Уважаемый пользователь! Почтовый сервер Mail.ru проводит проверку активности ящиков. Чтобы подтвердить, что ваш ящик используется, пошлите ответ на это письмо, в котором впишите имя владельца, логин, пароль, город проживания. С уважением, администрация Mail.ru». Жертва усыпляется техническими подробностями и витиеватыми объяснениями, а в итоге добровольно посылает злоумышленнику свой пароль. Такую же схему обмана применяют по телефону. Милый голос девушки в трубке: «Привет! Я вчера устроилась на работу, ещё не дали пароль доступа, а уже нагрузили делами. Можешь дать мне пока свой?».

Мошенничество становится всё более изощрённым и эксплуатирует наши лучшие чувства. Как же бороться? Не торопимся и включаем голову! Как бы нас ни старались испугать, поторопить, сбить с толку, остановимся и хладнокровно подумаем. Нужен ли мой пароль администрации почтовика, если они и без него могут видеть, захожу я в свой ящик или нет? Могли ли дать новому сотруднику задание, не дав инструмента для его выполнения? Если ситуация вызывает сомнения, посоветуйся с кем-то знающим. Главное не паникуй и не спеши выполнять требования подозрительного письма (звонка, сообщения в icq и так далее).

Фишинг — это другая техника жульничества. Вот типичный пример. Приходит сообщение в icq: «С кем это ты целуешься на этой фотке? http://vkontaket.ru/photo123123_321321». Пользователь заходит на сайт, вводит свой логин и пароль. Никакой фотографии нет. В чём же подвох? Внимательный читатель наверняка заметил, что адрес в ссылке «неправильный». Вместо «vkontakTE» написано «vkontakET». Сайт не тот! Но когда мы прошли по этой ссылке, мы увидели знакомый логотип, дизайн и окошко ввода пароля. В этом и есть ловушка. Жертва заходит на фальшивый сайт (социальной сети, банка или другой организации), думая, что он настоящий. Как только введён логин и пароль, обман удался: данные передаются злоумышленнику. Как же уберечься? Внимательно смотри на ссылки, приходящие по почте, в сообщениях icq и другими путями, особенно если эти сообщения содержат провокационный текст. Сложнее с сайтами банковских систем, их фишинг сулит злоумышленникам золотые горы. Но и защита таких сайтов выше: банки сами заботятся о безопасности и пресекают вредительство.

Есть и другие виды социальных технологий, менее распространённые. Один из них – «дорожное яблоко» – подразумевает «случайное» подбрасывание в людное место интересного диска (например, с логотипом города и подписью «Бух. зарплата, Сентябрь–2011» на нём). Из любопытства жертва может запустить такой носитель, установив тем самым уже известный нам троян или вирус. Всегда следует помнить: случайности очень редко происходят, а бесплатный сыр чаще всего бывает в мышеловке.

F-Secure

Смотрите выступление руководителя лабораторий по разработке антивирусного программного обеспечения F-Secure Микко Хюппонена «Борьба с вирусами, защита Сети» на сайте http://www.ted.com

СПАМ! СПАМ! СПАМ!

Спам – неприятная особенность Интернета – массовая назойливая рассылка рекламной и иной информации пользователям, которые вовсе не желали её получить. Чаще всего спам-письма или спам-сообщения рекламируют путешествия, медикаменты, элитные товары. Нередко при помощи спама рекламируется то, что сложно прорекламировать иными способами, например, порнография или пиратские программные продукты. Также спам используется в качестве антирекламы. Например, можно ежедневно рассылать тысячи писем с текстом: «Василий Иванович Пупкин – самый достойный кандидат в губернаторы нашей области!». Естественной реакцией пользователей будет неприязнь к этому «герою».

Спам представляет собой проблему как для пользователей, так и для организаций. Люди тратят драгоценное время на просмотр ненужных писем. Просмотреть одно письмо недолго, но что если этих писем 50, 100, 1000? Уходит время, рассеивается внимание, тратятся деньги (а вернее, они не зарабатываются, пока сотрудники читают спам, вместо того, чтобы работать). От захлёстывающих эмоций гибнут драгоценные нервные клетки.

Как спастись от этой напасти? Постарайся сделать так, чтобы почтовый адрес был меньше «засвечен» в сети. Не оставляй его на форумах, досках объявлений. Не подписывайся на сомнительные рассылки. Другим действенным методом борьбы являются антиспам-фильтры, но с ними важно не перестараться. Автоматический фильтр может случайно принять за спам нормальное письмо. В этом случае оно будет помещено в специальную папку почтового ящика (обычно она так и называется – «Спам»). Имеет смысл периодически просматривать эту папку, чтобы не потерять ценное письмо.

Современному человеку не прожить без Интернета. Это понимают как злоумышленники, так и специалисты по компьютерной безопасности. Пока простые пользователи спокойно спят, на просторах Интернета идёт непрерывная «борьба добра и зла». В наиболее важных и технически сложных операциях (к примеру, перевод денежных средств, защита персональных данных) покой рядовых пользователей берегут профессионалы. Но чем больше человек соприкасается с Интернетом в повседневной жизни, тем больше возникает «простых» случаев, когда безопасность зависит от спокойствия, рассудительности и разумности самого пользователя.

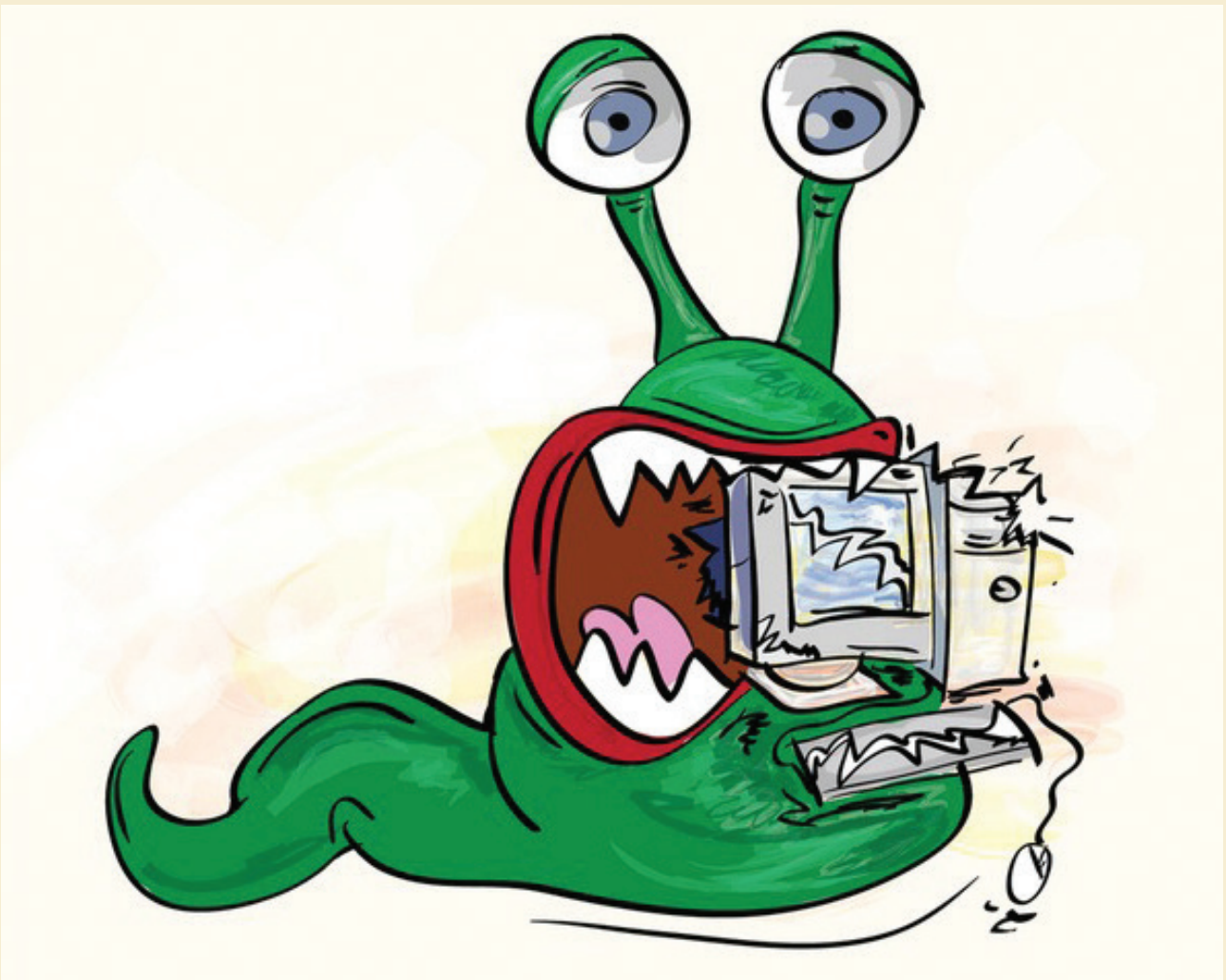

РИСУНОК ДМИТРИЯ ПОЗДНИКИНА