Александр Заика

КОМПЬЮТЕР ДЛЯ «ЧАЙНИКОВ»

Москва, 2017

УДК 004
ББК 32.973-018.2
З-17

Заика, А.

З-17 Компьютер для «чайников». Практическое пособие для успешной и безопасной работы на компьютере / А. Заика — М. : РИПОЛ классик / T8RUGRAM, 2017. — 160 с. : ил.

ISBN 978-5-519-61038-4

Прекрасная книга для пользователей PC начального и среднего уровней. В доступной для читателя форме автор представляет обзор основных компьютерных угроз, рассказывает об особенностях применения наиболее эффективных антивирусных программ, даёт практические советы по работе с программным обеспечением, освещает вопросы безопасности домашней (локальной) сети, организации резервного копирования, предлагает способы защиты от перебоев электропитания. Вы ознакомитесь с особенностями подбора компьютерного оборудования, а также с профилактикой вашего компьютера, и сможете выбрать оптимальный комплекс защитных мер с учётом безопасности пользователя.

УДК 004
ББК 32.973-018.2
BIC UTN
BISAC COM000000

ISBN 978-5-519-61038-4

Оглавление

Введение

Нередко люди задумываются о компьютерной безопасности слишком поздно. Обычно тогда, когда с их компьютером уже что-то произошло.

Представьте себе комнату, половина которой от пола до потолка забита распечатками документов. Эти документы нужно ввести в компьютер нескольким бухгалтерам. Зачем это? Просто потому, что в бухгалтерии случилось небольшое наводнение, жертвой которого пал компьютер, на котором хранились учетные данные. Если бы не счастливая случайность, им действительно пришлось бы выполнять титаническую работу. А ведь не всем так везет, хотя даже если данные, которые хранятся на компьютере, безвозвратно утеряны, некоторые превентивные меры позволяют их восстановить.

Представьте себе, что некто включает компьютер, а тот попросту не загружается. Включается, издает традиционный писк, возвещающий о том, что система прошла предварительную проверку, а потом — пишет что-то на экране и дальше дело не идет. Не помогает и перезагрузка. А на компьютере — дипломная работа — плод нескольких месяцев труда. Или архив фотоснимков за много лет, или важная статья, которую в редакции ждут через несколько часов. Что делать?

Бывает и так, что компьютер вдруг начинает работать хуже, чем обычно. Он слишком долго загружается, иногда необъяснимо «виснет», слишком сильно греется. Веб-браузер начинает работать как-то странно, периодически показывая странички, которые его никто не просил загружать. Пропадают какие-то файлы, портятся некоторые документы...

Или еще хуже — после загрузки компьютера на экран выводится окно, где пользователю предлагается отправить платное СМС на некоторый номер для того, чтобы получить код разблокировки компьютера. Работать на таком компьютере невозможно.

Некоторые люди становятся жертвами мошенников. Их обманывают, у них воруют деньги из электронных платежных систем. И хотя схемы компьютерного мошенничества обычно не так уж и сложны, если бы не было тех, кто верит

мошенникам, такого понятия как «афера» уже, наверное, не существовало бы.

А что, если злоумышленник взломает чей-то электронный почтовый ящик и сможет не только читать личную переписку, что само по себе очень неприятно, но и какое-то время писать письма от лица того, чей ящик взломан?

Компьютеры играют важную роль в жизни каждого из нас. Поэтому лучше всего задуматься о том, как защитить «электронного друга» от разного рода напастей, еще до того, как случилась какая-нибудь неприятность.

Эта книга о том, как защитить компьютер, информацию и собственные нервные клетки, которые, как известно, не восстанавливаются, от вирусов, хакеров, мошенников и прочих опасностей, которые подстерегают каждого, кто хотя бы раз в день нажимает на кнопку включения компьютера и берет в руки мышь. Книга рассчитана на пользователей, которые уже имеют некоторый опыт работы на компьютере и хотят повысить уровень защиты своей системы от различных угроз.

Глава 1
Что угрожает вашему компьютеру

Прежде чем рассматривать средства защиты от компьютерных неприятностей, поговорим о том, что угрожает компьютерам. Слово «компьютер» здесь используется в достаточно широком смысле, под «компьютером» имеется в виду как аппаратное обеспечение (системный блок, монитор и прочее), так и программы, и данные, которые хранятся в компьютерной системе.

Некоторые угрозы, вроде кражи, наводнения, или серьезного сбоя в питании, способны, конечно, физически повредить оборудование. Но существует гораздо больше угроз, которые, не вредя компьютерному «железу», приводят в негодность данные (документы, изображения). Они портят программы, замедляют работу системы, крадут что-то у пользователя, или, при вполне работоспособном компьютере, делают невозможной работу на нем.

Зная о том, что угрожает компьютеру, мы сможем приступить к построению эффективной системы безопасности. Начнем мы наш разговор с компьютерных вирусов. Вокруг них, даже в наш весьма просвещенный в компьютерном плане век, все еще ходит слишком много слухов и домыслов.

Вредоносное программное обеспечение

«Компьютерными вирусами» обычно называют все без исключения опасные программы. На самом же деле, собственно «компьютерные вирусы» — это лишь одна из разновидностей вредоносного программного обеспечения.

Иногда мне приходится беседовать с неподготовленными пользователями, компьютер для которых представляет собой еще более черный, чем для меня, ящик, а о вирусах они имеют и того меньшее представление. Когда начинаешь говорить о том, что «ваш компьютер заражен», у некоторых людей возникает недоумение. А некоторые панически боятся, наслушавшись где-то страшных рассказов о вирусах. Мне приходилось слышать

вопросы в духе: «А не опасно ли это для человека?», «А вы не шутите? Возможно ли это?». Об антивирусной защите не может идти никакой речи, если мнения о компьютерных вирусах часто не имеют ничего общего с реальностью.

Когда рассказываешь о том, что вирусы — это программы, написанные людьми, программы, умеющие распространяться, прятаться, и делать еще очень много всего, слушателей удивляет. И, причем, у многих большее удивление вызывает не сам факт существования вирусов, а то, что их кто-то пишет. «Зачем?», — спрашивают они. «Разве тем, кто пишет вирусы, больше нечем заняться?». На заре возникновения компьютерных вирусов они представляли исключительно научный интерес. Пожалуй, тогда можно было говорить о том, что люди пишут вирусы для развлечения и в исследовательских целях. Но уже очень скоро вирусы стали настоящим информационным оружием, с помощью которого можно уничтожать или красть данные. В наши дни вирусы создают обычно не для развлечения, а для незаконного достижения каких-то целей. Например — для того, чтобы, заразив некоторое количество компьютеров, подключенных к Интернету, получить над ними контроль и атаковать какие-либо Интернет-ресурсы.

Возможно, кого-то и в наши дни воспринимает написание вирусов как развлечение. Но это «развлечение» слишком дорого обходится тем, кто становится жертвой вирусов. Вирусы мешают работе, загружают ненужным трафиком соединение с Интернетом. Зараженные компьютеры начинают «тормозить». Усилиями вирусов тексты, заботливо набранные и отформатированные вами или вашими друзьями в MS Word, превращаются в бред сумасшедшего. Компьютеры иногда попросту перестают нормально загружаться. Подобное весьма неприятно даже «в масштабах» одного компьютера. А если речь идет о целой организации, которая не может работать из-за вирусной атаки? Последствия подобной атаки — это настоящая катастрофа.

Собственно говоря, не случайно в УК РФ имеется Статья 237, «Создание, использование и распространение вредоносных компьютерных программ». Пункт 1 этой статьи гласит следующее: *«Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничто-*

жения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации — наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев».

Итак, компьютерные вирусы — это программы, которые пишут люди. Деятельность эта незаконна, но в виду того, что авторов компьютерных вирусов непросто найти, новые вирусы появляются очень и очень часто.

Существуют различные признаки, по которым можно классифицировать вредоносное программное обеспечение (сокращенно — вредоносное ПО). Обычно выделяют три вида таких программ. Это компьютерные вирусы, сетевые черви и так называемые троянские программы.

Компьютерные вирусы

Классический **компьютерный вирус** (в английской терминологии Computer virus) ничего не портит, ничего не крадет и не уничтожает, он просто размножается. Кстати, сам факт размножения вируса может вызвать проблемы в инфицированной системе. Под системой здесь понимается, например, отдельный автономный компьютер, или компьютерная сеть. Вредоносные программы, которые распространяются, используя средства компьютерных сетей, принято называть сетевыми червями. Размножение вируса на компьютере занимает его системные ресурсы, заполняет ненужной информацией жесткий диск, замедляя, в результате работу компьютера. Однако вирусы обычно снабжаются некоторой «полезной» нагрузкой. Благодаря наличию механизма распространения, вирусы проникают в системы, после чего они используют дополнительные средства, которые позволяют им красть или портить данные.

Рассмотрим некоторые распространенные способы распространения компьютерных вирусов. Так, обычно вирусы либо заражают другие программы, либо, используя средства операционной системы, настраивают собственный автоматический

запуск при возникновении определенных событий. В первом случае при запуске инфицированной программы происходит запуск вируса (причем, после этого может быть запущена нужная программа, то есть внешне все выглядит вполне благополучно), который заражает другие файлы или выполняет еще какие-либо действия в системе. Во втором случае ничего запускать не нужно — вирус автоматически запускается, например, при загрузке операционной системы.

Так, например, сценарий работы вируса может выглядеть следующим образом. В инфицированной системе он «наблюдает» за подключаемым к компьютеру оборудованием. Если пользователь подключает флэш-диск, вирус, во-первых, записывает на диск свою копию, во-вторых, модифицирует файл **autorun.inf**, который находится на флэш-диске. Этот файл содержит команды, которые должны будут выполниться на компьютере, к которому подключается флэш-диск, он обеспечивает так называемый автозапуск программ. Например, если производитель флэш-диска разместил на нем какую-нибудь полезную программу, которая может запускаться при подключении диска к компьютеру, то команда запуска этой программы находится именно в данном файле. Если диск инфицирован, то после того, как он будет подключен к неинфицированному компьютеру, с него автоматически будет запущен вирус, который заразит систему.

Вирусы могут заражать не только программы, не только настраивать систему на собственный автозапуск. Они умеют заражать и внешне вполне безобидные файлы. Речь идет о так называемых макровирусах.

Макровирусы написаны с использованием одного из языков макропрограммирования. Макросы, макроопределения, макрокоманды — под этим названиями скрываются программы, которые могут выполняться в какой-либо среде, например, в текстовом, графическом, табличном редакторе и служат для автоматизации действий пользователя. Макросы хранятся во внешних файлах программных продуктов (Microsoft Word, Excel, Access, CorelDRAW и т.д.) и выполняются при помощи внутренних интерпретаторов. Таким образом, обычный, вовсе неопасный по мнению многих пользователей, Word'овский документ, может содержать опасный вирус. Не случайно в новых версиях Microsoft Office пред-