

УДК 004.42(075)
ББК 32.973.26
В 48

В оформлении книги использованы иллюстрации по лицензии от Shutterstock.com:
Feng Yu, Vladru

Виннер М.
В 48 Бесплатные антивирусы и защита компьютера для любимых родителей / Марина Виннер. – М. : Эксмо, 2014. – 208 с. + DVD. – (Компьютер на 100%).

ISBN 978-5-699-69947-6

В современном мире, где компьютер есть практически у каждого, несоблюдение компьютерной безопасности может плачевно закончиться для любого пользователя. В лучшем случае закончится потерей информации, в худшем – вы можете лишиться своих сбережений, когда злоумышленники получат доступ к вашему банковскому счету. Любой человек, независимо от возраста, может овладеть знаниями по компьютерной безопасности, которые надежно оградят вас от угроз из Интернета. Вы найдете информацию обо всех опасностях, которые подстерегают вас в Интернете, и научитесь самостоятельно справляться с возникающими проблемами.

К книге прилагается диск с бесплатными приложениями, которые сделают ваш компьютер по-настоящему надежной крепостью!

УДК 004.42(075)
ББК 32.973.26

Производственно-практическое издание

КОМПЬЮТЕР НА 100%

Виннер Марина

**БЕСПЛАТНЫЕ АНТИВИРУСЫ И ЗАЩИТА КОМПЬЮТЕРА
ДЛЯ ЛЮБИМЫХ РОДИТЕЛЕЙ**
(орыс тілінде)

Директор редакции *Е. Капьев*. Ответственный редактор *В. Обручев*
Художественный редактор *Г. Федотов*

ООО «Издательство «Эксмо»

123308, Москва, ул. Зорге, д. 1. Тел. 8 (495) 411-68-86, 8 (495) 956-39-21.

Home page: www.eksmo.ru E-mail: info@eksmo.ru

Өндіруші: «ЭКСМО» АҚБ Баспасы, 123308, Мәскеу, Ресей, Зорге көшесі, 1 үй.

Тел. 8 (495) 411-68-86, 8 (495) 956-39-21

Home page: www.eksmo.ru E-mail: info@eksmo.ru.

Tayar belrici: «Эксмо»

Қазақстан Республикасында дистрибьютор және өнім бойынша

арыз-талаптарды қабылдаушының

өкілі «РДЦ-Алматы» ЖШС, Алматы қ., Домбровский көш., 3-а», литер Б, офис 1.

Тел.: 8 (727) 2 51 59 89, 90, 91, 92, факс: 8 (727) 251 58 12 вн. 107; E-mail: RDC-Almaty@eksmo.kz

Өнімнің жарамдылық мерзімі шектелмеген.

Сертификация туралы ақпарат сайтта: www.eksmo.ru/certification

Сведения о подтверждении соответствия издания согласно законодательству РФ о техническом регулировании можно получить по адресу: <http://eksmo.ru/certification/>

Өндірген мемлекет: Ресей. Сертификация қарастырылмаған

Подписано в печать 23.12.2013. Формат 70х100¹/₁₆.

Печать офсетная. Усл. печ. л. 16,85.

Тираж 2000 экз. Заказ



ISBN 978-5-699-69947-6



© Виннер М., 2014

© ООО «Айдиономикс», 2014

© Оформление. ООО «Издательство «Эксмо», 2014

Краткое оглавление

Введение	7
Глава 1. Вирусы и способы борьбы с ними	8
Глава 2. Антивирусы.....	21
Глава 3. Сканеры.....	112
Глава 4. Антишпионы	147
Глава 5. Сетевая защита: брандмауэры.....	178
Глава 6. Защита от спама.....	197
Алфавитный указатель	208

Оглавление

Введение	7
Глава 1. Вирусы и способы борьбы с ними	8
Что такое вирус.....	8
Классификация вирусов.....	8
Способы заражения компьютера.....	10
Как определить заражение.....	11
Нежелательные программы.....	12
Фишинг.....	13
Нигерийские письма	14
Как бороться	16
Скачивание программы.....	19
Глава 2. Антивирусы.....	21
avast!.....	21
Установка	21
Регистрация.....	26
Знакомство с программой	29
Проверка компьютера.....	34
Обновление.....	39
Avira Free Antivirus.....	40
Установка	40
Знакомство с программой	44
Настройки	48
Проверка компьютера.....	50
AVG AntiVirus FREE.....	51
Установка	51
Знакомство с программой	55
Настройки	57
Проверка компьютера.....	62
Panda Cloud Antivirus.....	64
Установка	64
Знакомство с программой	67
Проверка компьютера.....	68
Настройки	70
COMODO Antivirus.....	78
Установка	78
Знакомство с программой	83
Настройки	91
Проверка компьютера.....	95

Zillya! Антивирус.....	99
Установка.....	99
Знакомство с программой.....	102
Проверка компьютера.....	111
Глава 3. Сканеры.....	112
Dr.Web CureIt!.....	112
Знакомство с программой.....	112
Настройки.....	115
Kaspersky Virus Removal Tool.....	118
Установка.....	118
Знакомство с программой.....	119
Обновление.....	119
Проверка компьютера.....	121
Настройки.....	123
Panda ActiveScan 2.0.....	126
Знакомство с программой.....	126
Проверка компьютера.....	128
Trend Micro HouseCall.....	133
Установка.....	133
Знакомство с программой.....	138
Проверка компьютера.....	139
Microsoft Safety Scanner.....	142
Установка.....	142
Проверка компьютера.....	143
Глава 4. Антишпионы.....	147
Spyware Terminator.....	147
Установка.....	147
Знакомство с программой.....	149
Проверка компьютера.....	152
Spybot - Search & Destroy.....	153
Установка.....	154
Знакомство с программой.....	159
Проверка компьютера.....	161
AVZ.....	162
Запуск.....	162
Знакомство с программой.....	163
Проверка компьютера.....	165
SUPERAntiSpyware.....	166
Установка.....	166
Знакомство с программой.....	167
Проверка компьютера.....	168

Оглавление

Malwarebytes Anti-Malware	171
Установка	171
Знакомство с программой	173
Проверка компьютера	176
Глава 5. Сетевая защита: брандмауэры	178
COMODO Firewall	178
Установка, знакомство с программой	178
Защита компьютера	178
Windows Firewall Control	180
Установка	180
Знакомство с программой	183
Защита компьютера	185
SterJo NetStalker	186
Установка	186
Знакомство с программой	188
Защита компьютера	188
ZoneAlarm Free Firewall	190
Установка	190
Знакомство с программой	192
Защита компьютера	194
Глава 6. Защита от спама	197
AGAVA SpamProtexx	197
Установка	197
Знакомство с программой	200
Mozilla Thunderbird	202
Установка	203
Знакомство с программой	205
Алфавитный указатель	208

ВВЕДЕНИЕ

Компьютерные технологии в жизни современного человека играют все большую роль. Если раньше умение обращаться с компьютером было прерогативой молодежи, то сейчас каждый человек, независимо от возраста, должен быть уверенным пользователем ПК. При этом важное значение имеет Интернет. Поговорить с близким человеком, который живет в другом городе, найти нужную информацию, посмотреть фильм — со всем этим вам поможет Всемирная сеть. Однако в Интернете вас подстерегает множество опасностей — вирусы, классифицировать и бороться с которыми должен уметь каждый пользователь. Ситуация в компьютерном мире напоминает гонку вооружений: постоянно появляется новое вредоносное программное обеспечение, и в то же время совершенствуются средства защиты от него. В такой ситуации бывает сложно сориентироваться и сделать правильный выбор.

Эта книга поможет вам разобраться в классификации угроз, узнать, какие программы разработаны для защиты от них, как их использовать и, конечно, как из огромного многообразия антивирусных приложений подобрать подходящее именно вам. Все программы, о которых рассказано в издании, распространяются бесплатно. Кроме того, мы прилагаем к книге компакт-диск с рассмотренным антивирусным программным обеспечением.

Глава 1

ВИРУСЫ И СПОСОБЫ БОРЬБЫ С НИМИ

Что такое вирус

Компьютерный вирус — небольшая программа, совершающая на компьютере вредоносные действия и способная к саморазмножению. Ваш компьютер зависает, медленно работает, вы не можете запустить программу — это признаки заражения.

Вред от вирусов не всегда явный. Никак не влияя на работу компьютера, программа может следить за действиями пользователя и передавать информацию посторонним лицам. Существуют также вирусы, основная задача которых — нанести вред пользователю. Попадая на компьютер, такой вирус зашифровывает данные, например личные фотографии, в результате чего вы не сможете их просмотреть. После этого приходит сообщение, что для расшифровки необходимо перечислить определенную сумму на конкретный счет. Излишне говорить, что, даже переслав злоумышленникам деньги, никакого ключа для расшифровки вы не получите.

ИНТЕРЕСНО ЗНАТЬ

Первая эпидемия компьютерных вирусов разразилась в 1987 г., когда вирус Brain заразил более 18 тыс. компьютеров.

Классификация вирусов

В зависимости от признака, положенного в основу, выделяют несколько классификаций вирусов.

По среде обитания:

- **сетевые** — вирусы, которые проникают на удаленный компьютер, используя электронную почту и компьютерные сети;
- **файловые** — вирусы, внедряющиеся в исполняемые файлы (обычно такие файлы имеют расширение `.com` и `.exe`);
- **загрузочные** — как следует из названия, это вирусы, которые записывают себя в загрузочный сектор жесткого диска и таким образом запускаются каждый раз, когда вы включаете компьютер;
- **файлово-загрузочные** — вирусы, которые заражают как файлы, так и загрузочный сектор, и, соответственно, являются наиболее опасными.

ПРИМЕЧАНИЕ

Расширение — это последовательность символов, отделенная от имени файла точкой. Расширения нужны, чтобы пользователь и система могли определить тип файла и в зависимости от типа возможные действия с ним. Например, глядя на файл `фильм.avi`, понятно, что это видеофайл, а `картинка.jpg` — изображение. Те файлы, которые запускают программы, обычно имеют расширение `.exe` (от англ. *executable* — исполнение) и наиболее часто подвержены заражению вирусами.

По способу заражения:

- **резидентные** — вирусы, которые постоянно находятся в памяти включенного компьютера;
- **нерезидентные** — вирусы, начинающие действовать только во время запуска зараженной программы.

По особенностям алгоритма работы:

- **паразитические** — вирусы, встраиваемые в файл, но при этом никак не влияющие на его работу;
- **репликаторы (черви)** — вирусы, которые размещают свои копии во всех возможных местах хранения данных, часто используются как средство распространения других вирусов;

- **трояны** — вирусы, маскирующиеся под существующие на компьютере программы (названы по аналогии с троянским коном);
- **невидимки** — вирусы, которые виртуозно скрываются в системе, ускользают от антивирусной программы и даже препятствуют работе антивируса;
- **мутанты** (полиморфные вирусы) — вирусы, каждая новая копия которых не похожа на своего прародителя, что, в свою очередь, сильно затрудняет их поиски на компьютере;
- **макровирусы** (документные) — вирусы, которые заражают такие популярные программы, как Microsoft Word, Microsoft Excel, а также другие продукты Microsoft Office, используя макросы (специальные приложения, встроенные в это программное обеспечение).

По степени воздействия:

- **неопасные** — вирусы, которые не наносят вреда компьютеру и вашим данным;
- **опасные** — вирусы, вызывающие сбои в работе компьютера, тормозящие выполнение операций;
- **очень опасные** — вирусы, в результате работы которых вы рискуете лишиться важной информации, хранящейся на компьютере. Личные данные могут быть переданы посторонним лицам.

Способы заражения компьютера

Многие пользователи не придают особого значения вирусам, пока не узнают, что компьютер заражен. Тогда и возникает вопрос: каким образом это могло случиться?

Одна из основных причин — беспечность пользователя во время работы за компьютером:

- отсутствие антивирусного программного обеспечения на компьютере;
- неосторожное использование чужих флеш-накопителей;

- установка неизвестных программ из Интернета;
- переход по ссылкам из спам-писем, открытие вложенных в письмо файлов.

ПРИМЕЧАНИЕ

Спам — нежелательная рассылка электронных писем рекламного характера; часто в такой корреспонденции содержатся ссылки на вредоносные сайты, а также сами вирусы в виде прикрепленных файлов.

Кроме того, если компьютер подключен к домашней сети, то вирус может прийти от одного из ее участников.

Как определить заражение

Вирусы подразделяются на безвредные и опасные. В первом случае их довольно трудно опознать без помощи антивируса. Обнаружить вредоносные вирусы можно по нескольким признакам, которые должны вас насторожить.

- Системный блок компьютера издает произвольные звуки (пищит), никак не связанные с вашей деятельностью.
- Периодически на экране появляются посторонние изображения или сообщения.
- На компьютере произвольно запускаются программы.
- Браузер сам открывает сайты и меняет настройки.

ПРИМЕЧАНИЕ

Браузер — это специальная программа для просмотра сайтов в Интернете. По умолчанию в операционной системе Windows установлен Internet Explorer, но многие предпочитают пользоваться обозревателями от сторонних разработчиков, например Mozilla Firefox, Opera и др.

- Компьютер стал работать медленнее: долго загружается операционная система и запускаются приложения.
- Ваш почтовый ящик сам отправляет сообщения.

- Увеличился расход интернет-трафика.
- Появляются новые файлы или, наоборот, исчезают старые.

Если вы столкнулись с подобным поведением, всерьез задумайтесь над мерами противодействия вирусным угрозам.

Нежелательные программы

Кроме собственно вредоносных приложений, которые явно тормозят работу вашего компьютера, существуют так называемые **нежелательные программы**. Сами по себе они не могут причинить вред. Для выполнения действий, заложенных в них разработчиком, необходимо разрешение пользователя. Другими словами, если такая программа захочет, например, перенаправить вас на какой-либо сайт, то сначала попросит у вас подтверждение.



Защищайте компьютер от нежелательного программного обеспечения

Нежелательные программы можно разделить на три группы.

- **Рекламные (Adware).** Отвечают за добавление рекламных баннеров в другие приложения, именно они открывают рекламные интернет-страницы. Некоторые рекламные программы собирают своеобразные досье на пользователя (названия посещаемых сайтов, статистику поисковых запросов в Интернете и пр.) и отправляют в маркетинговые отделы компаний-разработчиков. Но, опять же, для отправки подобной информации понадобится ваше согласие.

- **Порнографические (Pornware).** В принципе, это та же реклама сторонних сайтов, только порнографической направленности. Такие программы могут дозваниваться в порнографические телефонные службы, скачивать нежелательные файлы, встраивать в браузер специальные инструменты для поиска так называемых материалов для взрослых.
- **Прочие (Riskware).** Это вполне безвредные и даже полезные программы, которые в большинстве случаев пользователь устанавливает сам. Но они имеют функции, доступ к которым посторонних людей способен причинить вред вашему компьютеру. Это приложения для общения в Интернете, восстановления паролей, программы-загрузчики и т. д. Работая с подобными приложениями, вы сами определяете их пользу и возможные риски.

Фишинг

Один из видов интернет-мошенничества — **фишинг** (от англ. *fishing* — рыбная ловля). Цель мошенников — получение информации о пользователях, такой как пароли, данные кредитных карт, банковских счетов и др.

Суть фишинга заключается в следующем. На почту приходит письмо от «провайдера» (банка или какой-либо другой организации), в котором вас просят передать личные данные под предлогом сбоя в системе, утери информации и т. д. Зачастую в письме содержится ссылка, которая приведет вас на поддельный сайт, как две капли воды похожий на официальную страницу банка (провайдера, аукциона и т. д.). Заполнив на таком сайте поля **Логин** и **Пароль**, вы передадите их злоумышленникам. Представьте, что вы заполнили поля данных своей кредитной карты. Искушенный пользователь, конечно, обратит внимание на адрес сайта и, если он будет отличаться от настоящего, никакие данные там оставлять не будет. Мошенники тоже учитывают этот момент, поэтому адреса сайтов незначительно отличаются от официальных: лишнее слово, лишние символы, подмена символов — и на первый взгляд адрес выглядит правильно.

В последнее время мошенники используют особенности человеческой психологии: потенциальную жертву выводят из равновесия

всевозможными угрозами. Так, на почту может прийти поддельное письмо из банка с требованием передать личные данные, в противном случае счет будет заблокирован. Как особая насмешка выглядит способ фишинга, при котором от жертвы просят сообщить конфиденциальные сведения для защиты от фишинга.

Существуют признаки, по которым можно определить, что перед вами фишинговое сообщение.

- Вам угрожают закрытием счета в банке, удалением страницы в социальной сети или какими-либо другими репрессивными мерами, если вы не перешлете свои конфиденциальные сведения. Серьезные компании никогда не просят сообщать личные данные в письмах.
- Вам предлагают забрать денежный приз, правда, нужно поделиться личными данными.
- Письмо от «серьезной организации» содержит орфографические и пунктуационные ошибки. Согласитесь, это довольно странно.

Нигерийские письма

Этот вид мошенничества, использующий электронную почту, получил такое название, поскольку зародился и распространился первоначально в Нигерии. Сегодня письма приходят из различных африканских стран. Это бедные государства с нестабильной политической обстановкой.

Суть мошенничества заключается в том, что на электронный адрес приходит письмо, в котором вас просят помочь в переводе огромной суммы денег (миллионы долларов) из неблагополучной страны. Просит об этом бывший глава страны, чиновник, бизнесмен, олигарх и т. д. Помощь нужна, поскольку в данной стране якобы трудности с выводом денег из-за высоких налогов, преследований со стороны властей и т. д. Главное, что без вашей помощи никак не справиться и за это авторы письма готовы неплохо заплатить. Если жертва заинтересовалась и вступила с мошенниками в переписку, то ее начинают убеждать в реальности предложения: высылают документы, может даже позвонить «адвокат», сам «биз-

несмен». Далее начинается то, ради чего все затевалось, — чтобы «перевести» деньги из африканской страны, жертве мошенничества нужно сделать несколько вложений: пошлины, взятки, сопутствующие расходы. Мошенники будут тянуть деньги из жертвы, пока та не прозреет. Увы, после этого «миллионер» бесследно исчезает, а жертва остается без денег.



Нигерийские письма могут быть самыми разнообразными по содержанию

Характерная особенность нигерийских писем — их полная безграмотность. Дело в том, что для мошенников русский язык не родной, поэтому они пользуются компьютерными переводчиками, которые часто допускают ошибки.

Схем мошенничества с помощью нигерийских писем множество.

- Спасение дочери богатого человека из лагеря беженцев, что опять же потребует финансовых вложений.
- Неожиданное наследство от погибшего родственника. «Адвокат» погибшего очень хочет отправить вам деньги, но без информации о банковском счете это, увы, невозможно.
- Неожиданная победа в лотерее, в которой вы не участвовали. Заплатите налог на выигрыш — и сразу получите огромную сумму.
- Для небезразличных людей своя схема — разнообразные пожертвования в африканских странах. Выгоды здесь, конечно, не обещают, но ведь совестливым людям она и не нужна.

- Продавая вещи в Интернете, будьте внимательны. Вам «по ошибке» могут прислать чек с большей суммой, чем сумма покупки. Пообещают, конечно же, вернуть разницу при получении товара, только вот чек окажется поддельным.
- Разместили объявление на сайте знакомств? Вами может заинтересоваться знойная, красивая и богатая африканская девушка. Правда, и у нее есть определенные проблемы, поэтому от вас потребуются деньги.

Каждый день придумываются новые схемы, поэтому будьте бдительны и всегда помните: никто не будет делиться с вами своими миллионами.

Как бороться

Набор средств для защиты компьютера от вредоносных и нежелательных приложений довольно широк. В зависимости от выполняемых функций различают несколько типов защитных программ.

- **Антивирус** — для постоянной защиты компьютера от вирусов.
- **Сканер** — для поиска вирусов и нежелательных приложений. В отличие от антивируса она не обеспечивает постоянной защиты.
- **Брандмауэр** (от нем. *Brandmauer* — противопожарная стена) — для защиты сетевых подключений и контроля трафика.
- **Антишпионское ПО** — для борьбы с нежелательными программами.
- **Для защиты от спама.**

В зависимости от условий работы защитные программы также различаются.

- **Бесплатные**, как следует из названия, распространяются свободно.
- **Платные** позиционируются как очень качественный продукт, за использование которого необходимо внести деньги. Платные приложения по сравнению с бесплатными средствами защиты, имеют больше компонентов. Вместе с тем, соблюдая