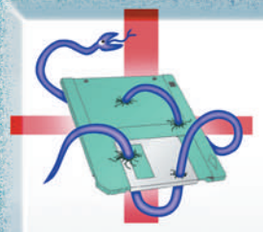


Защита компьютерной информации становится насущной проблемой, поскольку все больше людей полагается на компьютер для решения важных задач. Особенно обострились вопросы компьютерной безопасности в связи со взрывообразным ростом популярности World Wide Web. Всем пользователям ПК необходима информация о борьбе с компьютерными вирусами и знание правил безопасности при работе в локальных сетях и в Internet.

Второе, стереотипное издание книги Игоря Гульева (первое издание: «Компьютерные вирусы. Взгляд изнутри». М.: «ДМК Пресс») приводит конкретные примеры защиты информации от вирусов. Читатель получит подробные сведения о структуре и свойствах вирусов, о методах борьбы с ними, а также о правилах безопасности при работе с BBS и электронной почтой.

Издание предназначено для пользователей ПК и Internet, системных администраторов, разработчиков систем компьютерной безопасности.

- даны примеры вирусов на ассемблере
- рассмотрены способы выявления и лечения макровирусов
- приведена подробная классификация вирусов

ISBN 5-89818-087-7

ГУЛЬЕВ И.А.

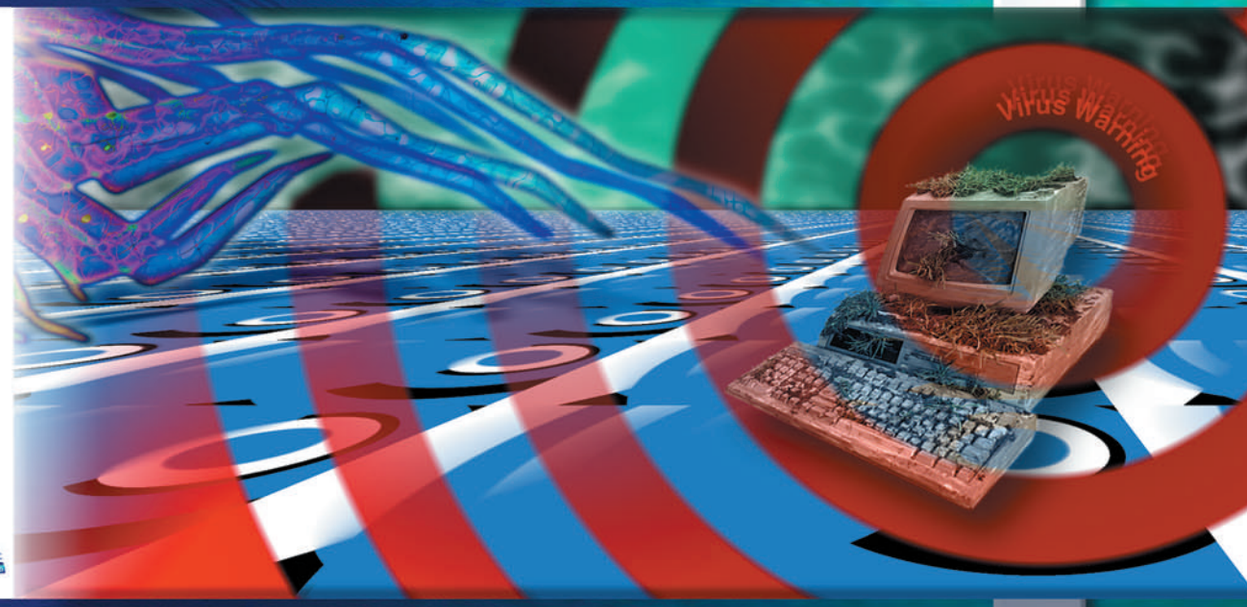
ДМК

Создаем вирус и антивирус

ГУЛЬЕВ И.А.

Создаем ВИРУС и антивирус

- **Осторожно, вирус!**
  Классифицируем компьютерные вирусы
- **Хотите знать, как он работает?**
  Изучаем исходные тексты вирусов
- **Как уберечь компьютер от инфекции**
  Исследуем алгоритм заражения
- **BBS в опасности**
  Осаждаем виртуальную крепость
- **Пароль не нужен**
  Гуляем по сети инкогнито



Игорь Гульев

Создаем вирус и антивирус

2-е издание, стереотипное

Москва

Электронный архив библиотеки авиационного факультета МГУ

Гульев Игорь

Г94 Создаем вирус и антивирус / Гульев Игорь — 2-е изд., стереотипное. – М.: ДМК. — 304 с.: ил.

ISBN 5-89818-087-7

Virus Warning!

С этим сообщением, хоть раз в жизни, сталкивался любой пользователь компьютера. Вирмейкеры с упорством маньяков плодят все новые и новые разновидности вирусов. Бытует мнение, что избавиться от них можно лишь с помощью сложных и дорогостоящих новейших антивирусных программ. Это не совсем верно – знание принципов действия и способов внедрения вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной «вакцины».

В этой книге вы найдете обширный материал, посвященный проблеме защиты информации, рассмотренной с обеих сторон баррикад (как от лица вирмейкера, так и создателя антивирусов).

ISBN 5-89818-087-7

СОДЕРЖАНИЕ

ŋqdqүəʏ bƎ dəqƎbʏзə d ɕɑɑbɔʏ Ɉqddүqүè

ВВЕДЕНИЕ

Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом – сейчас этим уже никого не удивишь. Достаточно вспомнить появление «первой ласточки», наделавшей много шума – вируса WinWord.Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0.

Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (Win95.CIH), который способен испортить «железо» компьютера. Другие же могут лишь уничтожить информацию, не более того.

В литературе весьма настойчиво пропагандируется, что избавиться от вирусов можно лишь при помощи сложных (и дорогостоящих) антивирусных программ, и якобы только под их защитой вы можете чувствовать себя в полной безопасности. Это не совсем так – знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной программы.

Глава 1

COM-ВИРУСЫ

В этой главе рассказано об алгоритмах работы вирусов, заражающих COM-файлы, и способах их внедрения. Представлен исходный текст одного из таких вирусов с подробными комментариями. Также приведены основные сведения о структуре и принципах работы COM-программы.