



CNews.ru

НОВОСТИ

АНАЛИТИКА

ТЕХНИКА

ВИДЕО

WIFI

ЖУР



Поиск

- ❖ КАЛЕНДАРЬ СОБЫТИЙ
- ❖ УЧЕБНЫЕ КУРСЫ
- ❖ КАТАЛОГ КОМПАНИЙ
- ❖ ПОДПИСКА

ВНИМАНИЕ

**ПРАКТИЧЕСКИЕ РЕШЕНИЯ ОТ INTEL. ЭФФЕКТИВНЫЙ IT-МЕНЕДЖМЕНТ.**

- ❖ ТЕЛЕКОММУНИКАЦИИ
  - ❖ ИНТЕРНЕТ
  - ❖ НАУКА И ТЕХНОЛОГИИ
  - ❖ БЕЗОПАСНОСТЬ
- от Лаборатории Касперского



АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

**При подписке на Аналитические бюллетени Gartner на русском языке — бесплатная годовая подписка на журнал CNews!**

- Распределительные, силовые, телекоммуникационные и серверные шкафы**  
Цена: 29 000 руб. [Купить](#)
- Российский рынок мобильного контента**  
Цена: 42 000 руб. [Купить](#)
- Телекоммуникационная карта России**  
Цена: 87 000 руб. [Купить](#)


**НОВОСТНАЯ ЛЕНТА**
**Тема:** Безопасность

05.12.05, Пн, 18:26, Мск

## "Иммунизация" интернета: новый способ борьбы с вирусами

Обычное антивирусное ПО использует для поиска и обезвреживания вирусов их сигнатуры. Это означает, что как правило, вирусы должны быть исследованы специалистами до того как антивирусное ПО научится их различать, что снижает скорость "ответной реакции", и может привести к тому, что некоторые быстрораспространяющиеся вирусы нанесут немалый ущерб, до того как будут обезврежены. Решением проблемы могут стать, так называемые "иммунные системы". Новый вид таких систем разработала команда из Тель-Авивского университета под руководством Эрана Шира (Eran Shir). Они применили теорию сетей к решению проблемы, и, как утверждают, нашли более эффективные способы борьбы с вирусными атаками.

Исследователи считают, что атаки вирусов всегда будут опережать ответные действия, исходящие от серверов, контролирующих сеть. Поэтому предлагают развить распределенную в интернете сеть компьютеров-"ловушек" (honeypots). Эти компьютеры будут "заманивать" вирусы, автоматически их анализировать и распространять контрмеры. "Ловушки" должны быть связаны между собой отдельными защищенными каналами. В этом случае, при обнаружении атаки на одной из "ловушек" остальные будут моментально оповещены, и начнут работать как центры распространения обезвреживающего кода. Моделирование показало что, чем больше сеть, тем более эффективно работает эта схема. Например, если в сети будет 50 тыс. узлов (компьютеров), и только 0,4 % из них "ловушки", вирусы успеют захватить не более 5% сети, а затем будут остановлены "иммунной системой". Для сети с 200 млн. узлов, при той же пропорции "ловушек" заражение составит всего 0,001 %.

Пока подобная "иммунная система" существует лишь в теории, но Шир надеется с помощью добровольцев запустить подобный проект в интернете.


**Мнение IT специалистов: как относятся к AMD в России?**
