Зияутдинов В.С., Корнев П.А., Малыш В.Н. Основные средства для борьбы с программными вирусами. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей IX Междунар. научно-техн. конф. – Пенза: ПДЗ, 2009. – С. 144-145.

ОСНОВНЫЕ СРЕДСТВА ДЛЯ БОРЬБЫ С ПРОГРАММНЫМИ ВИРУСАМИ

В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш

Липецкий государственный педагогический университет,
г. Липецк, Россия

Рассмотрены основные варианты классификации известных программных вирусов и средств борьбы с ними. Также приведен анализ текущих данных о тестировании известных комплексных антивирусных программных продуктов.

Ziyautdinov V.S., Kornev P.A., Malysh V.N. Main facilities for struggling against program viruses.

The article covers the key variants of viruses' classification and facilities for struggling against them. Also there is an analysis of current data on testing some well-known antivirus programs.

Программный вирус (ПВ) – это автономно функционирующая программа, которая обладает способностью к размножению и распространению в локальных и глобальных вычислительных сетях, и отдельных ЭВМ [1]. Так как программные вирусы являются весьма эффективным средством для практической реализации современных угроз информационной безопасности ЛВС, то вопросы исследования средств противодействия вирусам приобрели существенную актуальность.

Как правило, цикл жизни любого вируса состоит из следующих последовательно сменяющих друг друга этапов [1]:

1. Этап внедрения.
2. Инкубационный этап.
3. Этап репликации.
4. Этап проявления.

Физическое «строение» вируса весьма тривиально. Программный вирус состоит из так называемой «головы» и «хвоста». Как следует из названия, «голова» – это структурный элемент вируса, получающий управление в первую очередь. «Хвост» представляет собой возможное дополнение «головной» части, которое располагается в теле вредоносной программы отдельно. По наличию «хвоста» принято разделять вирусы на сегментированные (с «хвостом») и несегментированные (без «хвоста»).

Другим критерием для классификации является характер размещения вируса в памяти ПЭВМ. Согласно данному критерию принято выделять следующие виды вирусов [1]: файловые резидентные, файловые нерезидентные, пакетные, загрузочные, гибридные.

Для борьбы с программными вирусами используют различные антивирусные программы. По специфике выявления и нейтрализации вредоносных программ принято выделять следующие категории антивирусов: 1) детекторы; 2) вакцины; 3) прививки; 4) фаги; 5) ревизоры; 6) мониторы.

На практике широкое применение получили комплексные антивирусные решения. Следует выделить основные антивирусные программные продукты известных фирм-разработчиков:

1. Антивирус Касперского Personal Pro.
2. Doctor Web для ОС семейства Windows.
3. Norton Antivirus Professional Edition.
4. Panda Antivirus.
5. Avira AntiVir Premium.
6. Eset NOD 32 Antivirus.
7. BitDefender Antivirus.
8. Avast! Professional Edition.

Ежегодно различными сторонними фирмами производятся процедуры независимого тестирования антивирусного программного обеспечения на основе следующих критериев:

- скорость реакции на новые угрозы;
- степень надежности самозащиты;
- время реакции на угрозы;
- качество лечения активного заражения;
- степень эффективности проактивной защиты и т.д.

Необходимо кратко ознакомиться с результатами последнего тестирования антивирусов на степень эффективности проактивной защиты, проведенного на базе портала Anti-Malware.ru (таблица) [2].

Результаты теста проактивной антивирусной защиты

Антивирус	Процент обнаруженных вирусов, %	Процент ложных срабатываний, %
Avira	71	0,13
Kaspersky	60,6	0,01
DrWeb	61	0,20
BitDefender Antivirus	60,1	0,04
Eset	60,5	0,02
Norton	51,5	0
Avast	53,3	0,03
Panda Security	37,9	0,02

Очевидно, что по результатам тестирования первое место по эффективности проактивной защиты было присуждено таким антивирусам, как Kaspersky Anti-Virus, Eset Nod32 Anti-Virus и BitDefender Antivirus.

Библиографический список

1. Буйневич М.В., Доценко С.М., Малыш В.Н. Информационная безопасность и защита информации в компьютерных системах. – Липецк : ЛГПУ, 2007. – 255 с.
2. Основные результаты теста проактивной антивирусной защиты. – http://anti-malware.ru/proactive_test_2009.