

УДК 004.491
ББК 32.973-018.2
Р17

Разрушающие программные воздействия: *Учебно-методическое пособие* / А.Б. Вавренюк, Н.П. Васильев, Е.В. Вельмякина, Д.В. Гуров, М.А. Иванов, И.В. Матвейчиков, Н.А. Мацук, Д.М. Михайлов, Л.И. Шустова; под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. — 328 с.

В пособии рассматриваются тенденции развития разрушающих программных воздействий. Показывается, что появление новых компьютерных технологий, новых математических методов дают в руки нарушителей и создателей вредоносных программ все новые и новые возможности. Анализируются механизмы проведения атак на программные системы, основанные на использовании стохастических методов. Рассматриваются превентивные методы защиты от разрушающих программных воздействий.

Рекомендуется использовать при изучении дисциплин «Программирование на языке высокого уровня», «Методы и средства защиты компьютерной информации», «Безопасность информационных систем» для студентов, обучающихся по специальности «Вычислительные машины, комплексы, системы и сети». Может быть полезно разработчикам и пользователям компьютерных систем.

Подготовлено в рамках Программы создания и развития НИЯУ МИФИ.

Рецензент В.Г. Иваненко (НИЯУ МИФИ)

ISBN 978-5-7262-1503-7

© Национальный исследовательский
ядерный университет «МИФИ», 2011

СОДЕРЖАНИЕ

Введение	8
1. СТОХАСТИЧЕСКАЯ КОМПЬЮТЕРНАЯ ВИРУСОЛОГИЯ	12
1.1. Разрушающие программные воздействия (РПВ)	12
1.2. Структура комплекса программных средств антивирусной защиты	13
1.3. Критерии эффективности программных средств антивирусной защиты	16
1.4. Недостатки существующих средств защиты от РПВ	19
1.5. Перспективные методы защиты от РПВ	22
1.6. Стохастическая компьютерная вирусология: использование стохастических методов в атаках на компьютерные системы	23
1.6.1. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для затруднения своего обнаружения	24
1.6.2. Анализ механизмов функционирования компьютерных вирусов, использующих стохастические методы для выполнения деструктивных функций	29
1.7. Стохастические вычислительные машины	33
Выводы	36
Контрольные вопросы	37
2. КЛЕПТОГРАФИЧЕСКИЕ АТАКИ НА КРИПТОСИСТЕМЫ	38
2.1. Свойства клептографических скрытых каналов	39

2.2. Механизмы внедрения троянских компонент в реализацию алгоритма RSA	41
2.3. Необнаруживаемое восстановление секретного ключа для алгоритма цифровой электронной подписи ECDSA	58
2.4. Внедрение троянской компоненты в алгоритм Эль-Гамала	63
2.5. Клептографическая атака на алгоритм выработки общего секретного ключа Диффи-Хеллмана	66
2.6. Защита от клептографических атак	68
Выводы	69
Контрольные вопросы	70
 3. ТЕНДЕНЦИИ РАЗВИТИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	 71
3.1. Стохастические разрушающие программные воздействия (РПВ)	72
3.1.1. Простой криптоотроян	73
3.1.2. Улучшенный криптоотроян	74
3.1.3. Анонимная кража информации	75
3.1.4. Криптосчетчик	76
3.1.5. Конфиденциальное получение информации ...	78
3.1.6. Недоказуемое шифрование	82
3.1.7. Отрицаемое шифрование	85
3.1.8. Загрузчик РПВ	85
3.2. Симбиотические и распределенные вредоносные программы	87
3.2.1. Элементы теории игр	88
3.2.2. Информационный шантаж	89
3.2.3. Распределенные вычисления	95
3.2.4. Безопасный выкуп	101
Выводы	105
Контрольные вопросы	106

4. ПЕРСПЕКТИВНЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ВРЕДНОСНЫМ ПРОГРАММАМ	108
4.1. Иммунологический подход к антивирусной защите..	108
4.1.1. Понятие иммунной системы	108
4.1.2. Первый практический опыт	111
4.1.3. Пути дальнейшего развития	112
4.1.4. Архитектура компьютерной иммунной системы	114
4.1.5. Автономность надежной системы защиты	117
4.1.6. Стохастический подход к защите информации	121
4.2. Поведенческий анализ программ	124
4.2.1. Поведение по определению	124
4.2.2. Определение по поведению	125
4.2.3. Иммунологический подход	127
4.2.4. Распределенное обнаружение изменений	129
4.2.5. Современные тенденции в динамическом анализе кода	130
Выводы	133
Контрольные вопросы	134
5. СКРЫТЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ	135
5.1. История исследования скрытых каналов	137
5.2. Характеристики скрытых каналов	144
5.3. Современный взгляд на скрытые каналы	149
5.4. Потайные и побочные каналы	155
5.5. Скрытые каналы в системах обработки информации	157
5.6. Методы организации локальных скрытых каналов ..	161
5.7. Методы организации сетевых скрытых каналов	169
5.7.1. Скрытые каналы на основе протоколов TCP/IP	173
5.7.2. Скрытые каналы в протоколах уровня	

приложений	187
Выводы	190
Контрольные вопросы	191
6. УГРОЗА ПРОВЕДЕНИЯ АТАК НА UNIX-СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ СКРИПТ-ВИРУСОВ ДЛЯ КОМАНДНЫХ ИНТЕРПРЕТАТОРОВ	193
6.1. Интерпретатор и компилятор. Преимущества вирусов на интерпретируемых языках. Скрипт-вирусы на языке Shell	194
6.2. Классификация технических приемов, используемых скрипт-вирусами	196
6.3. Классификация скрипт-вирусов	199
6.4. Поиск скрипт-вирусов на основе анализа кода. Выделение эвристических признаков скрипт-вирусов	201
6.5. Другие признаки наличия в системе скрипт-вирусов	205
Выводы	206
Контрольные вопросы	206
7. ТЕХНОЛОГИЯ БЕЗОПАСНОГО ПРОГРАММИРОВАНИЯ	208
7.1. Безопасность компилируемых языков	211
7.1.1. Особенности построения и функционирования программных продуктов с точки зрения безопасного программирования	211
7.1.2. Уязвимость переполнения буфера.....	218
7.1.3. Уязвимость строки формата	237
7.1.4. Уязвимость целочисленного переполнения	246
7.1.5. Уязвимость индексации массива	262
7.1.6. Состязания	267
7.2. Безопасность интерпретаторов	279

7.2.1. Уязвимость подключения внешних файлов	279
7.2.2. Уязвимость использования глобальных переменных	283
7.2.3. Уязвимость внедрения команд	285
7.2.4. Уязвимость внедрения SQL кода	292
Выводы	297
Контрольные вопросы	298
Заключение	299
Список литературы	301
Приложение 1. Криптосистема Пайе	311
Приложение 2. Проблема ф-скрытия	313
Приложение 3. Криптосистема Эль-Гамала	315
Список используемых сокращений	317
Список терминов	317