

УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



Антивирусная безопасность цифровой информации

Горячая линия-Телеком



Н. Х. Нагаев

ОГЛАВЛЕНИЕ

От автора	3
Введение	4
I. Этногенез компьютерных вирусов	8
1.1. Доисторический период	10
1.2. У истоков вирусописания	11
1.3. Начало эры компьютерных вирусов	14
1.4. Первые компьютерные вирусы	14
1.5. Первый компьютерный сетевой вирус	16
1.6. Первая масштабная эпидемия	17
1.7. Рождение компьютерной вирусологии	18
1.8. Пандемия первого компьютерного вируса для IBM PC	19
1.9. Начало эры загрузочных вирусов	21
1.10. Эволюция компьютерных вирусов	27
1.11. Отсроченные эпидемии	29
1.12. Начало законодательных инициатив: сетевой червь Морриса	32
1.13. Компьютерные вирусные эпидемии	38
1.14. Компьютерные мистификации и вредоносная мимикрия	40
1.15. Первые конструкторы компьютерных вирусов	47
1.16. Первые антивирусные программы	51
II. Этносфера компьютерных вирусов	56
2.1. Толкование термина цифровой информации	56
2.2. Основы компьютерной вирусологии	60
2.2.1. Биологические родственники компьютерных вирусов	61
2.2.2. Определение понятия компьютерного вируса	62
2.2.3. Основные термины и определения компьютерной вирусологии	64
2.2.4. Стадии функционирования компьютерных вирусов	65
2.2.5. Основные признаки проявления компьютерных вирусов	65

2.3. Общепринятая классификация вредоносных компьютерных программ (глазами аналитика)	66
2.3.1. Классификация по среде обитания	67
2.3.2. Классификация по способу заражения	68
2.3.3. Классификация по деструктивному воздействию	68
2.3.4. Классификация по особенностям алгоритма вируса .	68
III. Вредоносное программное обеспечение	72
3.1. Классификация вредоносного программного обеспечения (с точки зрения профессионала)	72
3.1.1. Вредоносные программы	74
3.1.2. Потенциально нежелательные программы	88
3.2. Правила именования детектируемых объектов	90
3.3. Пути распространения вредоносного программного обеспечения	90
3.4. Формы организации вирусных атак	92
3.5. Стандартные методы заражения компьютерными вирусами	93
3.6. Признаки заражения вредоносным программным обеспечением	94
IV. Программно-математическое воздействие на информацию	95
4.1. Понятие программно-математического воздействия на информацию	95
4.2. Основные виды вредоносных программ (с точки зрения регулятора)	96
4.3. Классификация программных вирусов и сетевых червей (с точки зрения регулятора)	97
4.3.1. Среда обитания	97
4.3.2. Заражаемые операционные системы	105
4.3.3. Деструктивные возможности	105
4.3.4. Особенности алгоритма работы и в зависимости от сложности кода	105
4.3.5. Использование Интернет-технологий	106
4.3.6. Способы проникновения в систему	106
V. Зоопарк вирусных программ	107
5.1. Троянские программы-вымогатели (категория «Ransomware»)	107
5.1.1. Типы программ-вымогателей	107
5.1.2. Примеры программ-вымогателей	108
5.1.3. Как распознать вредоносное электронное сообщение?	111

5.1.4. Использование программы для расшифровки данных	111
5.2. Вирусные программы категории «Adware»	112
5.2.1. Виды Adware-программ	112
5.2.2. Защита от Adware-программ	113
5.2.3. Разновидности программ категории «Adware»	113
5.3. Вирусные программы категории «Pornware»	117
5.3.1. Виды Pornware-программ	117
5.3.2. Защита от Pornware-программ	117
5.4. Вирусные программы категории «Riskware»	118
5.4.1. Виды Riskware-программ	118
5.4.2. Защита от Riskware-программ	119
VI Анатомия антивирусной защиты информации	121
6.1. Классы антивирусных средств защиты информации	122
6.2. Методы антивирусной защиты информации	124
6.2.1. Сигнатурный анализ	125
6.2.2. Эвристический анализ	126
6.2.3. Понятие проактивной защиты	128
6.3. Функциональные модули антивирусных программ	128
6.4. Дополнительные средства антивирусной защиты информации	130
6.4.1. Модуль обновления	130
6.4.2. Модуль планирования	130
6.4.3. Модуль управления	131
6.4.4. Карантин	132
6.4.5. Тестирование работы антивирусной программы	132
6.5. Управление антивирусной защитой информации	133
6.5.1. Уровни антивирусной защиты информации	133
6.5.2. Централизованное управление антивирусной защитой информации	136
6.5.3. Комплексная система антивирусной защиты информации	139
6.6. Методы проведения испытаний программных средств на наличие компьютерных вирусов	143
VII. Вирусы категории «In the Wild»	144
7.1. Понятие «дикого вируса»	144
7.2. Проект «WildList»	146
7.3. Проект «Альянс антивирусных специалистов»	147
7.4. Британский «Virus Bulletin»	148
7.5. Сертификация по версии ICSA Labs	149

VIII. Компьютерный андеграунд	152
8.1. Субкультура компьютерного андеграунда.....	152
8.1.1. Основные группы компьютерного андеграунда	154
8.1.2. Характеристика представителей компьютерного андеграунда	160
8.2. «Подземная» география	160
8.3. Компьютерные преступления	163
8.3.1. Понятие компьютерного преступления.....	163
8.3.2. Группы компьютерных преступников.....	165
8.3.3. Уголовно-криминалистическая классификация компьютерных преступников	166
8.3.4. Классификация компьютерных преступлений, основанная на кодификаторе Интерпола	168
8.4. Преступления в сфере обращения цифровой информации	178
8.4.1. Понятие преступлений в сфере обращения цифровой информации	178
8.4.2. Виды преступлений в сфере обращения цифровой информации	179
8.4.3. Классификация преступлений в сфере обращения цифровой информации.....	180
8.4.4. Преступления в сфере обращения цифровой информации (в соответствии с УК РФ).....	182
8.5. Компьютерная криминалистика (форензика).....	183
8.5.1. Определение термина «форензика»	183
8.5.2. Состав форензики	185
8.6. Экскурс в историю хакерства	186
8.6.1. Определение термина «хакер»	187
8.6.2. «Настоящие программисты»	189
8.6.3. Зарождение хакерства	189
8.6.4. Телефонные фризеры и Cap'n Crunch	191
8.6.5. Создание ARPAnet.....	192
8.6.6. Хакерские доски сообщений и сообщества хакеров ...	194
8.6.7. Детские игры	195
8.6.8. Хакерские издания.....	196
8.6.9. От компьютера до тюрьмы	197
8.6.10. Хакерский инструментарий всем желающим.....	198
8.7. Портрет вирусописателя (вирмейкера)	199
Заключение.....	203
Литература.....	205