

ОГЛАВЛЕНИЕ

Предисловие.....	3
Глава 1. Анализ программных реализаций, защита программ от анализа	6
1.1. Общие сведения	6
1.2. Метод экспериментов с «черным ящиком»	9
1.3. Статический метод	14
1.4. Динамический метод.....	22
1.4.1. Программные отладочные средства	22
1.4.2. Методика изучения программ динамическим методом	27
Метод маяков	27
Метод Step-Trace первого этапа.....	31
Метод аппаратной точки останова	33
Метод Step-Trace второго этапа.....	33
1.4.3. Пример применения динамического метода.....	34
1.5. Особенности анализа некоторых видов программ.....	44
1.5.1. Особенности анализа оверлейных программ	44
1.5.2. Особенности анализа графических программ Windows.....	45
1.5.3. Пример анализа графической программы Windows	48
1.5.4. Особенности анализа параллельного кода	54
1.5.5. Особенности анализа кода в режиме ядра Windows	55
1.6. Вспомогательные инструменты анализа программ.....	58
Монитор активности процессов ProcMon.....	58
Утилита управления процессами Process Explorer	59
1.7. Защита программ от анализа	63
Динамическое изменение кода программы.....	66
Искусственное усложнение структуры программы	68
Нестандартные обращения к функциям операционной системы.....	72
Искусственное усложнение алгоритмов обработки данных	76
Выявление факта выполнения программы под отладчиком	77
Глава 2. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам.....	84
2.1. Общие сведения.....	84
2.2. Субъектно-ориентированная модель компьютерной системы	85

2.3. Модели взаимодействия программной закладки с атакуемой системой	89
2.3.1. Модель «наблюдатель»	89
2.3.2. Модель «перехват»	93
2.3.3. Модель «искажение»	97
Несанкционированное использование средств динамического изменения полномочий	98
Порождение дочернего процесса системным процессом	100
Модификация машинного кода монитора безопасности объектов	101
2.4. Предпосылки к внедрению программных закладок	103
2.4.1. Общие сведения	103
Утверждение	103
Следствие	104
2.4.2. Переполнения буферов	105
2.4.3. Отсутствие необходимых проверок входных данных	115
GetAdmin	115
Уязвимость %00	116
2.4.4. Некорректный контекст безопасности	117
AdminTrap	117
Системные окна на рабочем столе пользователя	118
2.4.5. Устаревшие функции	118
NetDDE Exploit	118
WMF Exploit (MS06-001)	119
2.4.6. Другие уязвимости	120
Уязвимость program.exe	120
2.5. Методы внедрения программных закладок	121
Маскировка программной закладки под прикладное программное обеспечение	123
Маскировка программной закладки под системное программное обеспечение	126
Подмена системного программного обеспечения	129
Прямое ассоциирование	131
Косвенное ассоциирование	132
2.6. Компьютерные вирусы как особый класс программных закладок	132
2.7. Средства и методы защиты от программных закладок	154
Сканирование системы на предмет наличия известных программных закладок	158
Контроль целостности программного обеспечения	162
Контроль целостности конфигурации защищаемой системы	164
Антивирусный мониторинг информационных потоков	168
Программные ловушки	169
2.8. Организационные и административные меры антивирусной защиты	169
Инструктирование пользователей	169
Просмотр и анализ данных регистрации и мониторинга	170

Контроль качества аутентификационных данных пользователей	171
Регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной защиты сети, в случае успешных вирусных атак.....	172
Регулярные инспекции состояния антивирусной защиты	172
2.9. Выявление программных закладок в ручном режиме	175
Приложение... ..	191
Методические рекомендации по организации изучения дисциплины «Защита программ и данных»	191
Анализ требований ФГОС ВПО	191
Организация изучения защиты программ и данных	193
Список литературы.....	195
Рекомендуемая литература	195
Интернет-ресурсы	196