

Казарин, О. В.

Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М.: Издательство Юрайт, 2017. — 312 с. — Серия : Специалист.

Оглавление

Принятые сокращения.....	7
Предисловие.....	8
Глава 1. Введение в теорию и практику защиты программного обеспечения.....	12
1.1. Проблема защиты программного обеспечения информационных систем.....	12
1.2. Объекты защиты.....	13
1.3. Уязвимости и угрозы безопасности программного обеспечения.....	14
1.3.1. Уязвимости программного обеспечения.....	14
1.3.2. Угрозы безопасности программного обеспечения.....	19
1.3.3. Вредоносные программы.....	20
1.3.4. Несанкционированное исследование и копирование программ.....	22
1.4. Жизненный цикл программного обеспечения информационных систем. Технологическая и эксплуатационная безопасность программного обеспечения.....	24
1.5. Основные принципы обеспечения безопасности программного обеспечения.....	27
1.6. Защита программного обеспечения как система научных дисциплин.....	29
<i>Контрольные вопросы и задания.....</i>	<i>31</i>
<i>Рекомендуемая литература.....</i>	<i>32</i>
Глава 2. Основания теории и практики защиты программного обеспечения.....	33
2.1. Элементы теории алгоритмов.....	33
2.2. Элементы теории сложности вычислений.....	36
2.2.1. Классы сложности вычислений.....	36
2.2.2. Односторонние функции и функции с секретом.....	37
2.2.3. Псевдослучайные генераторы.....	38
2.3. Элементы криптологии.....	39
2.3.1. Основные задачи криптографии.....	39
2.3.2. Криптосистемы с секретным и открытым ключом.....	39
2.3.3. Схемы электронной подписи.....	41
2.3.4. Криптографически стойкие схемы хэширования.....	43
2.3.5. Криптографически стойкие псевдослучайные генераторы.....	46
2.3.6. Схемы вероятностного шифрования.....	47
2.4. Информационные технологии и операционные системы.....	48
<i>Контрольные вопросы и задания.....</i>	<i>50</i>
<i>Рекомендуемая литература.....</i>	<i>51</i>

Глава 3. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	52
3.1. Классификация вредоносных программ.....	52
3.1.1. Троянские программы.....	52
3.1.2. Компьютерные вирусы.....	54
3.1.3. Прочие вредоносные программы.....	62
3.2. Защита от вредоносных программ.....	64
3.3. Методы тестирования программного обеспечения на его защищенность	67
3.3.1. Методы тестирования программ.....	67
3.3.2. Фаззинг программ.....	69
3.4. Методы защиты программ от несанкционированного исследования.....	70
3.4.1. Классификация средств несанкционированного исследования программ.....	70
3.4.2. Способы защиты программ от несанкционированного исследования.....	71
3.4.3. Обфускация программ.....	77
3.4.4. Способы встраивания защитных механизмов в программное обеспечение.....	85
3.5. Методы защиты программ от несанкционированного копирования.....	86
3.5.1. Криптографические методы защиты от копирования.....	86
3.5.2. Метод привязки к идентификатору.....	86
3.5.3. Методы, основанные на работе с переходами и стеком.....	87
3.5.4. Манипуляции с кодом программы.....	87
3.5.5. Методы противодействия динамическим способам снятия защиты программ от копирования.....	88
3.6. Методы описания и обнаружения уязвимостей программного обеспечения на примере операционных систем.....	89
3.6.1. Уязвимости на примере ОС Windows.....	89
3.6.2. Методы обнаружения уязвимостей операционных систем.....	91
3.6.3. Подходы к разработке защищенных операционных систем.....	95
<i>Контрольные вопросы и задания.....</i>	<i>96</i>
<i>Рекомендуемая литература.....</i>	<i>96</i>
Глава 4. Средства, системы и комплексы защиты программного обеспечения.....	98
4.1. Средства и комплексы защиты от вредоносных программ.....	98
4.2. Средства, системы и комплексы тестирования программного обеспечения при испытаниях его на технологическую безопасность.....	101
4.2.1. Методологические основы оценки качества, проведения испытаний и сертификации программных средств.....	101
4.2.2. Построение программно-аппаратных комплексов для контроля технологической безопасности программ.....	110
4.2.3. Фаззеры программ.....	119
4.2.4. Пример тестирования ПО средств защиты информации.....	122
4.3. Обфускаторы программ.....	132
4.3.1. Задача и цели и обфускации. Оценка эффективности обфускации	132
4.3.2. Примеры обфускаторов программ, написанных на скриптовых языках.....	138

4.4. Способы и средства защиты программ от несанкционированного копирования.....	143
4.5. Защищенные операционные системы.....	148
4.5.1. Создание дистрибутива ОС Linux с повышенными требованиями к ее защищенности.....	148
4.5.2. Пример построения мобильной защищенной операционной системы на базе ОС Android.....	149
<i>Контрольные вопросы и задания.....</i>	<i>156</i>
<i>Рекомендуемая литература.....</i>	<i>157</i>
Глава 5. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей.....	159
5.1. Сертификация средств защиты информации по требованиям безопасности информации.....	159
5.2. Проверка соответствия реальных и декларируемых функциональных возможностей.....	160
5.3. Проверка отсутствия недекларируемых возможностей.....	161
5.3.1. Методы проведения испытаний.....	161
5.3.2. Документация, представляемая на испытания.....	162
5.4. Контроль исходного состояния программного комплекса посредством утилиты «ФИКС».....	171
5.5. Статический анализ исходных текстов и исполняемых модулей ПО.....	172
5.5.1. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов.....	172
5.5.2. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.....	175
5.5.3. Контроль связей функциональных объектов по управлению и информации.....	175
5.5.4. Синтаксический контроль наличия заданных конструкций.....	176
5.5.5. Формирование и анализ маршрутов выполнения функциональных объектов.....	177
5.6. Динамический анализ исходных текстов программ.....	178
<i>Контрольные вопросы и задания.....</i>	<i>179</i>
<i>Рекомендуемая литература.....</i>	<i>180</i>
Глава 6. Краткое описание отечественных нормативных актов, регламентирующих деятельность в области защиты программного обеспечения.....	181
6.1. Федеральный закон «Об информации, информационных технологиях и о защите информации».....	181
6.2. ГОСТ Р ИСО/МЭК 15408-2013.....	182
6.3. ГОСТ Р ИСО/МЭК 18045-2013.....	183
6.4. ГОСТ Р МЭК 61508—2012.....	185
6.5. ГОСТ Р 56939-2016.....	186
6.6. Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей».....	186

6.7. Приказ ФСТЭК России от 14 марта 2014 г. № 31.....	187
6.8. Требования к средствам антивирусной защиты ФСТЭК России.....	188
6.9. Банк данных угроз безопасности информации ФСТЭК России.....	188
<i>Контрольные вопросы и задания.....</i>	<i>189</i>
<i>Рекомендуемая литература.....</i>	<i>189</i>
Заключение.....	191
Список литературы.....	192
Приложения.....	196
Приложение 1. Краткий терминологический словарь.....	196
Приложение 2. Примерные темы докладов, рефератов, заданий для самостоятельной работы студентов.....	199
Приложение 3. Примерные планы практических занятий и лабораторных работ и порядок их проведения.....	200
Приложение 4. Примеры выполнения заданий для самостоятельной работы студента.....	207
Приложение 5. Особенности вредоносных программ нового поколения.....	271
Приложение 6. Средства доставки вредоносных программ до объектов их атаки.....	308