

•ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ•

ВЫСШЕЕ ОБРАЗОВАНИЕ



О. В. Казарин, И. Б. Шубинский

# НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ

ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



**УМО ВО**  
РЕКОМЕНДУЕТ

 **Юрайт**  
Издательство

# Оглавление

Принятые сокращения.....	9
Предисловие .....	10
<b>Глава 1. Введение в надежность и безопасность программного обеспечения.....</b>	<b>14</b>
1.1. Виды программного обеспечения.....	14
1.1.1. Системное (базовое) программное обеспечение .....	14
1.1.2. Прикладное программное обеспечение.....	15
1.1.3. Программы встроенных систем .....	16
1.2. Функциональная надежность программного обеспечения в информационных системах.....	18
1.3. Понятие общей надежности информационной системы .....	24
1.4. Отказобезопасность и кибербезопасность информационных систем .....	26
1.4.1. Отказобезопасность информационной системы .....	26
1.4.2. Кибербезопасность информационной системы .....	30
1.5. Взаимосвязь функциональной и информационной безопасности критически важных систем.....	34
<i>Контрольные вопросы и задания.....</i>	<i>36</i>
<i>Рекомендуемая литература .....</i>	<i>36</i>
<b>Глава 2. Угрозы надежности и безопасности программного обеспечения .....</b>	<b>38</b>
2.1. Уязвимости программного обеспечения .....	38
2.2. Ошибки в программном обеспечении .....	40
2.3. Характерные недостатки эксплуатируемых программ.....	46
2.4. Вредоносные программы .....	46
<i>Контрольные вопросы и задания.....</i>	<i>47</i>
<i>Рекомендуемая литература .....</i>	<i>47</i>
<b>Глава 3. Качество программного обеспечения .....</b>	<b>48</b>
3.1. Модели качества программного обеспечения .....	48
3.2. Метрики качества программного обеспечения .....	52
3.2.1. Классификация метрик качества программ .....	52
3.2.2. Классификация метрик сложности программ .....	54
3.2.2.1. Метрики размера программ.....	54
3.2.2.2. Метрики сложности потока управления программ .....	55
3.2.2.3. Метрики сложности потока данных программ.....	56

3.3. Некоторые общие замечания по стратегии и тактике обеспечения надежности и безопасности различных видов программного обеспечения .....	58
3.4. Обеспечение надежности и безопасности программного обеспечения на различных этапах его жизненного цикла.....	59
3.4.1. Жизненный цикл функциональной надежности ПО .....	59
3.4.2. Жизненный цикл обеспечения безопасности ПО.....	64
<i>Контрольные вопросы и задания</i> .....	66
<i>Рекомендуемая литература</i> .....	66
<b>Глава 4. Правила и этапы построения надежного программного обеспечения.....</b>	<b>68</b>
4.1. Маршрутная карта обеспечения функциональной надежности программного обеспечения .....	68
4.2. Модели надежности программного обеспечения .....	70
4.2.1. Исходные данные и некоторые понятия .....	70
4.2.2. Анализ существующих моделей надежности программного обеспечения .....	71
4.2.2.1. Общие замечания .....	71
4.2.2.2. Прогнозирующие модели.....	72
4.2.2.3. Оценочные модели.....	73
4.2.2.4. Измерительные модели.....	78
4.2.2.5. Модель Нельсона .....	79
4.3. Показатели функциональной надежности и функциональной безопасности ПО.....	86
4.4. Пример расчета функциональной надежности программы .....	91
<i>Контрольные вопросы и задания</i> .....	93
<i>Рекомендуемая литература</i> .....	93
<b>Глава 5. Технологии разработки надежного программного обеспечения.....</b>	<b>95</b>
5.1. Рекомендации по разработке спецификации требований .....	95
5.2. Технология разработки архитектуры надежной программы .....	96
5.2.1. Классификация методов построения архитектуры надежной программы.....	96
5.2.2. Предупреждение ошибок .....	97
5.2.2.1. Защитное программирование .....	97
5.2.2.2. Многоверсионное программирование.....	100
5.2.3. Обнаружение ошибок.....	104
5.2.4. Исправление ошибок.....	106
5.2.5. Устойчивость к ошибкам.....	107
5.3. Проектирование надежного программного обеспечения и его реализация.....	111
5.4. Интеграция программного обеспечения с аппаратными средствами .....	113
5.5. Обеспечение надежности программного обеспечения в процессе подтверждения соответствия, эксплуатации и сопровождения .....	117
5.5.1. Подтверждение соответствия программного обеспечения.....	117

5.5.2. Эксплуатация, сопровождение и конфигурация функционально надежных программных средств.....	119
5.6. Требования к функциональной надежности и архитектуре программного обеспечения критически важных систем .....	122
5.6.1. Спецификация требований к функциональной надежности ПО .....	122
5.6.2. Требования к архитектуре функционально надежного ПО .....	123
<i>Контрольные вопросы и задания</i> .....	125
<i>Рекомендуемая литература</i> .....	125

## **Глава 6. Методы и технологии обеспечения безопасности программного обеспечения.....127**

6.1. Методы доказательства правильности программ .....	127
6.1.1. Общие положения .....	127
6.1.2. Предусловия и постусловия в доказательствах правильности .....	130
6.1.3. Правила вывода (доказательства) .....	131
6.1.4. Применение правил вывода .....	139
6.1.5. Пример доказательства правильности программы для алгоритма дискретного экспоненцирования .....	140
6.2. Методы создания самотестирующихся и самокорректирующихся программ.....	146
6.2.1. Общие положения .....	146
6.2.2. Пример самотестирующейся/самокорректирующейся программной пары для функции дискретного экспоненцирования .....	149
6.2.2.1. Обозначения и определения для функции дискретного возведения в степень вида $A^x \text{ modulo } N$ .....	149
6.2.2.2. Построение самотестирующейся/самокорректирующейся программной пары для функции дискретного экспоненцирования .....	150
6.2.3. Области применения самотестирующихся и самокорректирующихся программ и их сочетаний .....	154
6.2.3.1. Вычислительная математика .....	154
6.2.3.2. Криптография, интерактивные доказательства .....	160
6.3. Криптографические методы защиты от вредоносных программ .....	161
6.3.1. Методы аутентификации и обеспечения целостности программ.....	161
6.3.2. Методы инкрементальной криптографии .....	162
6.3.2.1. Цель разработки инкрементальных схем .....	162
6.3.2.2. Разработка алгоритмов инкрементальной аутентификации.....	163
6.3.2.3. Вопросы стойкости инкрементальных схем .....	165
6.3.2.4. Использование инкрементальных схем для защиты ПО .....	167
6.3.2.5. Заключительные замечания .....	169
6.4. Технологии защиты от вредоносных программ .....	169
6.4.1. Классификация вредоносных программ .....	169
6.4.1.1. Общие сведения.....	169
6.4.1.2. Троянские программы.....	170

6.4.1.3. Компьютерные вирусы.....	172
6.4.1.4. Прочие вредоносные программы .....	180
6.4.2. Защита от вредоносных программ.....	182
6.5. Технологии тестирования программного обеспечения на его защищенность.....	185
6.5.1. Методологические основы анализа программных средств на предмет наличия (отсутствия) недеklarированных возможностей .....	185
6.5.1.1. Статические и динамические способы исследования ПО.....	185
6.5.1.2. Методологические основы проведения испытаний, оценки качества и сертификации программных средств.....	188
6.5.1.3. Общая номенклатура показателей качества ПО .....	190
6.5.1.4. Выбор номенклатуры показателей качества ПО.....	192
6.5.1.5. Оценка значений показателей качества ПО.....	192
6.5.1.6. Организационные вопросы проведения испытаний ПО .....	196
6.5.1.7. Методологические вопросы проведения испытаний ПО .....	196
6.5.2. Построение программно-аппаратных комплексов для контроля технологической безопасности программ .....	197
6.5.2.1. Состав инструментальных средств контроля безопасности ПО при его разработке.....	197
6.5.2.2. Структура и принципы построения программно- аппаратных средств контрольно-испытательного стенда испытания технологической безопасности ПО .....	204
6.5.3. Методы тестирования и квалификационного тестирования программ.....	209
6.5.4. Фаззинг программ .....	211
6.6. Методы защиты программ от несанкционированного исследования .....	212
6.6.1. Способы защиты программ от несанкционированного исследования .....	212
6.6.1.1. Компоненты защиты исследуемой программы .....	212
6.6.1.2. Классификация способов защиты от несанкционированного исследования .....	213
6.6.1.3. Динамическое преобразование программы во время ее исполнения .....	215
6.6.1.4. Защита от трассировки программы по заданному событию.....	217
6.6.2. Способы встраивания защитных механизмов в программное обеспечение.....	218
6.6.3. Обфускация и деобфускация программ .....	219
6.6.3.1. Назначение обфускации и деобфускации программ .....	219
6.6.3.2. Определение обфускатора .....	221
6.6.3.3. Методы обфускации .....	221
6.6.3.4. Методы деобфускации.....	224

<i>Контрольные вопросы и задания</i> .....	225
<i>Рекомендуемая литература</i> .....	226

**Глава 7. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения..... 228**

7.1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» .....	228
7.2. ГОСТ Р ИСО/МЭК 15408—2013.....	230
7.3. ГОСТ Р ИСО/МЭК 18045—2013.....	231
7.4. ГОСТ Р МЭК 61508—2012 .....	232
7.5. Приказ ФСТЭК России от 14 марта 2014 г. № 31 .....	233
7.6. Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недеklarированных возможностей».....	234
7.7. Требования к средствам антивирусной защиты (информационное сообщение ФСТЭК России от 30 июля 2012 г. № 240/24/3095) .....	235
<i>Контрольные вопросы и задания</i> .....	236
<i>Рекомендуемая литература</i> .....	236

**Глава 8. Подтверждение соответствия надежности и безопасности программного обеспечения..... 238**

8.1. Основные понятия в области подтверждения соответствия .....	238
8.2. Натурные испытания надежности и безопасности информационных систем .....	243
8.3. Методы ускорения испытаний.....	246
8.3.1. Два подхода к ускорению испытаний.....	246
8.3.2. Метод Монте-Карло .....	248
8.3.3. Метод значимой выборки.....	250
8.4. Метод ускоренных натуральных испытаний на надежность и функциональную безопасность информационных систем .....	251
8.4.1. Теоретические основы метода ускоренных натуральных испытаний.....	251
8.4.2. Приложение метода к ускоренным натурным испытаниям информационной системы управления технологическими процессами .....	254
8.4.3. Оценка продолжительности испытаний.....	260
8.5. Пример ускоренных натуральных испытаний на функциональную безопасность информационной системы управления технологическим процессом .....	261
8.5.1. Описание объекта испытаний.....	261
8.5.2. Цель испытаний и критерии отказов.....	263
8.5.3. Алгоритмы генерации сбоев и помех.....	264
8.5.4. Порядок проведения испытаний.....	268
8.5.5. Обработка и оценка результатов испытаний.....	270

8.6. Основные положения Методики испытаний качества и функциональной безопасности программного обеспечения .....	271
8.7. Основные положения Методики испытаний по требованиям безопасности информации .....	275
8.7.1. Перечень проверок и испытаний .....	275
8.7.2. Контроль состава и содержания документации.....	277
8.7.3. Контроль исходного состояния ПО.....	279
8.7.4. Статический анализ исходных текстов программ .....	279
8.7.5. Динамический анализ исходных текстов программ.....	282
8.7.6. Контроль полноты и корректности реализации технических приемов .....	283
8.7.7. Обработка, анализ и оценка результатов испытаний .....	285
8.8. Порядок подтверждения соответствия требованиям комплексной безопасности программного обеспечения.....	286
<i>Контрольные вопросы и задания.....</i>	290
<i>Рекомендуемая литература .....</i>	290
<b>Заключение.....</b>	<b>293</b>

## Приложения

<b>Приложение 1.</b> Краткий терминологический словарь .....	297
<b>Приложение 2.</b> Перечень типовых дефектов разработки ПО, влияющих на его безопасность, и программных закладок, замаскированных под дефекты разработки ПО (пример) .....	301
<b>Приложение 3.</b> Формы проявления программных дефектов (пример) .....	302
<b>Приложение 4.</b> Перечень характеристик ПО, влияющих на защищенность и результаты работы ПО (пример) .....	304
<b>Приложение 5.</b> Извлечения из ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению» .....	305
<b>Список литературы .....</b>	<b>337</b>