

*А.И. Белоус, В.А. Солодуха, С.В. Шведов*

**ПРОГРАММНЫЕ  
И АППАРАТНЫЕ  
ТРОЯНЫ —  
СПОСОБЫ ВНЕДРЕНИЯ  
И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ**

*Первая техническая энциклопедия  
В 2-х книгах*

**Книга 1**



ТЕХНОСФЕРА



# МИР электроники

А.И. Белоус,  
В.А. Солодуха,  
С.В. Шведов

Программные  
и аппаратные трояны –  
способы внедрения  
и методы противодействия.  
Первая техническая  
энциклопедия

Под общей редакцией  
А.И. Белоуса

В 2-х книгах  
Книга I

ТЕХНОСФЕРА  
Москва  
2019

УДК 004.492  
ББК 32.85  
Б43

**Б43 Белоус А.И., Солодуха В.А., Шведов С.В.**  
**Программные и аппаратные трояны – способы внедрения  
и методы противодействия. Первая техническая энциклопедия**  
Под общей редакцией Белоуса А.И.  
В 2-х книгах  
Книга I  
**Москва: ТЕХНОСФЕРА, 2019. – 688 с. ISBN 978-5-94836-524-4**

Впервые в мировой научно-технической литературе в объеме одного комплексного издания последовательно и детально исследован феномен программных и аппаратных троянов, которые фактически являются технологической платформой современного и перспективного информационно-технического оружия (кибероружия). Материал энциклопедии представлен в виде 12 глав.

В первой вводной главе, обобщающей результаты анализа технических возможностей и ограничений современного оружия (атомного, космического, сейсмического, климатического, различных видов СВЧ-оружия), показано, что развитие всех «обычных» и «новейших» видов вооружений дошло до такой стадии, что их реальное использование на практике будет равносильно самоубийству начавшей войну стороны. Осознание этого факта привело к развитию информационно-технического оружия (кибероружия и нейрооружия). В главе 2 детально исследованы концепции, методы, технические средства и примеры реализации этого вида оружия. В главе 3 рассмотрены основные виды программных троянов, вирусов и шпионских программ, которые в «кибероперациях» обычно действуют солидарно, защищая и помогая друг другу. В главе 4 наглядно показан эволюционный путь развития аппаратных троянов от «ящиков» и «коробочек» до микросхем, приведены примеры их применения в компьютерах, серверах, мобильных телефонах, автомобилях и даже в одежде и обуви человека. В главах с 5-й по 9-ю детально рассмотрены основные типы троянов в микросхемах, принципы их проектирования и работы, способы внедрения, методы их маскировки, выявления в микросхемах, а также защиты и противодействия. В главах с 10-й по 12-ю представлен детальный сравнительный ретроспективный анализ основ государственной политики в США и России в области обеспечения безопасности каналов поставки микросхем.

Книга ориентирована на широкий круг читателей: от инженеров, специалистов по информационной безопасности, чиновников министерств и ведомств до школьников и пенсионеров, активно использующих социальные сети.

УДК 004.492  
ББК 32.85

© 2018, Белоус А.И., Солодуха В.А., Шведов С.В.  
© 2019, АО «РИЦ «ТЕХНОСФЕРА», оригинал-макет, оформление

**ISBN 978-5-94836-524-4**

## Содержание

<b>Предисловие</b> .....	15
<b>Введение</b> .....	19
<b>Глава 1. Современное оружие: технические возможности и ограничения</b> .....	22
1.1. Некоторые научно-технические и военно-стратегические аспекты построения и использования средств поражения космического эшелона противоракетной обороны .....	22
1.1.1. Технические возможности и ограничения потенциальных средств поражения баллистических ракет .....	22
1.1.2. Космический эшелон противоракетной обороны .....	23
1.1.3. Анализ основных типов потенциальных космических средств поражения противовоздушной обороны .....	25
1.1.4. Проблемы обеспечения надежности функционирования средств космического эшелона системы ПРО .....	29
1.1.5. Европейская безопасность и европейская СПРО.....	35
1.1.6. Космический эшелон системы предупреждения о ракетном нападении.....	39
1.1.6.1. Российская космическая система обнаружения стартов ракет.....	39
1.1.6.2. Военно-разведывательные спутники.....	44
1.1.6.3. Роль военно-технической разведки в современных локальных конфликтах .....	50
1.2. СВЧ-оружие наземного применения .....	52
1.2.1. Основные поражающие факторы и методы воздействия СВЧ-излучений на системы управления радиоэлектронных устройств .....	52
1.2.2. СВЧ-оружие боевого применения.....	54
1.3. Оружие несмертельного (нелетального) действия наземного применения.....	58
1.3.1. СВЧ-оружие «система активного отбрасывания» .....	59
1.3.2. Лазерное устройство PHASR для временного ослепления и дезориентации противника .....	64
1.3.3. «Бесшумный страж» (Silent Guardian).....	65
1.3.4. Наиболее известные системы нелетального оружия из арсенала Министерства обороны США.....	66
1.3.4.1. «Глушитель речи».....	66
1.3.4.2. The Incapacitating Flashlight .....	67
1.3.4.3. Суперзловонный артиллерийский снаряд .....	67
1.3.4.4. «Гей-бомба» – оружие на мощных афродизиаках .....	68
1.3.4.5. Генератор грома .....	68
1.3.4.6. Перцовая граната.....	69
1.3.4.7. Электрошокер Taser Shotgun .....	69
1.3.5. Проблемы безопасности применения нелетального оружия .....	70



1.4. СВЧ-оружие атмосферного и космического применения .....	72
1.4.1. Радиочастотное космическое оружие.....	72
1.4.2. Космическое оружие на основе новых физических принципов.....	75
1.4.3. Системы перехвата МБР на основе плазменного СВЧ-оружия.....	77
1.4.4. Лазерное оружие.....	79
1.4.5. Пучковое СВЧ-оружие.....	81
1.5. СВЧ-комплексы противодействия высокоточному оружию .....	82
1.5.1. Классификация, способы применения и типовые цели систем высокоточного оружия .....	82
1.5.2. Типовой состав и принцип работы комплекса защиты от высокоточного оружия .....	86
1.6. Использование СВЧ-импульсов в задачах защиты от элементов высокоточного оружия .....	89
1.7. Американская программа высокочастотных активных исследований HAARP .....	101
1.7.1. Теоретические механизмы возможного использования HAARP для управления погодой планеты Земля.....	101
1.7.1.1. Эксперименты Николы Теслы .....	101
1.7.1.2. Возможности использования HAARP в качестве атмосферного оружия.....	105
1.7.1.3. Управление погодой – побочный продукт работ по ПРО .....	107
1.7.2. Сравнение предполагаемых функции систем типа HAARP, созданных в мире (США, Европа, СССР).....	108
1.7.3. Хемоакустические волны – основа сейсмического оружия.....	112
1.8. Нейронное оружие .....	118
1.8.1. Военная нейробиология.....	118
1.8.2. Военная нейрофармакология .....	121
1.8.3. Искусственная стимуляция умственной деятельности .....	122
1.8.4. Интерфейсы типа «мозг – компьютер».....	123
1.8.5. Биохимическое нейронное оружие .....	124
1.8.6. Направленное энергетическое оружие (DEW) .....	125
1.8.7. Нейронное оружие на основе информации / программного обеспечения .....	126
1.8.8. Угрозы нейронного оружия .....	128
1.8.9. Опасности «неправильного» использования нейронных технологий.....	129
1.8.10. Особенности и преимущества США, России и Китая в гонке нейронных вооружений. ....	130
1.8.11. Новые «нейронные угрозы» международной безопасности.....	132
1.8.12. Нейронная безопасность и нейронная этика.....	133
1.8.13. Стратегия обеспечения нейронной безопасности .....	135
1.8.14. От психологических операций до нейровойны: основные опасности .....	137
1.9. Вместо заключения .....	139

<b>Глава 2. Информационное оружие в технической сфере: концепции, средства, методы и примеры применения</b> .....	152
2.1. Информационная безопасность суверенного государства .....	152
2.1.1. Исторические аспекты возникновения и развития информационной безопасности .....	152
2.1.2. Основные цели и объекты информационной безопасности государства .....	155
2.1.3. Источники угроз для информационной безопасности .....	155
2.1.4. Основные задачи обеспечения информационной безопасности .....	157
2.1.5. Технологии информационной безопасности .....	158
2.2. Основы ведения информационной войны .....	163
2.2.1. Понятие «информационная война» .....	163
2.2.2. Виды информационных атак .....	167
2.2.3. Средства информационной войны .....	167
2.2.4. Классификация информационно-технического оружия .....	169
2.3. Определение и классификация информационно-технических воздействий .....	175
2.4. Наиболее распространенные средства информационно-технического воздействия .....	183
2.4.1. Удаленные сетевые атаки .....	183
2.4.1.1. Определение и классификация удаленных сетевых атак .....	183
2.4.2. Примеры способов информационно-технических воздействий с использованием удаленных сетевых атак .....	187
2.4.2.1. Анализ сетевого трафика .....	188
2.4.2.2. Подмена доверенного объекта или субъекта информационной системы .....	189
2.4.2.3. Внедрение ложного объекта в информационную систему .....	190
2.4.2.4. Использование ложного объекта для организации удаленной атаки .....	191
2.4.2.5. Отказ в обслуживании .....	193
2.5. Технические каналы утечки информации .....	195
2.5.1. Классификация и принципы функционирования .....	195
2.5.2. Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники .....	199
2.5.3. Электрические каналы утечки информации .....	203
2.5.4. Специально создаваемые технические каналы утечки информации .....	206
2.6. Заключение .....	213
<b>Глава 3. Компьютерные вирусы, программные закладки и шпионские программы</b> .....	223
3.1. Компьютерные вирусы .....	223
3.1.1. Термины и определения .....	223

3.1.2. Краткая история возникновения компьютерных вирусов .....	224
3.1.3. Классификация компьютерных вирусов.....	227
3.2. Компьютерные вирусы и троянские программы .....	243
3.2.1. Особенности применения вируса Stuxnet как разновидности кибероружия .....	243
3.2.2. Программные закладки: типы, способы внедрения и методы защиты.....	246
3.2.2.1. Программные закладки: основные типы и определения.....	246
3.2.2.2. Опасности программных закладок .....	247
3.2.2.3. Классификации программных закладок .....	248
3.2.2.4. Разновидности программных закладок .....	250
3.2.2.5. Троянские программы: типы и особенности поведения.....	255
3.3. Программные закладки.....	257
3.3.1. Основные принципы реализации программных закладок.....	257
3.3.1.1. Введение в проблему программных закладок .....	257
3.3.1.2. Основные пути внедрения программных закладок.....	258
3.3.1.3. Механизмы организации необнаруживаемого управления.....	259
3.3.1.4. Использование криптографии .....	259
3.3.1.5. Использование корневых комплектов.....	260
3.3.1.6. Программные бекдоры в компьютерных системах.....	261
3.3.1.7. Примеры реально подтвержденных аппаратных закладок .....	265
3.3.1.8. Основные методы защиты от троянов и закладок.....	269
3.4. Модели воздействия на компьютеры программных закладок, способы внедрения и их взаимодействие с нарушителем.....	271
3.4.1. Модели воздействия программных закладок на компьютеры.....	271
3.4.2. Способы внедрения программных закладок и компьютерных вирусов .....	272
3.4.3. Сценарии внедрения программных закладок на различных этапах жизненного цикла программного обеспечения.....	274
3.4.4. Способы взаимодействия между программной закладкой и нарушителем .....	275
3.4.4.1. Определение понятия нарушителя .....	275
3.4.4.2. Интернет .....	276
3.4.4.3. Электронная почта .....	276
3.4.4.4. Методы защиты от программных закладок.....	277
3.4.4.5. Методы выявления внедренной программной закладки .....	278
3.4.4.6. Удаление внедренной программной закладки .....	279
3.4.4.7. Средства создания ложных объектов информационного пространства.....	279

3.5. Программные клавиатурные шпионы.....	281
3.5.1. Принцип работы клавиатурных шпионов .....	281
3.5.2. Методы слежения за клавиатурным вводом .....	282
3.5.2.1. Слежение за клавиатурным вводом при помощи ловушек.....	282
3.5.2.2. Слежение за клавиатурным вводом при помощи опроса клавиатуры .....	283
3.5.2.3. Слежение за клавиатурным вводом при помощи перехвата API-функций .....	283
3.5.2.4. Типовой пример клавиатурного шпиона.....	284
3.5.2.5. Методики поиска клавиатурных шпионов.....	285
3.5.2.6. Клавиатурные шпионы на основе драйверов-фильтров.....	285
3.5.2.7. Клавиатурные шпионы на базе RootKit-технологии в UserMode.....	287
3.5.2.8. Клавиатурный шпион на базе RootKit-технологии в KernelMode.....	288
3.5.2.9. Программы для поиска и удаления клавиатурных шпионов.....	289
3.6. Основные принципы работы RootKit-технологий .....	291
3.6.1. Что такое RootKit-технология?.....	291
3.6.2. Методы перехвата API-функций в режиме пользователя .....	292
3.6.3. Методы перехвата функций RootKit в режиме ядра .....	296
3.6.4. Основные методики обнаружения RootKit в системе .....	297
3.6.5. Типовой механизм проникновения в систему троянских программ RootKit.....	298
3.7. Шпионские программы типа cookies .....	300
3.7.1. Основные назначения cookies.....	300
3.7.2. Методика хранения cookies.....	302
3.7.3. Основные разновидности cookies .....	303
3.7.4. Пути утечки и угрозы, создаваемые cookies .....	304
3.7.5. Методы настройки параметров работы с cookies .....	306
3.7.5.1. Настройка параметров работы с cookies для IE 6 .....	306
3.7.5.2. Настройка параметров работы с cookies для Mozilla Firefox.....	309
3.8. Шпионская программа RegIn .....	310
3.9. Официальные позиции спецслужб США в отношении программных закладок .....	311
3.9.1. Официальная позиция ФБР США в отношении бекдоров.....	311
3.9.2. Официальная (публичная) позиция Агентства национальной безопасности (АНБ) США по отношению к бекдорам и аппаратным троянам и реальная ситуация .....	313
3.9.3. Шпионские программы АНБ .....	314
3.9.3.1. Основные программные средства АНБ .....	314
3.9.3.2. Программные средства АНБ для использования в сетях Wi-Fi.....	316



3.9.3.3. Программные средства АНБ для поражения серверов вычислительных сетей .....	316
3.9.3.4. Программные средства АНБ для контроля сетевого оборудования .....	317
3.9.3.5. Программные средства АНБ для контроля сетей GPM.....	318
3.9.3.6. Шпионские средства АНБ для контроля оборудования в помещениях типовых офисов .....	319
3.10. Пример способа внедрения программного трояна в стандартный PE-файл операционной системы Microsoft Windows .....	319
3.10.1. Назначение и структура PE-файлов .....	319
3.10.2. Основные методы размещения программного трояна в PE-файлах .....	322
3.10.3. Решение проблемы нахождения доступного пространства для кода трояна.....	324
3.10.4. Перехват текущего потока выполнения .....	329
3.10.5. Внедрение кода программного трояна .....	332
3.10.6. Восстановление потока выполнения.....	334
3.11. Примеры недокументированных функций в микросхемах 80-х годов .....	337
3.11.1. Причины появления недокументированных функций .....	337
3.11.2. Основные недокументированные команды микропроцессора Z80 .....	340
3.11.3. Недокументированные возможности процессоров Intel 80×86 .....	341
3.11.4. Недокументированные возможности микроконтроллеров семейства MCS-51 .....	344
3.11.5. Недокументированные функции микросхемы SA9605A.....	346
3.11.6. Метод сдвигового регистра (LSSD) как основной метод анализа микросхем на предмет наличия закладок.....	347
3.11.7. Описание метода JTAG как основного средства сканирования микросхемы.....	349
3.12. Методы снятия секретной информации на основании анализа акустических и электромагнитных излучений .....	353
3.12.1. Нейтрализаторы тестовых программ и программ анализа кода .....	354
3.12.2. Трояны .....	356
3.12.3. Back Orifice.....	357
3.12.4. NetBus .....	359
3.12.5. D.I.R.T.....	362
3.12.6. Paparazzi .....	364
3.12.7. Способы распознавания троянских программ.....	365
3.12.8. Логические бомбы .....	366
3.12.9. Мониторы .....	367
3.12.10. Компьютерные черви .....	367

3.12.11. Перехватчики паролей.....	368
3.12.12. Программы-шутки.....	369
3.13. Особенности организации защиты информации при работе с криптовалютами.....	369
<b>Глава 4. Трояны в электронной аппаратуре.....</b>	<b>378</b>
4.1. Программно-аппаратные трояны в телекоммуникационных системах .....	378
4.1.1. Трояны в сетевом оборудовании.....	378
4.1.2. Трояны в маршрутизаторах.....	380
4.1.3. Межсетевые экраны.....	381
4.1.4. Беспроводные сети.....	383
4.1.5. Трояны в рабочих серверах .....	383
4.1.6. Трояны в оборудовании рабочих мест операторов телекоммуникационных систем.....	384
4.2. Аппаратные трояны в компьютерах .....	385
4.2.1. Аппаратные трояны в системном блоке.....	385
4.2.2. Аппаратные трояны для подключения к USB.....	386
4.2.3. Трояны для перехвата информации, вводимой через клавиатуру компьютера.....	387
4.2.4. Троянские программы в жестких дисках компьютера.....	393
4.3. Трояны в системах мобильной связи.....	394
4.3.1. Основные эпизоды из истории противостояния спецслужб и хакеров в области телефонии .....	394
4.3.2. «Жучок» в запчасти для смартфона – еще одна возможность для шпиона .....	397
4.3.3. Предустановленный троян в китайских смартфонах Nomi и Leagoo .....	399
4.3.4. Расширение возможностей мобильных телефонов за счет подключения специализированных модулей .....	401
4.3.5. Мини-шпионы в мобильном телефоне.....	406
4.3.5.1. Устройство блокирования мобильного телефона .....	406
4.3.5.2. Использование мобильных телефонов Nokia в качестве мини-шпионов.....	408
4.3.5.3. Мобильный телефон со встроенным мини-шпионом в батарейном отсеке .....	408
4.3.5.4. Определение местоположения мобильного телефона путем пеленгации по трем точкам .....	409
4.3.6. Основные технические решения по защите телефонных переговоров .....	410
4.3.6.1. Аппарат TopSec GSM.....	411
4.3.6.2. Аппарат HC-2413 .....	412
4.3.6.3. Аппарат Sectra Tiger .....	413
4.3.6.4. Аппарат «Референт ПДА» (Россия) .....	413
4.3.6.5. Телефон-невидимка.....	414

4.3.6.6. Пути внедрения трояна в мобильный телефон .....	417
4.3.6.7. Специальные вирусы и программы для смартфонов .....	419
4.4. Электронные приборы для беспроводного перехвата данных .....	421
4.4.1. Черный ананас – WiFi Pineapple.....	421
4.5. Трояны и автомобили .....	425
4.5.1. Устройства для определения маршрута движения автомобиля с помощью GPS .....	425
4.5.2. Новый вид угроз – автомобильные вирусы .....	427
4.6. Экзотические «шпионские штучки» .....	430
4.6.1. Похищение данных через кулер компьютера .....	430
4.6.2. Перехват изображения с экрана ноутбука.....	432
4.6.3. Миниатюрные радиомаяки в обуви и в одежде .....	434
4.6.4. Извлечение 4096-битных ключей RSA с помощью микрофона .....	436
4.6.5. Как узнать все о человеке с помощью социальных сетей .....	438
4.7. Трояны в бытовой электронике .....	443
<b>Глава 5. Аппаратные трояны в микросхемах.....</b>	<b>447</b>
5.1. Основы проектирования безопасной электронной аппаратуры для ответственных применений.....	447
5.1.1. Введение в проблему .....	447
5.1.2. Оценка безопасности этапов маршрута проектирования микросхем .....	453
5.1.3. Потенциальные агенты (организаторы) атак с использованием аппаратных троянов.....	459
5.1.4. Авторская попытка систематизации имеющихся знаний о методах обеспечения безопасности каналов поставки микросхем .....	460
5.2. Описание первых задокументированных фактов обнаружения аппаратных троянов в микросхемах ответственного назначения .....	468
5.2.1. Введение в проблему .....	468
5.2.2. Особенности и критические точки структуры обеспечения безопасности микросхемы ProASIC3.....	473
5.2.3. Краткое описание методики экспериментального определения аппаратного трояна в микросхеме A3P250 Actel.....	478
5.2.4. Анализ результатов контрольного эксперимента по выявлению аппаратного трояна в микросхеме специального назначения ProASIC3.....	481
5.2.5. Аппаратные трояны в серийных процессорах .....	487
5.2.5.1. Способы реализации аппаратных троянов в процессорах.....	487
5.2.5.2. Аппаратные трояны в процессорах фирмы Intel .....	490
5.3. Классификация аппаратных троянов в микросхемах.....	496
5.3.1. Постановка задачи .....	496
5.3.2. Основная классификация аппаратных троянов .....	497

5.4. Способы внедрения аппаратных троянов в микросхемы .....	504
5.4.1. Введение в проблему .....	504
5.4.2. Иерархические уровни внедрения троянов в микросхемы .....	511
5.5. Механизмы активации внедренных аппаратных троянов.....	513
5.6. Методы выявления аппаратных троянов в микросхемах ответственного назначения.....	521
5.6.1. Введение в проблему .....	521
5.6.2. Основные методы выявления аппаратных троянов.....	524
5.6.2.1. Анализ методов с использованием сторонних каналов .....	524
5.6.2.2. Вредоносные компьютерные системы .....	524
5.6.2.3. Повышение успешности обнаружения троянов .....	525
5.6.2.4. Применение характеристики логических элементов для обнаружения троянов .....	525
5.6.2.5. Использование специальных шинных архитектур, защищенных от троянов .....	526
5.6.2.6. Передача данных посредством «тихих» троянов .....	526
5.6.2.7. Защита многоядерных архитектур .....	527
5.6.2.8. Использование определения в период исполнения .....	527
5.6.2.9. Развитие методов анализа по сторонним каналам .....	528
5.6.2.10. Метод локализации трояна в микросхеме .....	528
5.6.2.11. Усовершенствованная характеристика логических элементов .....	529
5.6.2.12. Утечка данных посредством троянов .....	529
5.6.2.13. Модели многоуровневых атак .....	530
5.6.2.14. Использование комбинированных методов анализа по сторонним каналам .....	530
5.6.2.15. Повышение вероятности активации троянов за счет дополнительных триггеров .....	531
5.6.2.16. Избегание внедренных троянов.....	531
5.6.2.17. Использование кольцевых генераторов для обнаружения троянов .....	532
5.7. Исследование конкретного случая разработки и реализации аппаратного трояна .....	537
5.7.1. Обоснование и мотивация .....	540
5.7.1.1. Критический анализ цепочки поставки ИС.....	540
5.7.1.2. Терминология уязвимостей цепочки поставки .....	541
5.7.1.3. Измерение.....	542
5.7.1.4. Воровство .....	542
5.7.2. Иерархическая классификация атакующих.....	543
5.7.2.1. Действия атакующего на этапе проектирования.....	544
5.7.2.2. Атакующий на этапе синтеза .....	544
5.7.2.3. Атакующий на этапе изготовления.....	545
5.7.2.4. Атакующий в структуре сбыта.....	546



5.8. Особенности внедрения аппаратных троянов в пассивные радиочастотные метки.....	565
5.8.1. Введение в проблему.....	565
5.8.2. Радиочастотные метки EPC C1G2 и аппаратные трояны.....	566
5.8.3. Механизмы запуска аппаратных троянов в радиочастотных метках EPC C1G2.....	568
5.8.4. Результаты экспериментальных исследований.....	573
5.9. Аппаратные трояны в беспроводных криптографических ИС.....	577
5.9.1. Особенности организации утечки информации из беспроводных криптографически защищенных микросхем.....	577
5.9.2. Существующие методы обнаружения троянов.....	585
5.10. Методы проектирования аппаратных закладок.....	592
5.10.1. Проектирование последовательных аппаратных закладок.....	593
5.10.1.1. Модель функциональных последовательных аппаратных закладок.....	594
5.10.1.2. Ожидаемое время до срабатывания.....	596
5.10.1.3. Оптимизированная реализация.....	597
5.10.1.4. Практические примеры проектирования аппаратных закладок, которые могут использоваться в программном обеспечении встраиваемого процессора.....	598
5.10.1.5. Условия срабатывания аппаратной закладки.....	599
5.10.2. Примеры проектирования аппаратных закладок с использованием дополнительных вентиляей.....	604
5.10.3. Пример внедрения аппаратной закладки на вентиляльном уровне для обхода структуры, защищаемой сетью кольцевых генераторов (RON).....	607
5.11. Оптимистический анализ методов выявления аппаратных троянов в микросхемах.....	613
5.11.1. Авторское введение в проблему.....	613
5.11.2. Основные методы обнаружения троянов в ИС после изготовления в серийном производстве.....	617
5.11.3. Методы обнаружения троянов до реализации микросхемы в кремнии.....	620
5.11.4. Определение наиболее точной модели атаки троянов.....	627
5.11.4.1. Комплексные модели атаки.....	627
5.11.4.2. Отношение между ранее проведенными исследованиями и моделями атаки.....	629
5.11.4.3. Анализ основных тенденций исследований аппаратных троянов.....	630
5.11.5. Методы обнаружения аппаратных троянов в микросхемах.....	634
5.11.5.1. Обнаружение аппаратных троянов в коммерческих микросхемах.....	634

5.11.5.2. Обнаружение аппаратных троянов без эталонной модели .....	635
5.11.5.3. Аппаратные трояны в трехмерных интегральных схемах .....	637
5.11.6. Перспективы развития методов выявления троянов .....	638
5.11.6.1. Определение подлинности приобретенных на рынке коммерческих микросхем .....	638
5.11.6.2. Общий подход к анализу уязвимостей .....	639
5.11.6.3. Конструкция микросхемы, невосприимчивой или устойчивой к аппаратным троянам .....	640
5.11.6.4. Появление новых видов аппаратных троянов .....	640
<b>Глава 6. Особенности внедрения аппаратных троянов в микросхемы памяти .....</b>	<b>648</b>
6.1. Введение в проблему .....	648
6.2. Основные виды моделей отказов в микросистемах SRAM .....	651
6.3. Анализ стандартных алгоритмов тестирования микросхемы SRAM .....	653
6.4. Анализ типовых механизмов запуска троянов в SRAM .....	656
6.5. Анализ аппаратных троянов типа «короткое замыкание» .....	660
6.6. Аппаратные трояны в SRAM типа «резистивный обрыв» .....	664
6.7. Верификация внедренных в SRAM аппаратных троянов .....	668
6.8. Механизм функционирования в SRAM аппаратных троянов типа «короткое замыкание» .....	672
6.9. Экспериментальные результаты исследований аппаратных троянов типа «короткое замыкание» .....	677
6.10. Экспериментальные результаты исследований аппаратных троянов типа «обрыв» .....	680