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 2

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 2

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 2
Москва: ТЕХНОСФЕРА, 2019. – 630 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

ISBN 978-5-94836-524-4

Содержание

Глава 7. Методы выявления аппаратных троянов в микросхемах.....700
7.1. Краткий обзор основных методов выявления аппаратных троянов в микросхемах ответственного назначения.....700
7.1.1. Введение в проблему.....700
7.1.2. Анализ с использованием сторонних каналов.....703
7.1.3. Вредоносные компьютерные системы.....703
7.1.4. Методы повышения вероятности обнаружения троянов.....704
7.1.5. Методы характеризации логических элементов для обнаружения троянов.....704
7.1.6. Использование специальных шинных архитектур, защищенных от троянов.....705
7.1.7. Передача данных посредством «тихих» троянов.....705
7.1.8. Обнаружение троянов в многоядерных архитектурах.....706
7.1.9. Методы выявления и программной изоляции внедренных троянов.....706
7.1.10. Усовершенствованные методы анализа по сторонним каналам.....707
7.1.11. Применение дополнительной цепи сканирования для локализации трояна в микросхеме.....707
7.1.12. Методы термического кондиционирования.....708
7.1.13. Методы предотвращения утечки информации по скрытым каналам.....709
7.1.14. Модели многоуровневых троянских атак.....709
7.1.15. Использование комбинированных методов анализа по сторонним каналам.....709
7.1.16. Повышение вероятности активации троянов за счет дополнительных триггеров.....710
7.1.17. Методы нейтрализации внедренных в микросхемы троянов.....711
7.1.18. Использование кольцевых генераторов для обнаружения троянов.....712
7.2. Методы обнаружения аппаратных троянов в микросхемах на основе анализа спектра электромагнитного излучения.....717
7.2.1. Ретроспективный обзор альтернативных методов выявления троянов в микросхемах.....717
7.2.2. Методы выявления аппаратных троянов с помощью анализа спектров электромагнитных излучений.....721
7.2.3. Экспериментальные результаты проверки эффективности метода.....726
7.3. Особенности выявления последовательных аппаратных троянов с использованием метода TeSR.....731
7.3.1. Введение в проблему.....731
7.3.2. Особенности учета технологического разброса параметров микросхемы при реализации методов выявления троянов.....735

7.3.2.1. Критический обзор других близких методов выявления аппаратных троянов 735
7.3.2.2. Используемые модели атаки при реализации метода TeSR 737
7.3.3. Демонстрационные примеры выявления последовательных аппаратных троянов с использованием TESR 738
7.3.4. Концепция и способы реализации метода TeSR 741
7.3.5. Необходимые пояснения и уточнения к методу TeSR 744
7.3.5.1. Методологический подход к генерированию измерительных тестов MERO 744
7.3.5.2. Описание схемы обработки результатов измерений 747
7.2.5.3. Точность обнаружения внедренного аппаратного трояна 748
7.3.5.4. Роль цепей сканирования при выявлении аппаратных троянов 749
7.3.6. Метод проектирования микросхем с учетом обеспечения требований безопасности (DFS) 752
7.3.7. Основные отличительные особенности тестирования 755
7.3.8. Примеры оценки эффективности выявления троянов по методике TeSR 756
7.3.8.1. Исходные данные для проведения экспериментальных исследований 756
7.3.8.2. Анализ результатов моделирования 757
7.3.9. Экспериментальное подтверждение метода анализа побочных каналов 760
7.4. Другие методы исследований и обнаружения аппаратных троянов в микросхемах 767
7.4.1. Введение в проблему 767
7.4.2. Особенности проектирования и классификация троянов 770
7.4.3. Методы обнаружения троянов 773
7.4.3.1. Методы обнаружения троянов с использованием анализа сигналов сторонних каналов 773
7.4.3.2. Методы анализа по мощности потребления микросхем 774
7.4.4. Анализ на основе временных характеристик 778
7.4.5. Методы активации троянов 780
7.4.6. Методы обнаружения троянов на уровне архитектуры 782
7.4.7. Методы обеспечения аппаратной защиты от троянов 785
7.5. Конкретные примеры из опыта работы белорусских «охотников за троянами» 794

Глава 8. Обратное проектирование микросхем 810
8.1. Введение в проблему обратного проектирования микросхем 810
8.1.1. Предпосылки возникновения проблемы, термины и определения 810

8.1.2. Стандартный маршрут реализации процесса Reverse Engineering 817
8.1.3. Особенности современного машиностроительного производства 818
8.2. Защита прав интеллектуальной собственности на полупроводниковые микросхемы 820
8.2.1. Особенности использования процесса обратного проектирования для защиты патентных прав 820
8.2.2. Закон США «О защите прав на полупроводниковые микросхемы» 826
8.2.2.1. История появления закона 826
8.2.2.2. Особая форма защиты полупроводниковых микросхем 828
8.2.2.3. Описание закона США «О защите прав на полупроводниковые микросхемы» 830
8.2.2.4. Положения о международной двусторонней защите 835
8.2.2.5. Иностранные законы о защите топологий интегральных микросхем 837
8.2.2.6. Об охране интеллектуальных прав на топологии интегральных микросхем в Российской Федерации 842
8.3. Основы искусства обратного проектирования 844
8.3.1. Роль и место обратного проектирования в полупроводниковой промышленности 844
8.3.2. Основные этапы реализации классического процесса обратного проектирования микроэлектронных устройств 846
8.3.2.1. Демонтаж изделия 846
8.3.2.2. Анализ микроэлектронного изделия на системном уровне 847
8.3.2.3. Анализ технологического процесса изготовления устройства 851
8.3.2.4. Экстракция параметров микросхемы 854
8.3.2.5. Разгерметизация корпуса микросхемы 855
8.3.2.6. Получение изображений 858
8.3.2.7. Верификация и создание восстановленной электрической схемы 860
8.3.2.8. Упорядочивание и анализ электрической схемы 860
8.3.2.9. Пример практической реализации обратного проектирования для ASIC 861
8.4. Типовая методика восстановления топологии кристалла микросхем 866
8.4.1. Сравнительный анализ микроскопических методов анализа топологий интегральных схем 866
8.4.2. Особенности реализации покадрового совмещения фрагментов топологии 868
8.4.3. Методика реализации процесса совмещения двух кадров изображения топологии 870

8.4.4. Описание процесса совмещения группы кадров изображения 875
8.4.5. Описание процесса послойного наложения слоев топологии кристалла.....877
8.4.6. Конкретные способы повышения качества воспроизведения топологии ИС 882
8.4.7. Описание типовой системы обратного проектирования (реинжиниринга) интегральных микросхем 887
8.5. Методы восстановления электрической схемы из топологии кристалла.....894
8.5.1. Методы автоматизации процесса размещения элементов на растровом изображении топологии 894
8.5.2. Особенности программной реализации процесса восстановления электрической схемы из топологии 900
8.5.3. Методы автоматизации трассирования восстановленных электрических связей между элементами 906
8.5.4. Основные требования к качеству исходных растровых изображений топологии 908
8.6. Методика подготовки образцов субмикронных микросхем для исследований электрофизическими РЭМ-методами.....914
8.6.1. Разработка методики подготовки образцов субмикронных микросхем для исследования их с помощью РЭМ.....914
8.6.1.1. Изготовление сколов ИМС.....915
8.6.1.2. Изготовление шлифов.....915
8.6.1.3. Запыление непроводящих образцов 916
8.6.1.4. Исследование сколов ИМС без декорирования 917
8.6.1.5. Метод декорирования 918
8.6.1.6. Методика подготовки образцов для исследования методом РЭМ.....920
8.6.2. Методика подготовки образцов кристаллов для исследований электрофизическими методами при последовательном механическом и химическом удалении топологических слоев с использованием автоматической системы селективной обработки ASAP-1.....920
8.7. Методы защиты и противодействия процессам реинжиниринга микросхем космического и военного назначения 921
8.7.1. Классификация основных методов противодействия реинжинирингу микросхем специального назначения 921
8.7.2. Конструктивно-схемотехнические методы противодействия реинжинирингу микросхем военного и специального назначения 925
8.7.2.1. Конструктивно-технические методы противодействия реинжинирингу микросхем военного и специального назначения 926
8.7.2.2. Способы внедрения в конструкцию микросхем скрытых (замаскированных) межсоединений 926

8.7.2.3. Способ введения дополнительных проводящих трасс и межслойных соединений 927
8.7.2.4. Способы внедрения нефункционирующих (всегда включенных или всегда выключенных) транзисторов 929
8.7.3. Схемотехнические методы противодействия реинжинирингу микросхем специального назначения 934
8.8. Практические примеры схемотехнических методов защиты микросхем от реинжиниринга 941
8.8.1. Интегральная реализация встроенной схемы контроля питания 942
8.8.2. Нестандартные элементы защиты биполярных микросхем от электрических перегрузок и статического электричества 946
8.8.3. Особенности схемотехники защищенных выходных каскадов микросхем с диодами Шоттки 949
8.8.4. Примеры проектирования триггерных схем с повышенной защитой от реинжиниринга 956
8.9. Аналитические возможности отечественных реинжиниринговых центров 962
8.9.1. Аналитические возможности холдинга «Интеграл» 962
8.9.2. Российские реинжиниринговые центры 975

Глава 9. Методы противодействия аппаратным троянам в микросхемах 977
9.1. Программно-аппаратные методы противодействия аппаратным троянам в микросхемах 977
9.1.1. Защита данных 977
9.1.2. Защищенные архитектуры на RTL-уровне 981
9.1.3. Реконфигурируемые архитектуры 983
9.1.4. Репликация и другие методы защиты 985
9.2. Проектирование в целях обеспечения безопасности системы на кристалле 989
9.2.1. Введение в проблему 989
9.2.2. Описание структуры модуля безопасности 992
9.2.2.1. Введение в IP-инфраструктуры 992
9.2.2.2. Стандарт IEEE 1500 993
9.2.3. Структура модуля IIPS 995
9.2.4. Проектирование функций безопасности IIPS 998
9.2.4.1. Модели атак и стратегии по устранению их последствий 998
9.2.4.2. Примеры реализации простейших безопасных структур SoC 1001
9.2.5. Протокол испытаний микросхемы согласно стандарту IEEE Std. 1500 1008
9.2.5.1. Режимы работы элементов обвязки микросхемы 1008
9.2.5.2. Особенности протокола тестирования SoC уровня IIPS 1010

9.2.6. Результаты моделирования демонстрационной версии безопасной SoC ... 1013
9.2.6.1. Временная диаграмма работы системы ... 1013
9.2.6.2. Методики обнаружения аппаратных троянов в SoC ... 1015
9.2.6.3. Оценка необходимых аппаратных затрат для выявления трояна ... 1018
9.2.7. Описание дополнительных возможностей блока IIPS ... 1020
9.3. Безопасная архитектура SoC ... 1027
9.3.1. Введение в проблему ... 1027
9.3.2. Структура и принцип работы стандартной шины SoC ... 1029
9.3.3. Организация и принцип работы дешифратора адреса ... 1031
9.3.4. Структура и принцип работы блока арбитра ... 1033
9.3.5. Описание работы системы на кристалле непосредственно после обнаружения аппаратного трояна ... 1036
9.3.6. Оценка аппаратных затрат на реализацию метода обеспечения безопасности ... 1038
9.4. Основы безопасности проектирования микросхем ... 1042
9.4.1. Постановка задачи ... 1042
9.4.2. Анализ типового маршрута проектирования микросхем ... 1044
9.4.3. Возможные типы атак ... 1046
9.4.4. Основные различия между разработкой безопасных микросхем и разработкой безопасных программ ... 1047
9.4.5. Жизненный цикл разработки безопасного программного обеспечения ... 1048
9.4.6. Методы безопасного проектирования микросхем ... 1049
9.4.6.1. Этапы безопасного проектирования микросхем ... 1049
9.4.6.2. Описание моделей угроз ... 1049
9.4.6.3. Прослеживаемость в микросхеме ... 1050
9.4.6.4. Цикл обнаружения ... 1052
9.4.7. Экспериментальные результаты применения метода HTDS ... 1053
9.4.8. Краткий обзор близких по тематике HTDS-исследований ... 1055
9.5. Использование «песочницы» как метод защиты от аппаратных троянов в SoC ... 1058
9.5.1. Введение в проблему ... 1058
9.5.2. «Песочница» как инструмент обеспечения безопасности ... 1060
9.5.3. Анализ сходных направлений решения проблемы безопасности проектирования SoC ... 1061
9.5.4. Особенности организации процедур перемещения аппаратных троянов в «песочницу» при проектировании SoC ... 1063
9.5.5. Основные программные методы помещения в «песочницу» ... 1065
9.5.6. Типовая структура аппаратной «песочницы» ... 1066
9.5.7. Описание типового процесса проектирования защищенной SoC ... 1067
9.5.8. Анализ практических примеров реализации «песочницы» в SoC ... 1071

9.6. Пример использования математических инструментов теории игр для противодействия аппаратным троянам в ИС 1077
9.6.1. Введение в проблему 1077
9.6.2. Технические решения проблемы 1078
9.6.3. Математический аппарат моделирования атак 1079
9.7. Программно-аппаратные методы защиты FPGA от несанкционированного копирования информации 1080
9.7.1. Защита микросхем специальной памяти на основе метода IFF 1080
9.7.2. Микросхемы серии Reference Design компании Altera 1082
9.8. Методы отслеживания безопасности микросхем после их изготовления в производстве 1086
9.8.1. Введение в проблему 1086
9.8.2. Модели отслеживания безопасности изготовленных микросхем 1087
9.8.3. Пассивные измерения микросхем 1090
9.8.4. Активные аппаратные измерения микросхем 1094
9.8.5. Внутренние (интегрированные) активные аппаратные измерения микросхем 1096
9.8.6. Внешние активные аппаратные измерения микросхем 1099

Глава 10. Основы государственной политики США в области обеспечения безопасности каналов поставки микросхем 1103
10.1. В качестве введения 1103
10.1.1. Мнения авторитетных экспертов по проблемам обеспечения информационной безопасности 1103
10.1.2. Первые задокументированные факты выявления недостоверных каналов поставки микросхем военного назначения 1110
10.1.3. Реакция АНБ и DARPA на появление новых угроз 1115
10.2. Структура и функции Министерства обороны США 1117
10.3. Стратегия обеспечения кибербезопасности в США 1120
10.4. Организационная структура DARPA 1125
10.5. Структура формирования и управления программами научно-исследовательских работ Министерства обороны США 1133
10.5.1. Научно-исследовательские проекты Министерства обороны США 1133
10.5.2. Особенности формирования и управления проектами DARPA 1138
10.5.3. Контрактация НИОКР 1142
10.6. Стратегия Министерства обороны США по обеспечению безопасности микросхем 1144
10.6.1. Основные положения стратегии безопасности 1144
10.6.2. Политика Министерства обороны США в области планирования методов защиты каналов поставок микросхем военного назначения 1148

10.6.3. Основные требования МО США к доверенным источникам приобретения изделий микроэлектроники 1153
10.6.4. Нормативная база Министерства обороны США по обеспечению безопасности каналов поставки микросхем 1156
10.6.4.1. Введение в проблему 1156
10.6.4.2. Описание структуры типового плана программной защиты 1158
10.6.4.3. Краткое описание структуры нормативного документа 1159
10.7. Анализ специальных проектов DARPA в области киберугроз 1168
10.7.1. Введение 1168
10.7.2. Краткий аннотированный перечень реализованных проектов DARPA 1169
10.7.3. Модели киберугроз по определению DARPA 1175
10.7.4. Краткий аннотированный перечень российских проектов противодействия кибератакам 1180
10.8. Основы государственной политики США и ЕС в области экспорта микросхем ответственного назначения 1182
10.8.1. Законодательные ограничения экспорта в Россию микросхем, произведенных в США 1182
10.8.2. Законодательные ограничения экспорта электронных компонентов из Европы и других стран 1188
10.8.3. Международные организации контроля экспорта изделий военного назначения 1190
Приложение 1 к главе 10 1194
Приложение 2 к главе 10 1202

Глава 11. Особенности российской системы управления развитием военной электроники 1212
11.1. Основные проблемы обеспечения информационной безопасности российского оборонно-промышленного комплекса 1212
11.2. Система управления развитием российской военной электроники 1220
11.2.1. Введение в проблему 1220
11.2.2. Научно-методические основы решаемых 22 ЦНИИ функциональных задач 1221
11.2.3. Организация исследований надежности и анализа причин отказов военной электроники 1229
11.2.4. Ретроспективный анализ преобразований системы управления военной электроникой в РФ 1234
11.2.5. Перспективы развития филиала 46 ЦНИИ 1240
11.3. Каналы поставки микросхем для ОПК РФ 1244
11.3.1. Экономические причины и следствия глобализации полупроводниковой промышленности 1244

11.3.2. Основные источники поставок микросхем для ОПК РФ 1256
11.3.3. Основные риски каналов поставки микросхем для ОПК РФ 1260
11.4. Достоинства и недостатки применения индустриальной ЭКБ иностранного производства 1265
11.5. Анализ текущего состояния и перспектив развития российской ЭКБ специального и двойного назначения 1271
11.6. Аналоги DARPA и их роль в решении проблемы аппаратных троянов 1278
11.6.1. Введение в проблему 1278
11.6.2. Аналоги американского агентства DARPA в других странах 1279
11.7. О необходимости формирования государственной программы восстановления и развития отечественной электронной промышленности 1284

Глава 12. Вместо заключения 1289
12.1. Об авторской концепции изложения материала 1289
12.2. Что авторы узнали о троянах? 1290
12.3. О поиске подходящего «плагиата» для формулировки итогового заключения 1297
12.4. Еще раз об американском опыте обеспечения безопасности каналов поставок микросхем 1301
12.5. Американская «золотая пятерка безопасности» 1307

Приложение. Перечень авторов основных работ, графические и текстовые материалы которых использованы в книге 1313