



МИР электроники

В.Н. Федорец,

Е.Н. Белов,

С.В. Балыбин

ТЕХНОЛОГИИ ЗАЩИТЫ
МИКРОСХЕМ
ОТ ОБРАТНОГО
ПРОЕКТИРОВАНИЯ
В КОНТЕКСТЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ТЕХНОСФЕРА
Москва
2019

УДК 621.374
ББК 32.85
Ф33

*Рецензенты: д.т.н., профессор Колковский Ю.В. (АО НПП «Пульсар»),
д.т.н., доцент Сазонов К.В. (ВКА им. А.Ф.Можайского)*

Ф33 Федорец В.Н., Белов Е.Н., Балыбин С.В.

**Технологии защиты микросхем от обратного проектирования
в контексте информационной безопасности**

Москва: ТЕХНОСФЕРА, 2019. – 216с. ISBN 978-5-94836-562-6

В книге рассмотрены вопросы обеспечения информационной безопасности современной электронной компонентной базы, используемой при разработке радиоэлектронной аппаратуры различного назначения. Особое внимание уделено вопросам уязвимости, возникающим при разработке и изготовлении микросхем, создаваемых по fabless-технологии.

Авторами рассмотрены инженерно-технические и организационно-методические решения по защите от обратного проектирования современных микросхем.

Книга может быть полезна специалистам в области микроэлектроники, разработчикам отечественной элементной базы, а также студентам, обучающимся по специальностям, связанным с разработкой микросистем и информационной безопасностью.

УДК 621.374
ББК 32.85

© Федорец В.Н., Белов Е.Н., Балыбин С.В., 2019

© АО «РИЦ «ТЕХНОСФЕРА», оригинал-макет, оформление, 2019

ISBN 978-5-94836-562-6

СОДЕРЖАНИЕ

Предисловие	6
Список использованных сокращений	10
Введение	12

РАЗДЕЛ 1

Вопросы информационной безопасности и обратное проектирование микросхем	14
--	-----------

1.1. Глобализация в микроэлектронике – основная тенденция ее развития	18
1.2. Могут ли содержать угрозы изделия микроэлектроники?	27
1.2.1. Проблема контрафактных изделий микроэлектроники в России	28
1.2.2. Практические шаги к выявлению контрафакта.....	31
1.3. Угроза снижения безопасности изделий микроэлектроники злоумышленниками	38
1.4. Роль «доверия» при анализе информационной безопасности микросхем	46
1.4.1. «Доверие» и защищенность систем	46
1.4.2. Особенности угроз в области модулей доверенной загрузки и связь с обратным проектированием микросхем	47

РАЗДЕЛ 2

Обратное проектирование микросхем и защита от него	52
2.1. Цели и задачи обратного проектирования изделий микроэлектроники.....	54
2.2. Обратное проектирование микросхем и его возможности.....	55
2.2.1. Основные этапы обратного проектирования микросхем.....	55
2.2.2. Оценка возможностей обратного проектирования применительно к микросхемам, используемым в аппаратуре ответственного применения, разрабатываемой в России.....	59

2.3.	Защита от анализа структуры микросхемы	63
2.3.1.	Защита от удаления корпуса и защитного покрытия.....	63
2.3.2.	Защита микросхем от послойного восстановления топологии	64
2.3.3.	Защита микросхем от обратного проектирования с помощью разрушения объекта исследования	70
2.3.4.	Защита микросхем от обратного проектирования с помощью экранирования и камуфлирования.....	78
2.4.	Защита от анализа функций микросхемы	82
2.5.	Экономический аспект обратного проектирования	85

РАЗДЕЛ 3**Информационная безопасность в контексте
защиты интеллектуальной собственности
в микросхемах.....**

3.1.	Общие вопросы идентификации микросхем.....	90
3.2.	Кремниевая фабрика как потенциальный нарушитель.....	92
3.3.	Специализированные блоки идентификации	94
3.4.	Использование обфускации при защите микросхем.....	103
3.5.	Идентификация и аутентификация изделий микروэлектроники на основе физически неклонированных функций.....	106
3.5.1.	Краткая характеристика ФНФ.....	108
3.5.2.	Подход к использованию ФНФ в случае недоверия к кремниевой фабрике	115
3.6.	Скрытые метки для защиты собственной продукции.....	121

РАЗДЕЛ 4**Контроль однородности партий микросхем и
радиоэлектронной аппаратуры путем
измерения s-параметров (радиопортрета)
четырёхполюсника**

4.1.	Исследование s-параметров усилителя в корпусе	131
------	--	-----

4.2.	Исследование s-параметров микросхемы ПЛИС	140
------	--	-----

РАЗДЕЛ 5**Аппаратно-программная целостность
программируемых логических интегральных
схем в контексте обратного проектирования**

5.1.	Обратное проектирование ПЛИС: история и угрозы	145
5.1.1.	Обратное проектирование конфигурационного битового потока ПЛИС.....	146
5.1.2.	Защита от обратного проектирования конфигурационного битового потока ПЛИС.....	151
5.2.	Технические параметры ПЛИС и особенности объектов, для которых необходим контроль целостности	152
5.3.	Особенности обеспечения контроля целостности для высокоскоростных и многоядерных решений на базе ПЛИС	159
5.4.	Перспективы применения криптографии для контроля целостности	160
5.5.	Определение необходимых для реализации механизмов контроля аппаратной целостности конфигурационных данных	166
5.6.	Система оценок для определения уровня контроля целостности конфигурационных данных ПЛИС	170

Заключение.....	173
-----------------	-----

Список рисунков	175
-----------------------	-----

Список таблиц	180
---------------------	-----

Список литературы.....	181
------------------------	-----

Приложение А

«Иностранное» и «отечественное» производство: от диалектической борьбы к словесной казуистике.....	200
---	-----

Приложение В

Полезные термины и определения	204
--------------------------------------	-----