

Гелль П.

## Мобильные телефоны

### сопряжение ПК с сотовыми телефонами

В книге Патрика Гелля изложены основные принципы построения и работы системы сотовой связи GSM, описывается устройство мобильного телефона и рассказывается об услугах, предоставляемых сетью GSM. Отдельная глава посвящена SIM-картам.

Второе издание дополнено подробным описанием нового инструментария для работы с SIM-картами (BasicCard, BasicSIM), представлено программное обеспечение для считывающих устройств PC/SC. Рассматриваются как специальные программы, которые размещены на компакт-диске, так и имеющиеся на рынке промышленные программные продукты и сопутствующий инструментарий для экспериментов с SIM-картами при помощи ПК. Приводятся схемы и рисунки печатных плат, необходимые для самостоятельного изготовления устройств считывания SIM-карт, а также различных полезных и недорогих аксессуаров к мобильным телефонам.

В приложениях к книге содержатся глоссарий терминов и данные по международному роумингу.

Эта книга предназначена как для радиолюбителей, так и для тех пользователей сотовых телефонов, которые интересуются всевозможными техническими хитростями и оригинальными решениями.

ISBN 5-94074-406-0



**DMK**  
издательство



Мобильные телефоны тайны и секреты мобильных телефонов



Гелль П.

## Мобильные телефоны

### сопряжение ПК с сотовыми телефонами

**DMK**  
издательство

# Мобильные телефоны

**Патрик Гёлль**

Инженер EFREI

---

## **СОПРЯЖЕНИЕ ПК С СОТОВЫМИ ТЕЛЕФОНАМИ**

Второе издание,  
исправленное и дополненное



Москва, 2010

**УДК 621.396.218**  
**ББК 32.884.1**  
**Г31**

**Гёль П.**

**Г31** Сопряжение ПК с сотовыми телефонами: Пер. с фр. – 2-е изд., испр. идоп. – М.: ДМК Пресс, 2010. – 232 с.: ил. (Мобильные телефоны).

**ISBN 5-94074-406-0**

В книге Патрика Гёлля изложены основные принципы построения и работы системы сотовой связи GSM, описывается устройство мобильного телефона и рассказывается об услугах, предоставляемых сетью GSM. Отдельная глава посвящена SIM-картам.

Второе издание дополнено подробным описанием нового инструментария для работы с SIM-картами (BasicCard, BasicSIM), представлено программное обеспечение для считывающих устройств PC/SC. Рассматриваются как специальные программы, которые размещены на компакт-диске, так и имеющиеся на рынке промышленные программные продукты и сопутствующий инструментарий для экспериментов с SIM-картами при помощи ПК. Приводятся схемы и рисунки печатных плат, необходимые для самостоятельного изготовления устройств считывания SIM-карт, а также различных полезных и недорогих аксессуаров к мобильным телефонам.

В приложениях к книге содержатся глоссарий терминов и данные по международному роумингу.

Эта книга предназначена как для радиолюбителей, так и для тех пользователей сотовых телефонов, которые интересуются всевозможными техническими хитростями и оригинальными решениями.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельца авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно остается, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможный ущерб любого вида, связанный с применением содержащихся здесь сведений.

Все торговые знаки, упомянутые в настоящем издании, зарегистрированы. Случайное неправильное использование или пропуск торгового знака или названия его законного владельца не должно рассматриваться как нарушение прав собственности.

ISBN 2-10-006416-9 (фр.)  
 ISBN 5-94074-406-0 (рус.)

© DUNOD, Paris  
 © Перевод на русский язык,  
 оформление ДМК Пресс, 2010

# СОДЕРЖАНИЕ

	<b>Предисловие</b> .....	8
<b>1</b>	<b>Система GSM</b> .....	9
	1.1. Немного истории .....	10
	1.2. Стандарты GSM и ETSI .....	14
	1.3. Сеть цифровой связи .....	14
	1.4. Сеть сотовой связи .....	16
	1.5. Международная сеть .....	19
	1.6. Мобильный телефон в упрощенном варианте .....	20
<b>2</b>	<b>Сети</b> .....	23
	2.1. Операторы мобильной телефонной связи .....	24
	2.2. Используемые частоты .....	26
	2.3. Соты и базовые станции .....	29
	2.4. Мощность, радиус действия и распространение сигнала .....	35
	2.5. Пропускная способность и насыщение .....	38
	2.6. Услуги, предоставляемые сетями .....	40
	<i>Передача речи</i> .....	40
	<i>Вызов срочной помощи</i> .....	42
	<i>Передача данных и факсов</i> .....	44
	<i>Передача коротких сообщений</i> .....	45
	<i>Дополнительные услуги</i> .....	48
	2.7. Регистрация мобильных телефонов .....	50
	2.8. Автоматическая настройка на местную сеть связи, или роуминг .....	52
	2.9. Принципы тарификации .....	54
	2.10. Предоплаченное «путешествие» .....	55
<b>3</b>	<b>Мобильный телефон</b> .....	59
	3.1. Строение мобильного телефона стандарта GSM .....	61
	<i>Радиоблок</i> .....	61
	<i>Аудиоблок</i> .....	65
	<i>Блок логики</i> .....	66
	<i>SIM-карта</i> .....	67
	<i>Блок питания</i> .....	69
	<i>Антенны</i> .....	70
	<i>Вибраторы</i> .....	74

3.2. Основные типы мобильных телефонов .....	75
«Персонализированные» мобильные телефоны .....	76
Мобильные терминалы GPS .....	76
3.3. Интерфейс пользователя .....	78
Тональности сигнализации .....	78
Обычные команды .....	79
Специальные команды .....	82
Скрытые команды .....	86
<b>4 Набор инструментов GSM .....</b>	<b>89</b>
4.1. Детектор – повторитель звонка .....	90
4.2. Устройство считывания SIM-карт для ПК .....	97
4.3. «Шпион» за SIM-картами .....	107
4.4. Интерфейсы обмена данными .....	115
4.5. Вариант для однопроводной шины .....	120
4.6. «Пассивный усилитель» на 8 Вт .....	121
4.7. SIM-карта для тестирования .....	126
4.8 «BASICSIM» – инструментальная SIM-карта .....	126
<b>5 SIM-карта .....</b>	<b>131</b>
5.1. Кому принадлежит SIM-карта .....	132
5.2. Что содержит SIM-карта .....	133
5.3. SIM-карта и идентификация .....	137
5.4. Аутентификация и шифрование .....	140
5.5. Клонирование и подделка .....	142
5.6. Фазы развития стандарта GSM и таблица услуг, предоставляемых SIM-картой .....	143
5.7. Предварительный выбор языка .....	150
5.8. Классы доступа .....	152
5.9. Управление сетями .....	153
5.10. Локализация мобильного телефона .....	155
5.11. Административные данные и карты для тестирования .....	157
5.12. Промышленные считывающие устройства и программное обеспечение .....	160
Управление директориями .....	164
Управление короткими сообщениями .....	165
Управление сетями .....	166
Управление секретными кодами .....	166
Исследование SIM-карты .....	167
Копии SIM-карт .....	168
5.13. Программное обеспечение для считывающих устройств PC/SC .....	168
Программа диагностики .....	172
Программа сканирования SIM-карты .....	172

Проверка криптографии .....	173
«Навигатор» для SIM-карты .....	174
Интеграция в графический интерфейс Windows .....	176
5.14. Программы, размещенные на компакт-диске, и приложения .....	177
Каталог ACS .....	177
Каталог BASIC .....	178
Каталог BASICCARD .....	178
Каталог BASICSIM .....	179
Каталог CHIPDRIVE .....	180
Каталог CYBMOUSE .....	180
Каталог ELV .....	181
Каталог ESPION .....	181
Каталог INTERNET .....	181
Каталог LECTSIM .....	181
Каталог PCB .....	182
Каталог PCSC .....	182
Каталог SONS .....	183
Словарь GSM .....	183
Данные по международному роумингу .....	183
Требования к аппаратному и программному обеспечению ....	184

<b>6</b> Приложения .....	185
6.1. Глоссарий .....	186
6.2. Международный роуминг компании Swisscom Mobile .....	209
6.3. Требования к аппаратному и программному обеспечению .....	226
6.4. Библиография .....	226

---

## ПРЕДИСЛОВИЕ

За очень короткий промежуток времени сотовый телефон GSM стал товаром широкого потребления, доступным практически каждому. Отовсюду звучит реклама, предлагающая приобрести эти аппараты иногда совсем недорого.

Подавляющее большинство пользователей мобильных телефонов и не подозревают об удивительной сложности системы сотовой связи. Ведь перед ними чаще всего раскрывается лишь ничтожно малая часть всех ее возможностей. Однако, имея в своем распоряжении компьютер и устройство для считывания чип-карт, можно без особых сложностей заняться исследованием телефонов, их SIM-карт, а также сетей связи различных операторов.

В данной книге рассматриваются вопросы, которые непременно встают перед пользователями, и над которыми им совсем не хочется ломать себе голову. Кроме того, в ней раскрывается множество различных манипуляций, которые операторы и поставщики сознательно «забывают» осветить в сопроводительной технической документации.

Таким образом, эта книга будет полезна многим, как радиолюбителям, так и пользователям сотовых телефонов, — тем, кто интересуется всевозможными техническими хитростями и оригинальными решениями.

## БЛАГОДАРНОСТИ

Автор выражает благодарность всем, кто оказал помощь при подготовке к изданию настоящей книги: компаниям Gemplus Card International, L'ETSI, Swisscom Mobile, ZeitControl, Towitoko, Advanced Card Systems, Crownhill Associates, Pipistrel, ELV Electronik, ELEA, а также организаторам замечательного салона CARTES.

И, конечно, «теплый привет» французским операторам, которые нашли возможность установить антенны в нескольких метрах от лаборатории автора.