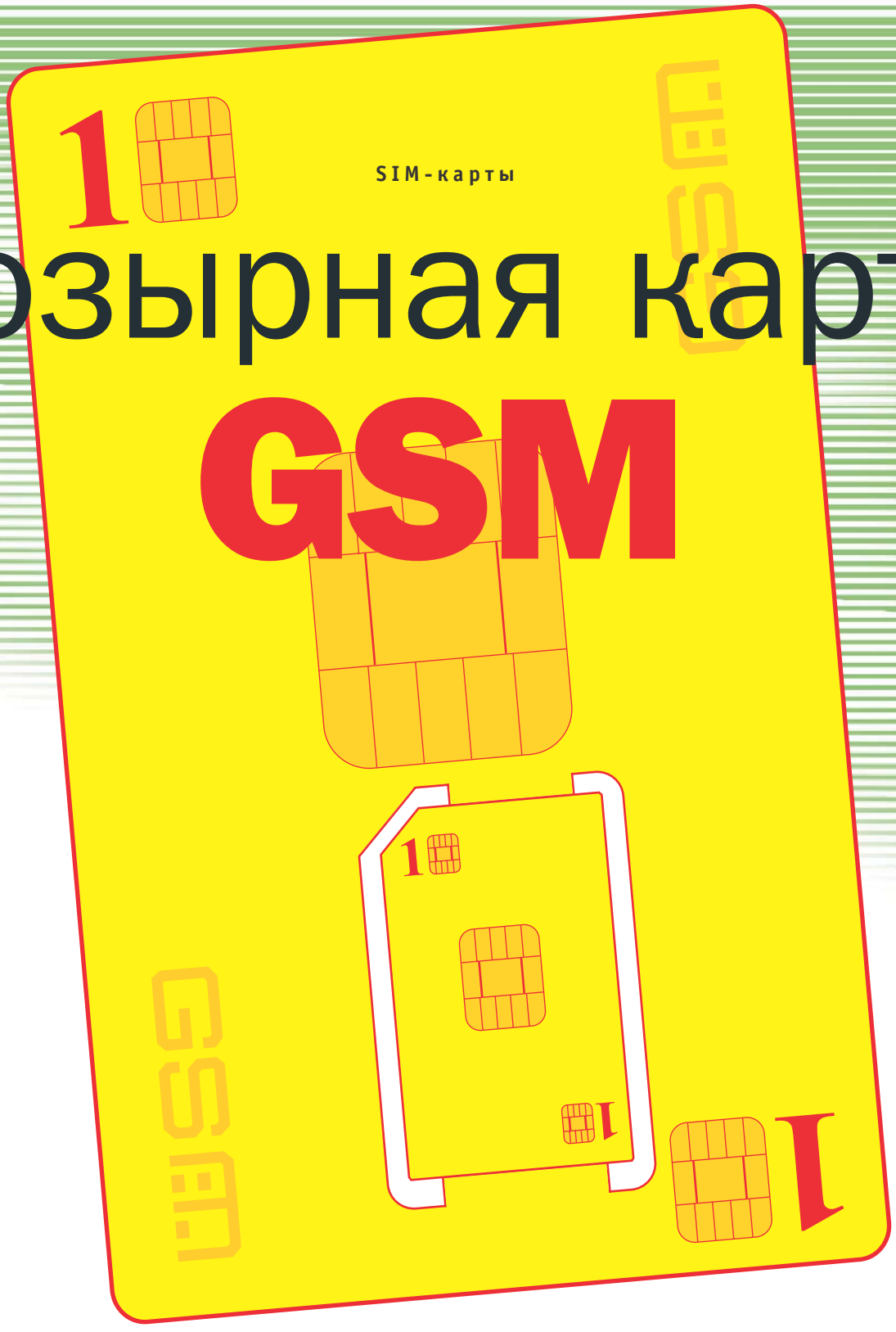
SIM-карты

Козырная карта GSM



Возьмите в салоне связи любой GSM-телефон и включите его. Все, что вы увидите, — это запрос на установку SIM-карты. И самое большее, что вы сможете сделать, — это позвонить по телефону экстренной помощи. Но стоит вставить SIM-карту, и безжизненный до этого гибрид пластика и кремния оживает, как будто обретая душу.

Разделяй и властвуй

Когда в конце 80-х — начале 90-х создавался новый европейский стандарт мобильной связи — GSM, то в него сразу были заложены требования по разделению терминала и модуля идентификации абонента. Именно так началась история SIM-карт.

Изначально в функции Subscriber Identity Module (именно так расшифровывается аббревиатура SIM) входили авторизация абонента в сотовой сети и хранение персональных данных. Использование отдельного модуля для идентификации абонента в сети стало абсолютно новой концепцией того времени. Ведь до появления GSM эти функции были возложены непосредственно на абонентский терминал. Недостаточная защищенность процедур идентификации в аналоговых телефонах зачастую приводила к появлению двойников и в этом смысле стандарт GSM с использованием SIM-карт и улучшенных процедур идентификации стал просто спасением для владельцев сотовых телефонов.

Вторая функция SIM, хранение персональных данных, оказала не менее важное влияние на развитие GSM. Во-первых, с точки зрения оператора объектом биллинга стала именно SIM-карта, а не телефон, что позволило ввести ряд дополнительных сервисов, например продажу предоплаченных контрактов. С таким подходом у абонентов появилась реальная возможность экономить свои средства в роуминге. Ведь достаточно купить в стране пребывания подобный предоплаченный контракт — и для совершения звонков уже совсем необязательно платить роуминговые отчисления своему оператору.

Во-вторых, такое разделение «души» и «тела» дает нам возможность совершенно спокойно подобрать себе телефон по вкусу и затем, вставив в него SIM-карту, оживить его. Это позволяет оторваться от зачастую скудного выбора телефонов у оператора и от его неразумной ценовой политики в отношении телефонов.

И, наконец, SIM-карта позволяет совершать звонки, даже если в вашем телефоне сядет батарейка, что происходит не так уж редко. Достаточно лишь попросить друга — «давай переставим «симки», — и можно позвонить, не опустошая счет своего знакомого. Точно так же можно ознакомиться и с новой моделью телефона, не покупая его. Всего лишь вставьте свою SIM-карту — и все функции телефона перед вами.

Итак, как же этот маленький кусочек пластика справляется со своими обязанностями?

Вещь в себе

По своей сути SIM-карта является разновидностью широко распространенных в мире смарткарт стандарта ISO 7816. Вы, без сомнения, уже встречались с подобными картами, когда звонили по таксофону. Размер этих карт также совпадает с размером обычных кредиток.

В связи со спецификой применения при создании стандарта GSM 11.11 разработчики внесли ряд изменений в оригинальные спецификации смарткарты, чтобы наилучшим образом приспособить ее к использованию в сотовых телефонах. Во-первых, изменения коснулись размера карты. Действительно, величина существенно влияла на размеры телефонного аппарата, поэтому уменьшение габаритов SIM до 25x15 мм было весьма целесообразным. Во-вторых, увеличилось давление на контакты карты — в пять раз по сравнению с ISO 7816, это положительно сказалось на надежности системы в целом. В-третьих, было уменьшено напряжение питания карты до 3 В. Подобное решение заложило перспективы миниатюризации телефонов благодаря использованию более компактных аккумуляторов.

Все свое ношу с собой

Теперь самое время более подробно поговорить о функциях, которые выполняет SIM-карта. Наиболее важная из них, как и отмечалось ранее, это, безусловно, идентификация абонента в сотовой сети. Каждая SIM-карта имеет свой IMSI (Interntational Mobile Subscriber Identity — международный идентификационный номер абонента). Этот номер является аналогом IMEI (International Mobile Equipment Identity — международный идентификационный номер мобильного терминала) у мобильного телефона, но никоим образом не зависит от него. В SIM-карте также хранится уникальный ключ »

Передача данных

К вопросу о безопасности

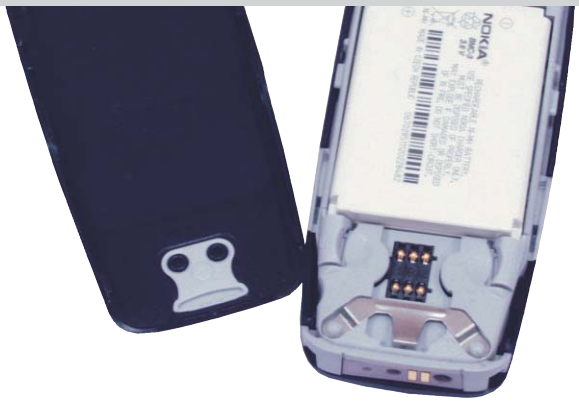
С развитием стандарта WAP и рождением WAP 1.2 появилось и новое средство защиты канала связи WAP и идентификации абонента. Таким средством стал WIM (WAP Identity Module). По сравнению с WAP 1.1, WAP 1.2, WIM обеспечивает защиту данных не только на участке терминал абонента — WAP-шлюз, но и на всем остальном пути, вплоть до получателя данных. Концепция WIM требует безопасного хранилища для данных и персонального кода, который используется при генерации ключей для установления защищенного канала связи и цифровых подписей.

В функции WIM входит поддержка WTLS (Wireless Transport Layer Security — защита беспроводного канала данных), который позволяет проводить авторизацию абонентов и защиту, и хранение данных при помощи криптографических алгоритмов и цифровой подписи, подтверждающей подлинность транзакций, что располагает к активному развитию мобильной коммерции.

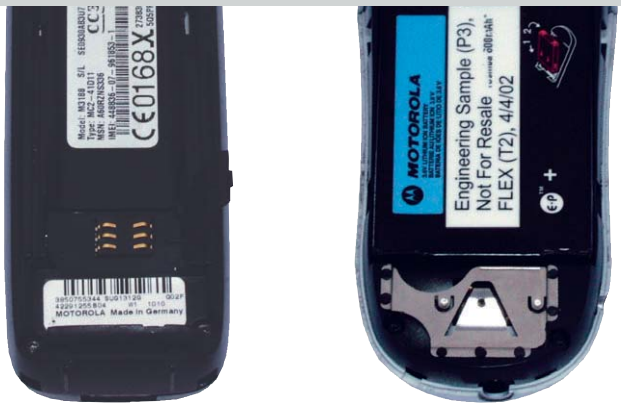
Естественно, эти данные должны храниться на SIM-карте мобильного телефона. Отдельные модели телефонов уже позволяют владельцу совершать защищенные транзакции и хранить в памяти телефона необходимые для этого данные.

Однако стоит владельцу поменять телефон, как все данные придется заносить туда по новой. Или, что тоже возможно, пользователь обратится к этому сервису и не будет идентифицирован, что может вызвать блокировку аккаунта, и придется все начинать сначала.

В свете повышенных требований к безопасности наилучшим вариантом практической реализации WIM является смарткарта. При этом весьма целесообразно объединение WIM и SIM, так как оно не снижает уровень безопасности, но существенно повышает комфорт использования WIM. Следует отметить, что на рынке уже появились SIM-карты с поддержкой WIM, что указывает на востребованность подобного продукта.



▲ В телефонах Nokia SIM-карту дополнительно прижимает задняя крышка телефона



▲ Эволюция способов фиксации карты: от специальной пластиковой крышки (модель M3788) до железной скобы (C300)

» авторизации Ki, который в паре с IMSI позволяет проводить идентификацию абонента. Стоит отметить, что IMSI, который позволяет однозначно идентифицировать пользователя, редко передается через радиоинтерфейс. Это происходит, например, на стадии активации SIM-карты. В остальное время используется временный IMSI — TIMSI (Temporary IMSI). Подобная мера защищает абонента от получения злоумышленником данных о сервисах, им используемых, от определения точного местоположения абонента и от сопоставления IMSI и конкретного радиосигнала.

В общем случае идентификация производится следующим образом: мобильный терминал получает случайное число, которое является аргументом функции, использующей ключ авторизации. Вычисления производятся при помощи криптографического процессора SIM-карты. Результат вычисления отправляется в авторизационный центр сотовой сети. В авторизационном центре производятся аналогичные вычисления, а результаты вычислений сравниваются. В случае, если результаты совпадают, доступ к сети разрешается. Подобная проверка может быть проведена авторизационным центром в любой момент времени.

Следующая, не менее важная функция SIM-карты — это хранение персональных данных абонента. Что для вас самое важное в телефоне? Конечно же, адресная книга, которая содержит все телефоны ваших родных, друзей и коллег. Разумеется, вы можете хранить эти данные и в памяти телефона, но если у вас модель начального уровня, то, скорее всего, для решения этой проблемы вам придется обратиться к ресурсам SIM-карты. Такой подход имеет свои преимущества и в случае с телефоном, который оснащен собственной памятью для адресной книги. Все дело в том, что в случае с хранением телефонов на SIM-карте их очень легко перенести на другой телефон — нужно всего лишь переставить карту.

Помимо хранения телефонов SIM-карта позволяет хранить и SMS-сообщения. Ситуация с сохранением SMS на SIM-карте полностью аналогична предыдущей. При этом стоит отметить, что единственный недостаток такого подхода заключается в том, что зачастую работа с памятью SIM-карты намного медленнее, чем с памятью телефона. Что ж, за удобство пока приходится расплачиваться производительностью.

Последняя важная функция персонализации — автоматический выбор языка меню. Не секрет, что при покупке язык меню телефона зачастую установлен на язык по умолчанию, которым редко является русский. Если вы не знаток иностранных языков, то автоматический выбор языка меню, который поможет сделать SIM-карта, будет для вас очень кстати. Для этого оператору достаточно создать на SIM-карте запись о необходимом языке, и он при наличии такового в телефоне будет выбран при установке SIM-карты. Безусловно удобная функция.

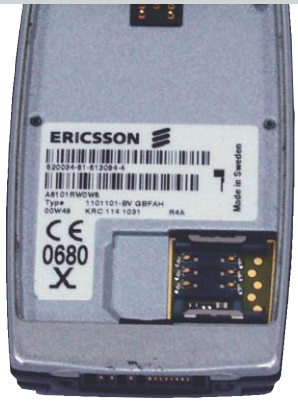
Все выше, и выше, и выше

Сама природа SIM-карты, которая позволяет однозначно идентифицировать абонента, располагает к разработке приложений мобильной коммерции, банковского обслуживания и предоставления различных информационных сервисов, в том числе и зависящих от местоположения абонента. В этом случае в качестве конечного устройства используется мобильный телефон абонента. При этом базовые функции могут выполняться при помощи звонков по определенным номерам и набора цифровых последовательностей, но это громоздкий и неудобный путь. Именно поэтому подобные сервисы получили свое развитие позже, когда GSM совершил новый эволюционный виток.

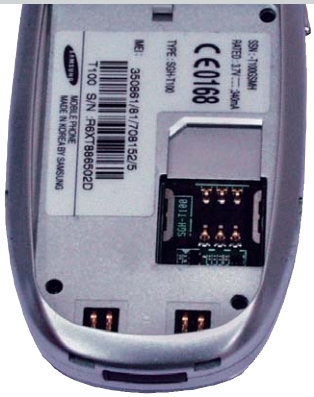
С разработкой стандарта GSM 11.14, известного также как GSM Phase II+, SIM-карты получили уникальные возможности, предоставляемые SIM Application Toolkit (STK). С началом эксплуатации STK SIM-карта ушла от роли пассивного хранилища данных пользователей и заняла активную позицию по отношению к телефону. Фактически STK превратил SIM-карту в главный компьютер, сделав для нее телефон ни чем иным, как клавиатурой с дисплеем.

Идея STK очень проста. Раз процессор SIM-карты способен выполнять программы, то почему бы этим не воспользоваться? Но без пользовательского интерфейса программа способна разве что манипулировать файлами на SIM-карте. GSM 11.14 предоставил программам на SIM-карте необходимый набор инструментов для организации пользовательского интерфейса.

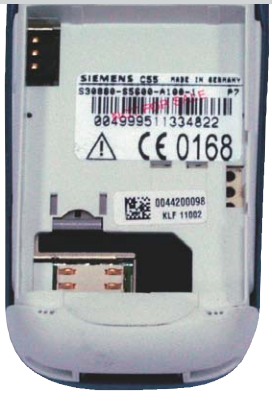
При помощи этих команд программа, написанная для SIM-карты, может создать дополнительное меню аппарата. Данные, получаемые при выборе пользователем того или иного пункта меню, могут быть отправлены для обработки на сервер, а результаты — отображены на дисплее телефона. Таким образом, возможно легко организовать различные сервисы по оплате товаров и услуг, а также разнообразные информационные и развлекательные сервисы. Необходимо сказать пару слов о специфике создания подобных сервисов. »



▲ В этом аппарате SIM-карта вдвигается и прижимается направляющими (T28)



▲ Аналогичное решение фиксации карты направляющими (T100)



▲ Малые размеры диктуют свои условия расположения и фиксации (C55)

» Дело в том, что загруженное в память SIM-карты STK-приложение не может быть модифицировано дистанционно. В связи с этим фактом оператору придется либо предусмотреть и реализовать все возможные функции сразу, либо модифицировать программу при посещении абонентом сервис-центра. Но есть и более универсальный метод. Оператор может хранить все сервисные меню на своем сервере, а на SIM-карту при этом записывается программа-браузер, содержащая в себе ссылки на разделы меню. При этом оператор может совершенно произвольным образом дополнять эти разделы — все изменения станут тут же доступны пользователю. Кстати, частный случай такого браузера — WAP-браузер, реализованный посредством STK. Подобное решение предполагалось использовать еще до широкого распространения телефонов с WAP. Правда, вследствие быстрого появления телефонов с поддержкой WAP, большой популярности WAP-браузер на SIM не нашел. Тем не менее реализация WAP-браузера вполне по плечу SIM-карте, и сейчас эта идея, похоже, переживает второе рождение с появлением разнообразных информационно-развлекательных сервисов на основе STK, развиваемых столичными операторами сотовой связи.

Дальнейшее развитие создание приложений для SIM-карт получает с появлением новых открытых стандартов программирования. К подобным стандартам относятся, например, MULTOS, разработанный консорциумом MAOSCO, и JavaCard, разработанный Sun Microsystems. Оба стандарта позволяют размещать на смарткартах вообще и на SIM-картах в частности сразу несколько различных приложений. Наиболее широкое распространение на данный момент получил JavaCard, поэтому остановимся подробнее на его преимуществах по сравнению с STK.

Нужно сразу же уточнить, что взаимодействие программ, написанных при помощи JavaCard, происходит при помощи стандартных инструментов STK, но это их единственная точка соприкосновения. Огромное преимущество JavaCard состоит в основной концепции Java — полной »

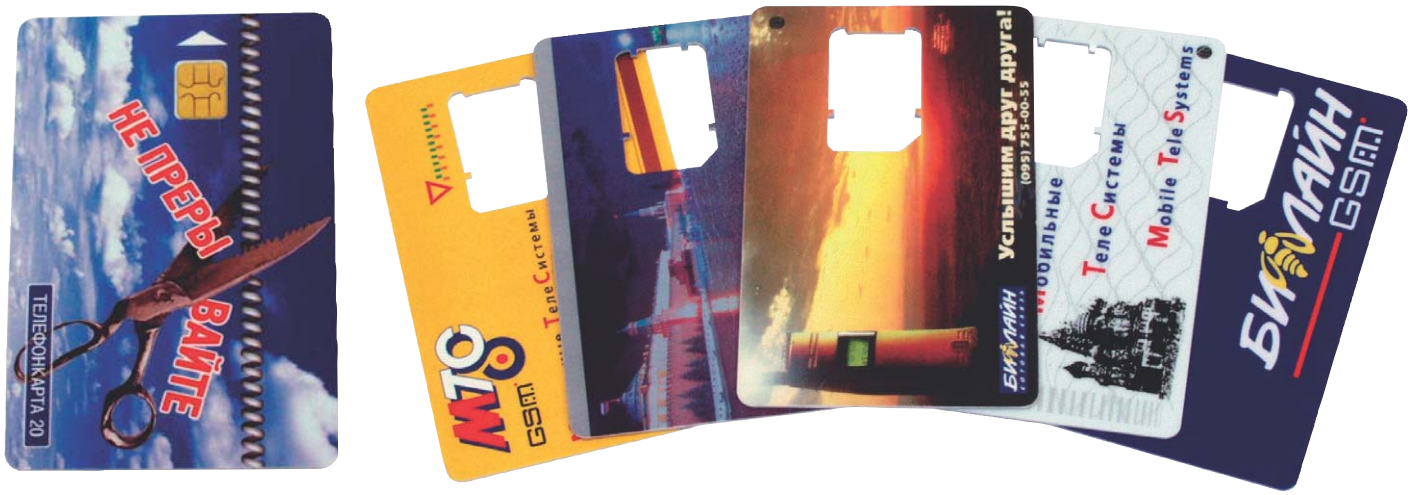
Внутреннее устройство

Пластиковый микрокомпьютер

SIM-карты относятся к разновидности микропроцессорных смарткарт. Это означает, что SIM-карта является миниатюрным компьютером. В состав SIM-карты входят собственно процессор, flash-память для хранения данных и приложений, оперативная память, а также криптографический сопроцессор. В широко распространенных сейчас SIM-картах используются 8- или 16-разрядные процессоры и от 16 до 64 Кбайт flash-памяти. Параметры, как видите, не самые современные, но для тех целей, для которых изначально предназначалась SIM-карта, вполне подходящие. Впрочем, на подходе уже более мощные, 32-разрядные процессоры.

Как и любой компьютер, SIM-карта использует свою собственную файловую систему для хранения разнообразных данных. За основу, разумеется, взята файловая система смарткарт ISO 7816. Эта файловая система довольно проста: имена файлов состоят из четырех байтов, каталоги имеют фиксированный размер. Всего для хранения данных существует несколько типов файлов. Тип Transparent представляет собой файлы с произвольным доступом к содержимому. Тип Linear fixed представляет собой записи фиксированной длины. Этот тип файлов может использоваться, например, для хранения телефонной книги или SMS. Тип Cyclic — практически полный аналог Linear fixed — содержит записи фиксированной длины, при этом последняя запись «замыкается» на первую. Подобные файлы могут использоваться для хранения различных списков звонков (принятых, совершенных, не отвеченных), а также для хранения списка последних набранных номеров. Хорошо продуманная система прав доступа к файлам позволяет сделать их доступными только для чтения или записи, доступными для чтения и записи после ввода PIN (персонального идентификационного кода) или вообще запретить доступ к файлам извне. При этом однажды введенный PIN действует на протяжении всей сессии, обычно до выключения питания. Подобные меры защиты файлов обеспечивают весьма высокий уровень безопасности данных, которые хранятся на SIM-картах.

Смарткарты и SIM-карты соответственно допускают создание для них программ. В общем случае создание программы для SIM-карты не представляет собой ничего необычного. Разумеется, это верно, если вы знакомы с ассемблером. Впрочем, в последнее время ситуация изменилась и появились более эффективные способы программирования SIM-карт.



▲ Слева: SIM-карта для таксофона. Справа: после извлечения SIM-карты у пользователя остается красивая безделушка

» переносимости кода между различными платформами. Это обеспечивается благодаря тому, что SIM-карта оснащается собственной виртуальной Java-машиной и набором Java API, которые позволяют выполнять код программы. Разработка стандарта велась Sun Microsystems в тесном сотрудничестве с ведущими производителями смарткарт, такими как Gemplus, Oberthur, Schlumberger. Таким образом, приложение, написанное для SIM-карты одного производителя, будет работать и на любой другой — при условии поддержки этими картами стандарта JavaCard. Добавьте к этому более двух миллионов программистов во всем мире, работающих с Java, — и вы в полной мере оцените потенциал этой технологии. Простота создания приложений и их полная переносимость — одни из важнейших преимуществ JavaCard по сравнению с STK. Возможность загрузки новых приложений (так называемых апплетов) по радиоинтерфейсу — еще одно их достоинство. Это позволяет оператору изменять набор сервисов, доступных абоненту, и обновлять программные модули.

Будущее за умными SIM

По мере своего развития SIM-карты приобретают новые функции, становятся умнее и самостоятельнее. Благодаря уникальной возможности однозначно идентифицировать абонента SIM-карты располагают к созданию разнообразных дополнительных услуг. Эти услуги — информационно-развлекательные сервисы, мобильная коммерция и банковское обслуживание — способны принести значительную прибыль операторам сотовой связи. Именно поэтому можно не сомневаться, что они будут получать все большее развитие в свете снижения стоимости услуг голосовой связи.

Сама идея SIM-карты как отделяемого модуля идентификации и хранения персональных данных оказалась настолько успешной, что и другие стандарты начинают использовать SIM. Например, уже разработаны SIM-карты для стандарта CDMA. Но наиболее важно то, что SIM-карты останутся и в терминалах третьего поколения. Вместе с SIM-картами в третье поколение сотовой связи шагнут и все используемые ими технологии — и STK, и JavaCard, и WIM.

Технологии не стоят на месте, и SIM-карты, несомненно, получат более мощные процессоры и более значительные объемы памяти. Это означает, что в будущем нас ожидают новые возможности применения SIM-карт, которые позволят целиком и полностью настроить телефон под себя, сделав его универсальным устройством, верным спутником в делах и на отдыхе.

■ ■ ■ **Сергей Чернов**

Основные команды, поддерживемые SIM-картой

Команда	Описание
Display Text	Отображение текста на дисплее телефона
Get Inkey	Получение кода нажатой клавиши
Get Input	Получение строки
More Time	SIM-карте требуется дополнительное время на обработку данных
Play Tone	Воспроизвести сигнал
Poll Interval	Установка интервала опроса SIM-карты
Reset	Сброс SIM-карты
Setup Menu	Построение дополнительного меню в телефоне
Select Item	Выбор пункта меню
Send Short message	Отправка короткого сообщения без участия пользователя
Send SS	Отправка сообщения SS (Supplementary Services)
Setup Call	Совершение звонка
Polling Off	Прекращение опроса SIM
SMS PP	Получение SMS. SMS загружается без уведомления пользователя
Cell Broadcast download	Получение CB-сообщения. Загружается без уведомления пользователя