

# В тесном кругу NFC

А. ГОЛЫШКО, канд. техн. наук, г. Москва

*"Эксплуатация оборудования должна доставлять не удовольствие, а бизнес-эффект".*

(из пособия по оптимизации бизнеса)

## Технология

Технология связи в ближнем поле — NFC (Near Field Communication) — входящая "звезда" инфокоммуникационного рынка. Она базируется практически на тех же технологиях, которые используются в радиочастотных метках и бесконтактных смарт-картах. С точки зрения пользователя, NFC невероятно гибка: достаточно двум устройствам фактически соприкоснуться, чтобы между ними образовалась связь, не требующая ни мучительной процедуры инициации соединения, ни ввода паролей. NFC организуется не только между двумя аппаратами, оснащёнными соответствующими NFC-модулями, но и, к примеру, между телефоном и стикером, содержащим, по аналогии со штрихкодом, информацию вроде адреса web-страницы или контактных сведений.

"Родители" NFC — компании **Philips** и **Sony**. Технология впервые продемонстрирована в 2002 г. NFC была одобрена как стандарт ISO/IEC (18092) 8 декабря 2003 г., а позже как стандарты ECMA и ETSI. С 2004 г. развитием NFC занимается некоммерческая организация **NFC Forum**, основанная компаниями **Sony**, **Philips** и **Nokia**. Компания **Nokia** выпустила свой первый телефон с NFC-интерфейсом в 2005 г.

Статус спонсоров **NFC Forum** имеют производитель микрoeлектроники **NXP Semiconductors**, а также владельцы известных платёжных систем **American Express**, **MasterCard Worldwide** и **Visa Int.** В январе 2004 г. **Visa Int.** совместно с **Philips** впервые продемонстрировала работу платёжных приложений на выставке Consumer Electronics Show в Лас-Вегасе. Участниками **NFC Forum** ныне являются практически все крупные операторы и поставщики оборудования связи. В числе ассоциированных участников — крупнейшей мировой производитель смарт-карт **Gemalto** и ряд других.

NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092. Эти стандарты определяют параметры модуляции, кодирования, скорости передачи и радиочастотную структуру интерфейса устройств NFC, а также схемы инициализации и условия, требуемые для контроля за конфликтными ситуациями (коллизиями) во время инициализации — и для пассивных, и для

активных режимов NFC. Кроме того, они также определяют протокол передачи, включая протокол активации и способ обмена данными. NFC объединяет множество ранее существовавших стандартов, включая ISO 14443, ISO 15693. Таким образом, телефоны, снабжённые NFC, способны к взаимодействию с уже созданной ранее инфраструктурой считывателей.

Изначально NFC разрабатывалась для бесконтактной оплаты товаров и услуг с помощью мобильного телефона, как беспроводный интерфейс "длинной" в десяток сантиметров к электронному кошельку, с которого при покупке автоматически списывается определённая сумма. Но в итоге сфера её применения оказалась гораздо шире. В частности, NFC используется для считывания радиометок — при приближении модуля NFC к специальной радиометке (RFID) на объекте на экране телефона появится информация об этом объекте, например, цена, состав, срок годности и прочее. А ещё с помощью NFC возможно получение разнообразных платных и бесплатных справочно-информационных услуг или информации от различных систем мониторинга и т. п. То есть модуль NFC может использоваться просто как малагобаритный приёмопередатчик сверхмалого радиуса действия, который может, к примеру, передавать информацию с одного устройства на другое, если их поднести друг к другу.

Следует отметить, что последний вариант имеет множество аналогов в лице различных радиointерфейсов — от Bluetooth до WHDI (Wireless Home Digital Interface), разработчики которых боролись за качество, дальность и скорость передачи информации (вплоть до HD-видео). Каждый из них в чём-нибудь превосходит NFC, но основные преимущества NFC заключаются в сочетании простоты и дешевизны. По сравнению с другими бесконтактными технологиями, такими как Bluetooth, IrDa, Wi-Fi и т. п., NFC-технология характеризуется быстрой установлением канала связи (менее 0,1 с), малой энергоёмкостью и относительно высокой скоростью передачи данных. Да и аппаратная реализация NFC-интерфейса оказывается значительно дешевле.

В NFC используются те же методы организации радиоканала, что и в бесконтактных пассивных картах ближнего радиуса действия (до 10 см), вклю-

чая диапазон радиочастот, используемый в промышленности и медицине: несущая — 13,56 МГц (диапазон ISM — Industrial, Scientific and Medical radio Bands, промышленные, научные и медицинские частоты) с полосой пропускания 2 МГц. Технология базируется на явлении взаимной индукции, которая лежит в основе работы трансформатора. Если два устройства с чипами NFC поместить рядом, то их антенны в виде миниатюрных катушек индуктивности (рамочных антенн) образуют высокочастотный трансформатор. При этом с одного устройства на другое начнёт передаваться закодированная информация со скоростью 106, 212 или 424 кбит/с. Рабочее расстояние с компактными стандартными антеннами — до 20 см. На этом предельном расстоянии скорости передачи может уменьшиться вдвое или вчетверо, но, собственно, большей дальности и не требуется. Зачем мешать соседям заниматься тем же самым?

Технология NFC подразумевает два режима работы оборудованных ею устройств: пассивный и активный. В первом случае с "молчащего" объекта (он выступает в роли ретранслятора) информация считывается с помощью электромагнитного поля, создаваемого другим объектом, являющимся инициатором сеанса связи. При активном режиме оба объекта обмениваются информацией, попеременно создавая электромагнитное поле и выступая в роли ретрансляторов.

Существуют три коммуникационных режима для NFC-устройств:

- режим Peer-to-Peer (P2P) определён для коммуникаций устройство-устройство, когда два "электронных собеседника" обмениваются разнообразной информацией;
- режим чтения/записи позволяет приложениям обмениваться NFC-сообщениями (не является безопасным) — устройство ведёт себя как обычная бесконтактная карта;
- режим эмуляции NFC-карты позволяет мобильному телефону с NFC работать в качестве стандартной смарт-карты.

При организации передачи данных в NFC используется адаптивное кодирование. При хороших условиях приёма (424 кбит/с, 212 кбит/с) используется Manchester coding с коэффициентом модуляции 10 %, а в противном случае (на предельном расстоянии) — модифицированное Miller coding со 100 %-ной модуляцией, обеспечивающее 106 кбит/с. С целью повышения достоверности передачи информации устройства NFC могут получать подтверждение о сигнале, принятом на стороне "собеседника".

Функционально NFC позволяет организовать радиоканал для передачи данных на малые расстояния между различными типами электронных устройств, как обладающими функциями считывателя бесконтактной карты и непосредственно карты, так и имеющими возможность связываться друг с другом в качестве равноправных узлов. Таким образом, NFC может также работать, когда одно из устройств не

снабжено источником питания, и это может быть, к примеру, не просто бесконтактная кредитная смарт-карта, но и выключенный (!) мобильный телефон. Кроме того, используя NFC, можно устанавливать связь и с помощью других протоколов связи, например, Bluetooth и Wi-Fi, а также дистанционно осуществлять настройку различных электронных устройств. Например, для того чтобы связать по Bluetooth два смартфона с поддержкой NFC, можно просто поместить их достаточно близко друг к другу, чтобы сработало соответствующее подключение. Другими словами, инициирование подключения NFC используется в качестве события для запуска процесса автоматического связывания устройств по Bluetooth и передачи информации, избавляя пользователей от лишней манипуляций.

### Конструкция

Встроить NFC-чип в какое-либо устройство можно разными способами. В частности, носителем чипа и передающей антенны может выступать сам аппарат, как это сделано в смартфонах Google Nexus S и Nokia C7. Можно поместить чип в сим-карту мобильного оператора, что позволит оплачивать товары и услуги не только с банковского, но и мобильного счёта. В этом случае при необходимости очень просто заблокировать услугу — достаточно позвонить оператору. Подобным образом технология реализована в смартфоне Nokia 6216. Третий способ — встраивание NFC-чипа в карту памяти, который предложила компания **Tyfone**, — сегодня практически любой телефон имеет слот microSD. В целом все крупные производители стремятся оснастить технологией NFC свои самые лучшие high-end смартфоны. Однако появились и другие тенденции — компания **Huawei** встроила NFC в Android-смартфон HuaweiSonic ценой всего 150 евро.

### Прогнозы

Крупнейшие мировые операторы, включая **America Movil, Axiata Group Berhad, Bharti, China Unicom, Deutsche Telekom, KT Corporation, MTS, Orange, Qtel Group, Softbank Mobile, Telecom Italia, Telefonica, Telekom Austria Group, Telenor и Vodafone**, заявили о своей поддержке технологии NFC. Кроме того, они анонсировали планы по введению коммерческих услуг на основе этой технологии в ряде стран к концу 2012 г.

Согласно исследованиям **Gartner**, из года в год количество платежей, совершаемых с помощью мобильных телефонов, будет расти с большой скоростью. В прошлом году их объём составил 32 млрд долл., а к 2014 г. ожидается уже 245 млрд. Ожидается также, что до конца текущего года на рынок поступит 35 млн телефонов с поддержкой NFC, а в 2012 г. их станет в два раза больше. По прогнозам **Juniper Research**, благодаря NFC к 2014 г. каждый пятый смартфон будет одновременно и электронным кошельком. Новая технология получит

максимальную поддержку в США, Франции и Великобритании и только потом начнёт покорение остальных стран мира. В общем и целом, к 2014 г. в мире будет более 300 млн смартфонов, поддерживающих NFC. Более половины из них — в странах Северной Америки.

### Защита

Считается, что NFC обеспечивает максимально удобный способ обмена информацией в режиме "точка—точка" и реализует это максимально безопасным образом. Но там, где проходят платежи, всегда наблюдаются повышенная концентрация криминального элемента. Идеальная ситуация для "беспроводного" преступника, когда "клиент" просто прошёл мимо него и лишился всего содержимого электронного кошелька (прямо как в рекламе — "мы сидим, а денюжка идет"). Несмотря на то что малая дальность действия NFC-устройств сама по себе является неплохой защитой, на каждый радиосигнал найдётся сверхчувствительная антенна. Однако и в этом случае эффективность "атаки" не превышает нескольких метров, а используемые в NFC режимы работы дополнительно её затрудняют.

Впрочем, разработчики стандарта NFC и не ставили задачу создания защиты от подслушивания. Поэтому стек протоколов должен использовать криптоалгоритмы поверх NFC для защиты данных, чем и должны быть озабочены поставщики платёжных услуг. В частности, в начале 2011 г. **NXP Semiconductors** и **Giesecke & Devrient (G&D)** разработали ПО для формирования защищённых интерфейсов между мобильными устройствами на платформе Android и других операционных систем. Новое решение объединяет NFC-контроллеры NXP для мобильных устройств, программную систему безопасности и функции выполнения защищённых транзакций от **G&D**. Программные функции безопасности действуют во всех режимах связи, предусмотренных технологией NFC, — чтение и запись NFC-радиометок, обмен данными в пиринговом режиме, оплата услуг с помощью мобильного телефона, контроль доступа. Исходные программные коды открыты для разработчиков, что обеспечивает гибкость при интеграции функций в различные платформы от разных производителей. Последняя возможность особо важна, поскольку любая платёжная система должна обеспечивать массовость.

В свою очередь, производитель чипов **Infineon** выпустил интегральную схему SLE 97144SE модуля защиты, предназначенную для встраивания в мобильные телефоны с поддержкой NFC. В ней использована технология компании **Integrity Guard** для обеспечения обработки конфиденциальных данных с самым высоким уровнем защиты. Все данные хранятся в зашифрованном виде и остаются таковыми для обработки на всём пути прохождения (процессоры, память, кэш и шины). Встроенный микроконтроллер безопас-

ности модуля защиты состоит из двух центральных процессоров и сложной системы обнаружения ошибок.

Разумеется, существующие методы радиоэлектронной борьбы позволяют осуществить разрушение данных, передаваемых NFC-устройствами, с помощью так называемых "глушилок RFID". Однако и украсть при этом ничего нельзя. Модифицировать данные в NFC затруднительно, поскольку NFC-приёмник весьма чувствителен к смене амплитуды и фазы наведённого сигнала.

Для атаки с использованием ретрансляции (relay attack), которую часто используют автоугонщики, злоумышленник должен отправить жертве запрос считывателя и её ответ в режиме реального времени передать дальше на считывающее устройство. Это делается для того, чтобы выполнить задачу, симулирующую владение смарт-картой жертвы. На практике это трудно реализовать из-за весьма жёстких требований к временному интервалу (а это микросекунды), в течение которого должен поступить ответ от "соседа" или при выполнении обязательной процедуры антиколлизии.

Представители компании **Google** утверждают, что платёжная система на базе NFC в мобильных аппаратах будет безопаснее, чем кредитная карта, так как обеспечиваемая аутентификация будет более высокоуровневая. В этом случае, взамен импринтинга вашего счета на слабо защищённую карту, устройства с NFC будут хранить ваши данные в защищённом пароле зашифрованном состоянии в самом телефоне.

### Проблемы

Идеальных технических решений не бывает. Первая проблема NFC — энергозависимость. Даже находясь в неактивном режиме работы, чип всё равно использует энергию для поддержания работоспособного состояния. Привязка к мобильному устройству в случае разрядки его аккумулятора может сыграть злую шутку — не будет возможности оплатить запланированную покупку или услугу.

Вторая проблема — все дополнительные функции для защиты информации должны быть понятны, активированы во многих устройствах, а ещё лучше — стандартизованы.

Третья проблема — необходимость подготовительных действий, порой очень сложных в реализации. Чтобы бабушка смогла позвонить в скорую простым прикладыванием телефона с NFC к соответствующему чипу, необходимо предварительно разместить этот чип у неё дома, а также настроить его по всем правилам. В магазине кто-то должен на каждый товар нанести метки с необходимой информацией и настроить их корректную работу. Если смарт-карт будет установлено несколько (а это тоже вероятная ситуация), их нужно будет каждый раз выбирать через интерфейс телефона.

Четвёртая проблема — а что, если смартфон потерян или украден? Надо

придумать, как его быстро заблокировать.

Пятая проблема — проблема абонентской конкуренции. К примеру, трудно сомневаться, что афиша, снабжённая NFC и призывающая заказать билет "тут и сейчас", будет вывешена в людном месте. Вы, было, протянули к ней смартфон, но таких желающих может быть много. Все их смартфоны будут находиться в непосредственной близости от NFC-чипа, и с каждым он будет обмениваться информацией. Как бы не перепутать.

## Что ещё бывает

С помощью NFC можно быстро собрать необходимые статистические данные, обменяться виртуальными визитками с деловым партнёром, передать сохранённый маршрут с одного навигатора на другой. С помощью NFC легко учитывать рабочее время персонала, и развитие в технологическом плане страны — США, Япония, Тайвань — уже давно взяли это на вооружение. Например, в США NFC активно используют для предоставления скидочных купонов для постоянных покупателей магазинов и торговых центров. Мобильные операторы Америки всерьёз хотят работать с NFC, и ведущие операторы **AT&T**, **Verizon Wireless** и **T-Mobile** заявили, что собираются создать под брендом **Isis** совместную сеть бесконтактных платежей (заменяющую кредитные карты), основанную на NFC-технологии. Ведь сколько бы смартфонов не имело бы эту технологию, она бесполезна, если не будет поддерживаться магазинами. Если не будет возможности расплачиваться по этой системе в различных местах, то вряд ли технологию ожидает перспективное будущее. NFC будет использоваться не только в торговле, но и появится возможность загружать разнообразную информацию с установленных в городе датчиков. Этот же принцип действия можно применять для поддержания связи между клиентами и магазинами. Ожидается, что к концу 2012 г. каждый третий американский магазин будет оснащён терминалом с NFC. Кстати, инициаторам **Isis** пришлось идти на поклон к **Visa** и **MasterCard**, международным провайдерам платёжных систем, с тем, чтобы совместно разработать "менее честолюбивую" систему, альтернативную, а не заменяющую кредитные карты. Подобный результат способен оказаться менее интересным и прибыльным для операторов, но удобным для конечных потребителей.

Вполне логичная сфера использования NFC — совершение покупок людьми с ограниченными физическими возможностями. Если сделать в квартире несколько меток и запрограммировать их на определённые действия, пожилому человеку будет просто и удобно заказывать продукты на дом, совершать звонки родным и по экстренным номерам телефонов. А можно быстро выбрать компакт-диск с кино или музыкой на стенде в магазине или в собственной домашней коллекции. Для

всего этого нужно будет просто приблизить телефон с NFC к соответствующему чипу.

Недавно компания **Google** оформила патент на свою систему платежей, которая превратит **Google** в своего рода "независимого брокера". Последний получает информацию о заказах, оформляемых пользователями посредством NFC, и обрабатывает такие заказы, предоставляя варианты доставки, другие опции и общую сумму заказа клиенту. Кроме того, **Google** будет собирать платежи, информацию по вариантам доставки, выбранной пользователем, и отправлять все эти данные продавцу для завершения транзакции. Таким образом, компания-продавец получает ещё один удобный способ распространения своих товаров и услуг с централизованной системой оплаты.

Летом 2011 г. компания "**МегаФон**" намеревалась запустить в коммерческую эксплуатацию услугу оплаты проезда в петербургском метрополитене с помощью мобильного телефона по технологии NFC. **МТС** и "**МегаФон**" также заинтересованы в реализации аналогичного проекта в московском метрополитене. **МТС** ещё в прошлом году представила совместный с московским метрополитеном проект на основе NFC, и теперь от метрополитена требуется решение ряда технологических вопросов. "**МегаФон**" в сотрудничестве с администрацией Петербурга планирует реализовать оплату проезда с помощью мобильного телефона на всех видах городского транспорта. **МТС** с проектом "Мобильный билет" собирается выходить в регионы. Группа компаний "**ВымпелКом**" совместно с Петербургским метрополитеном и **ООО "Амбик Тэк СПб"** также запустили аналогичный проект. Пассажирам достаточно установить под крышку используемого ими мобильного телефона специальный NFC-модуль, после чего телефон обретает функции платёжного устройства и проездного билета.

В Великобритании начала работать мобильная платёжная система **Quick Tap**, совместный проект сотового оператора **Orange** и компании **Barclaycard** — подразделения банка **Barclays**, выдающего кредитные карты. С 20 мая в нескольких британских торговых сетях, в том числе закусочных быстрого питания **McDonald's**, кофейнях **EAT** и **Pret-a-Manger**, а также в некоторых аптеках **Boots** появились устройства, к которым для оплаты товаров достаточно поднести смартфон. Правда, подойдёт не любой смартфон, а только **Samsung Tocco Lite**, а стоимость покупок, оплаченных таким образом, не может превышать 15 фунтов (около 24 долл.).

В 2009 г. компания-оператор **O2** протестировала в лондонском метро возможность оплаты проезда и покупок с помощью мобильных телефонов, а к Олимпийским играм 2012 г. сразу несколько операторов намерены значительно расширить возможности бесконтактных платежей, однако, как отмечают многие эксперты, и в 2012 г.

покупателям в Лондоне всё равно придётся искать магазины, поддерживающие платежи с помощью мобильных. Основной проблемой внедрения систем бесконтактных платежей называют наличие нескольких не связанных между собой стандартов оплаты, а также отсутствие у продавцов новых терминалов.

**Samsung** и **Visa** подписали соглашение о том, что к Олимпийским играм в Лондоне они выпустят смартфон, поддерживающий мобильные платежи через NFC и внешне напоминающий **Galaxy S**. Согласно описанию проекта, среди олимпийских объектов будет установлено 60 тыс. терминалов с приёмом NFC-платежей.

Найденный в Бюро по регистрации патентов и торговых марок США документ возродил слухи о синхронизации компьютеров **Mac** и **iPhone** компании **Apple** с помощью NFC. Внедрение технологии NFC в компьютеры позволит использовать их на торговых точках в качестве платёжных терминалов, к примеру, терминалы **PayPass** от **MasterCard** для системы **Google Wallet**. Такое же оборудование может быть использовано для чтения смарт-карт. Согласно другим слухам, технология NFC будет-таки присутствовать в будущем смартфоне **iPhone 5**, причём она будет применяться не только для беспроводной оплаты счетов с помощью телефона, но и для совместной работы с компьютером, куда станут попадать некоторые данные из профиля пользователя. Там же смогут появляться приложения, которые пользователь купил в **Mac App Store** (сетевом магазине **Apple**), — сначала это будут просто "иконки", которые позже могут быть скачаны и активизированы. Можно будет перемещать и редактировать документы там, где вы ни находились — достаточно лишь поднести ваш **iPhone** к любому компьютеру **Apple**. Но как только NFC-соединение разрывается, ваши приложения, документы и другие файлы удаляются с гостевого компьютера, возвращая его к тому виду, в котором он был до вашего "вмешательства". Правда, пока ничего ещё нельзя утверждать со 100 %-ной вероятностью.

А пока NFC-поддержка появилась в **OS Android 2.3 Gingerbread**, но **Google** хочет расширить её применимость, и для этого придумана инициатива под названием "взаимодействие без кликов" (**0-click**). Это позволит владельцам **Android**-телефонов устанавливать прямые и мгновенные подключения к устройствам друг друга для таких операций, как обмен контактами, web-страницами, **YouTube**-видео — любым контентом без необходимости в установке отдельного приложения. **Sticky Notes** — приложение, предназначенное для передачи пользователям посланий друг другу через касания телефонами. **Google Talk Portal**, другой пример NFC-использования, при прикосновении открывает видеочат со случайным человеком.

Отныне эффективный гражданин — это человек со "связями" в новом смысле этого слова. А NFC-чип ему можно просто вживить — пусть общается. ■