



О Ч Е Н Ь

У М Н Ы Й

Т Е Р М И Н А Л

Екатерина Оганесян



**Терминал** – устройство, в котором клавиатура и дисплей используются для передачи и получения данных посредством коммуникационных связей. Отличается от микрокомпьютера тем, что сам по себе работать не может.

**Глупый терминал** – устройство, предназначенное только для ввода в компьютер и вывода из него.

**Умный терминал** – терминал, обладающий памятью, командами для редактирования, графикой и т. д., в отличие от глупого терминала.

(собрано с просторов Интернета)

Сразу оговорюсь: *очень умный терминал* – устройство, которого еще нет. То, что есть на сегодняшний день, “очень умным терминалом” назвать нельзя, максимум просто “умным” (см. определения выше). Но он появится, потому что необходимость в нем ощущается уже сейчас. Я не знаю, каким именно он будет, ведь в сфере технологий все меняется слишком быстро. Могли ли вы предположить в году эдак восьмидесятом, что мобильники так распространятся и будут оснащены такими сопутствующими функциями? А ведь сейчас даже в простеньких мобильных телефонах стоят карты памяти, емкость которых в разы, а то и на порядки превышает объем ПЗУ тогдашних компьютеров, причем даже тех, что считались на редкость навороченными для своего времени! Зато я могу предположить, какие функции смогут выполнять очень умные терминалы, для чего они будут служить и какими характеристиками будут обладать. Давайте сначала разберемся, какие устройства можно назвать терминальными, даже если с некоторой натяжкой. Телефон – это терминал? Да. И стационарный, и мобильный. Они будут соответствовать первому определению, если его расширить за пределы компьютерной сферы и распространить на все области, в которых так или иначе передается информация. Собственно, чем речевая информация хуже данных? Если же вспомнить об IP-телефонах и мобильных смартфонах, то тем более принципиальной разницы нет. Да и в аналоговых телефонах теперь дисковый номеронабиратель ушел в прошлое, кнопки по праву можно назвать клавиатурой, и многие модели действительно оснащены дисплеем. Лет десять-двенадцать назад, если кто не жалует на память, был самый расцвет пейджеров. Можно ли их называть терминалами? Да, с тем лишь ограничением, что они были устройствами односторонней связи; их удел – только прием, а не пе-

редача информации. Но затем появились твейджеры – слово образовано от названия Two Way pager, двусторонний пейджер – и их можно называть терминалами без всяких ограничений. Им не суждено было получить широкое распространение, потому что их нишу моментально заняли мобильные телефоны – голосовая мобильная связь и сами аппараты подешевели, перестало быть обязательным официальное разрешение на радиотелефон, а затем стали чрезвычайно популярными сообщения SMS, что совершенно эквивалентно работе твейджера. Сейчас к списку терминалов можно смело добавить всевозможные наладонники и коммуникаторы – срастание компьютерных технологий и телефонии идет полным ходом. Разумеется, КПК, ноутбуки, лаптопы, стационарные компьютеры и прочую технику тоже можно относить к терминалам, причем вполне умным. Но все они имеют те или иные ограничения: по размеру, весу, зоне приема, набору функций... Список функций постепенно расширяется. К ставшим привычными SMS-кам добавились MMS-ки, появился мобильный интернет, часть аппаратов оснащена клиентами электронной почты, многие способны служить модемами для беспроводного подключения ноутбуков к сети. Коммуникаторы и мобильники с e-mail-клиентами позволяют принимать и отправлять электронную почту, а более продвинутые модели оснащены набором приложений, вроде упрощенного текстового редактора, электронных таблиц, мультимедиа проигрывателя и т.п., не говоря уж о калькуляторах, календарях, записных книжках и игрушках. В некоторых странах с помощью мобильного телефона уже платят за проезд в наземном общественном транспорте, отправляя сообщение за определенную цену на определенный номер и получая в ответ “билет” прямо на мобильный телефон (интересно, кстати, как восприняли эту новинку контролеры в общественном транспорте?). Но все это лишь часть того, что потенциально способны выполнять терминалы, даже ноутбуки. Во-первых, не везде вы сможете взять ноутбук с собой: он большой и тяжелый, даже так называемые “супертонкие” модели. Он потребляет много энергии, и даже если вы не хотите остаться с севшей батареей после нескольких часов работы, большой аккумулятор или дизель-генератор вы с собой потащите вряд ли. Значит, вы привязаны к сети электропитания. Выход в интернет – проводной ли, беспроводной ли, через локальную сеть, через модем – есть не везде, значит, вы привязаны и к этому ресурсу. Добавьте сюда еще требование к пропускной способности канала связи и надежности со-

единения с провайдерским узлом. В общем, даже такой умный терминал требует доработки. Будет вполне логично, когда либо все функции будут объединены в одном устройстве, которое можно постоянно носить с собой, либо повсеместно будут установлены терминалы доступа к той или иной услуге, а с собой вы будете иметь лишь средство идентификации, дающее вам право воспользоваться терминалом.

Уже сейчас в воздухе носится идея отказаться от так называемых персональных компьютеров в пользу терминальных устройств, а местами уже предприняты попытки внедрения. Раньше, еще до появления персоналок, все работали на терминалах, которые были подключены к главной машине. Новое – хорошо забытое старое, и теперь на полном серьезе звучат предложения не держать пользовательские приложения и высокопроизводительные процессорные “мозги” у самого пользователя, а свести их в единые центры, к которым пользователи будут обращаться с помощью относительно простых терминальных устройств. Пример конкретной реализации такого подхода – тонкие клиенты. Эта технология предусматривает размещение системного программного обеспечения, всех пользовательских приложений и всех данных на центральном сервере. На рабочих местах стоят не персоналки, а Windows-терминалы (умные, но, в соответствии с нашей градацией, не очень). С их помощью пользователи получают доступ к ресурсам сервера, при этом картинка на экране практически не отличается от привычной нам по среде Windows, установленной на персональном компьютере. Основное отличие тонких клиентов от клиент-серверной архитектуры, ставшей сейчас классической, состоит в том, что при технологии тонкого клиента прикладные программы и данные на рабочем месте пользователя не хранятся вообще. В случае клиент-серверной архитектуры многие приложения и данные хранятся на персональных компьютерах, поэтому

операционная система должна обладать полной функциональностью, а запоминающие устройства – порядочной вместимостью. Отсюда и пошло название “толстый” клиент и, в свою очередь, его противоположность, клиент “тонкий”. Если следовать этой же терминологии, то очень умный терминал будет очень тонким клиентом.

По сути, тонкий клиент – прямой наследник древних терминалов, но только с очень существенной разницей: он предоставляет доступ к точно такому же набору услуг, что и толстый клиент, без какого бы то ни было ущерба для пользователя. Просто услуги эти сосредоточены не там, где обычно. У тонкого клиента обычно нет жесткого диска, а памяти и вычислительной мощности столько, сколько нужно для предоставления доступа к серверу, у которого и мощностей, и памяти в избытке, чтобы хватило на всех. Тот же принцип можно использовать и для нашего предполагаемого очень тонкого клиента, только он будет еще меньше и еще тоньше. Доступ к услугам, сосредоточенным в некоем центре, будет осуществляться по высокоскоростным линиям связи с помощью предельно компактных терминальных устройств, причем не только в границах одного здания или организации, а повсюду – из дома, в поездке, по всему миру. Разумеется, сразу возникают вопросы: скорость подключения, надежность связи, конфиденциальность информации, но потенциально такие проблемы решаются техническими методами. Среда передачи должна иметь высокую пропускную способность; приложения для подключения не должны много “весить” (компьютерщики сейчас открыто признают, что сети часто работают медленно не потому, что им нужна дополнительная пропускная способность, а потому, что по сети надо слать меньше мусора); наконец, конфиденциальность можно обеспечить с помощью грамотно примененного шифрования. Систем, совершенно не подверженных взлому, нет и сейчас, вопрос только в силах, средствах и

времени, которые будут потрачены на преодоление защиты. Точно так же будет и в царстве терминальных технологий.

### Что же должен уметь делать очень умный терминал?

Представьте себе: вам не нужен ни кошелек, ни паспорт, ни пропуска, ни билеты на транспорт, ни кредитная карточка, ни записная книжка, ни мобильный телефон, ни часы, ни калькулятор... Продолжите этот список сами, если хотите. Суть в том, что есть вы (пользователь), есть некое средство вас идентифицировать и отличить от других пользователей, и есть набор информации и услуг, к которым вы имеете доступ, причем часть этой информации открытая – например, справочная информация, интернет, расписание движения поездов, атласы и карты, а другая часть – закрытая. К ней относятся ваши личные данные, номера счетов, адреса, ваши файлы, базы данных, фотографии, и к ним имеете доступ только вы сами. Деньги – это та же информация, и никто не мешает все расчеты вести в безналичной форме. Вы больше не будете носить с собой бумажник, греметь мелочью в кармане или держать кредитные карточки в специальном отделении кошелька. При покупке или плате за проезд, за услуги и т.п. вы просто будете идентифицировать себя как лицо, вносящее платеж, и эта информация будет поступать в единый центр данных, в котором с вашего счета будет списана соответствующая сумма. Любой таксофон (тогда, наверное, уже будут видеофоны) на улице позволит вам позвонить, когда вы идентифицируете себя. Если развить идею дальше, то везде – на почте, в магазинах, на рабочих местах, дома – будут стоять умные терминалы (немножко более толстые, чем очень умные терминалы), которые позволят вам после идентификации выйти в интернет, найти свои файлы, поработать с ними, скачать что-либо, перемес-



титель информацию из одного места в другое, просмотреть, распечатать и т.п. В чем-то это похоже на работу с пластиковыми карточками, с той лишь разницей, что технология будет расширена и станет применяться во всех сферах жизни, а не только для оплаты покупок или бронирования билетов. Разумеется, все это возможно только в том случае, если существует некий глобальный информационный центр, и весь мир опутан маршрутами доступа к нему – местами проводными, местами беспроводными, но везде с соответствующим интерфейсом. Магазиновые терминалы ведут по такой глобальной сети к базе данных товаров и цен и к счетам физических лиц, с которых списываются средства: телефонные терминалы ведут к счетам и к записным книжкам, где пользователь хранит данные о своих контактах; общедоступные справочные терминалы дают выход в интернет; терминал-считыватель у милиционера ведет в базу данных адресов, фотографий, паспортных данных гражданина и в список числящихся за ним правонарушений; считыватель гаишника ведет в базу данных транспортных средств и статистику аварий с участием водителя; считыватель врача скорой помощи – в базу данных, где хранится медицинская карта человека, данные о его группе крови, аллергии на лекарственные препараты; считыватель родителей дает доступ к базе данных школьных оценок их чада, а считыватель учителя позволяет без труда найти данные по прошлой успеваемости ученика и статистике прогулов, даже если он учился в другой школе в другом городе.

### Как может выглядеть очень умный терминал?

Мы уже практически описали его, но нужно внести несколько уточнений. Во-первых, подчеркнуть, что одно дело – терминал, и другое дело – идентификация человека, который в данный момент им пользуется.

Можно сказать так: любой терминал должен быть оснащен интерфейсом идентификации, а уж остальное – аппаратное исполнение, функциональность и предоставление доступа с ограничениями или без – конкретика, которая зависит от области применения устройства. Терминал может быть стационарным или мобильным, большим или маленьким, с экраном с высоким разрешением или с маленьким дисплейчиком. В зависимости от своих функций он может быть либо совсем глупым, либо достаточно продвинутым. Область использования глупых терминалов – турникеты в метро и наземном транспорте, считыватели в магазинах, в пунктах приема платежей за мобильную связь и коммунальных платежей, в билетных кассах театров и т.д., подобно тому, как сейчас действует система пластиковых карт. Фактически, эти самые пластиковые карты – одна из разновидностей идентификаторов. Другая разновидность – паспорт или военный билет. Третья – водительские права. Четвертая – удостоверение, карта доступа или членский билет того или иного клуба. Даже ИНН, индивидуальный номер налогоплательщика, и номер пенсионного страхового свидетельства – тоже идентификаторы. Думаю, у каждого из нас такой список составит с десяток пунктов, а то и несколько десятков. Спрашивается, зачем их так много, если все они характеризуют одного и того же человека, просто в разных сферах жизни? Если уж доводить до ума всю систему, то необходимо, чтобы у человека идентификатор был один, и чтобы в зависимости от ситуации и от прав других людей на получение информации он давал доступ к тем или иным сведениям. И еще желательно, чтобы идентификатор было трудно потерять и еще труднее подделать. Когда же кто-либо запрашивает информацию о человеке, в системе должен фиксироваться и идентификатор запрашивающего

лица. Логирование всех действий позволит отследить, кто, о ком и какую информацию получал, и тогда любые злоупотребления будут легко отслеживаться. Два требования, касающиеся сложности подделки и невозможности утери, сходу отмечают носимые идентификаторы – укоротить или потерять можно и паспорт, и карточку, и права, и удостоверение. Значит, остаются биометрические средства идентификации либо еще один вариант – вживление микрочипа под кожу. Биометрические интерфейсы совершенствуются с каждым годом. Можно сказать, предтечей этого направления выступает популярная сейчас идентификация по фотографии. Но если раньше для этого способа обязательным было участие оператора-человека – сурового таможенника, милиционера или паспортистки – то теперь есть алгоритмы, позволяющие оцифровать параметры лица. Не сохранить фото в цифровом формате, а зафиксировать N-ное количество параметров/измерений, по сочетанию которых можно было бы сделать заключение, тот это человек или не тот, с высокой степенью точности. В конце концов, почему лицо должно хуже подходить для идентификации цифровым методом, чем отпечатки пальцев? На данный момент такие цифровые системы идентификации по фото уже показывают неплохие результаты. Накопленные в базе данные по лицам позволяют проанализировать картинку с видеокамеры и дать положительное или отрицательное заключение: соответствует человек описанию или нет. Если кто-то скажет, что метод грешит неточностью, то на самом деле такое утверждение не вполне верно. Точность зависит от количества фиксируемых параметров. Если их полсотни, то результаты уже очень точные, и даже если портретное сходство введет в заблуждение человека-оператора, бесстрастная и точная машина может увидеть разницу. Плюс этого метода – бесконтактность, а также то, что за ним не тянется та-



за снятием отпечатков пальцев. Безусловный минус – зависимость от освещенности, разрешающей способности камеры, ракурса, ну и, наконец, от наличия на лице очков, усов, бороды, флюса, следов побоев, неумеренного макияжа и т.п. Все это преодолимо, но на преодоление потребуются дополнительные средства.

Дактилоскопия в этом отношении надежнее, это более испытанное средство. И хотя до сих пор научного доказательства уникальности отпечатков пальцев нет, но на самом деле это уже давно стало аксиомой. Есть расчет вероятности, который показывает, что для совпадения отпечатков пальцев у двух лиц численность населения должна составить такое количество, которое просто физически не уместится на нашей планете. Да, отдельный отпечаток может оказаться похож (хотя вероятность и этого события мала), но тогда можно сравнить все десять. Наконец, можно дактилоскопировать всю ладонь целиком. Устройства доступа на основе проверки отпечатка пальца (одного или нескольких) существуют уже много лет. Они совершенствуются, становятся все более точными и быстродействующими. Если же еще учесть, что криминалисты ведут базы отпечатков уже много лет и что во многих странах снятие отпечатков обязательно для военнослужащих, полицейских и других официальных служащих, то такой метод идентификации становится одним из самых перспективных. Его главный минус состоит в том, что для людей, воспитанных на боевиках и детективах, снятие отпечатков пальцев воспринимается как унижение человеческого достоинства. Кто-то скажет, что неприятна также контактность метода, но, в конце концов, вам же не мажут краской пальцы и не прижимают их к бумаге! Контактности тут не больше, чем в автобусе или вагоне метро, когда вы беретесь за поручень, за который до вас хватались сотни и тысячи людей.

Такие биометрические данные, как отпечатки пальцев ног, карта зубов и особенности походки, конечно, тоже позволяют идентифицировать человека, но применяют их в довольно специфических случаях, когда другими способами воспользоваться по тем или иным причинам нельзя. Они представляют интерес больше для правоохранительных органов, а для тех людей, кто относит себя к законопослушным гражданам, остаются еще идентификация по голосу и по сетчатке глаза. И то, и другое легко представить на охраняемом входе в лабораторию исследовательского институ-

та и сложно – в общественном транспорте, в магазине или на почте. Вдобавок, голосовую информацию могут услышать окружающие, для чьих ушей она не предназначена, ее могут записать на какой-нибудь носитель и затем воспроизвести, и наконец, обладатель голоса может просто охрипнуть, или тембр его голоса поменяется с возрастом. Идентификация по сетчатке таких недостатков не имеет, но зато ее минус – дороговизна оборудования и потребность в высокой точности. Довольно трудно себе представить использование такого метода, например, на турникетах в метро.

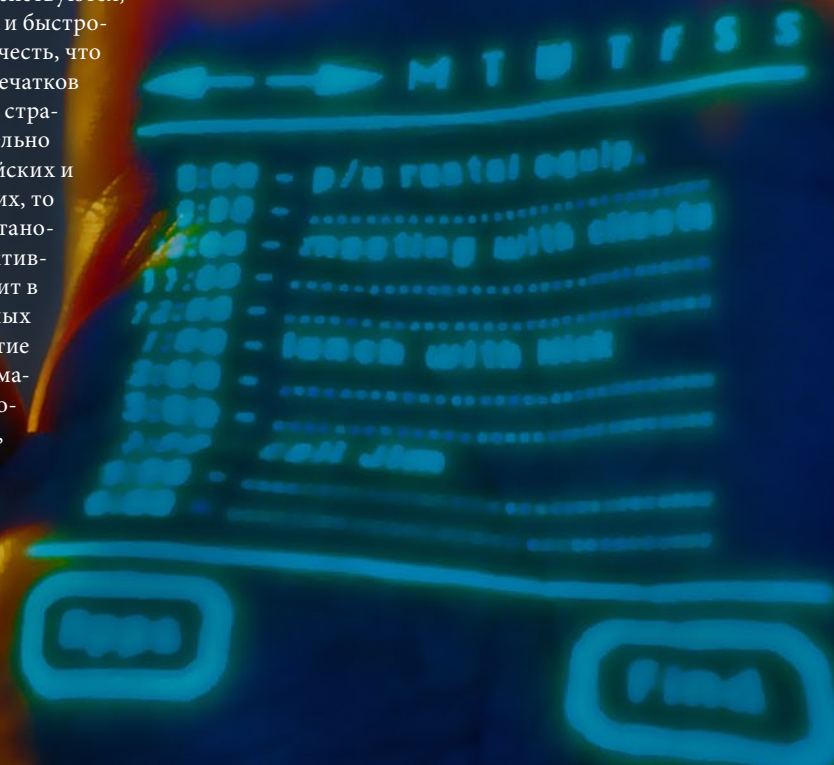
Получается, что биометрические методы пригодны не всегда и не везде. В этом отношении вживление микрочипа кажется более привлекательным вариантом. Правозащитники могут привести множество аргументов против, настаивая на том, что использование микрочипов нарушает права граждан, противоречит демократическим принципам и т.п., но тут всегда можно возразить: скажите, чем это нарушает права законопослушного гражданина?

Конечно, ею не будут злоупотреблять сторонние лица. Примеры этого есть и сейчас: украденные у провайдеров базы данных адресов, телефонных номеров, ворованные паспорта, данные банков о кредитных карточках клиентов и т.п. Принципиальной разницы между тем, что есть сейчас, и тем, что будет при использовании микрочипов, нет, просто лица, обслуживающие такую систему, должны внимательно относиться к вопросам безопасности, учитывая и технические, и организационные меры. Человеческий фактор был, есть и будет серьезным аспектом безопасности абсолютно любой системы.

А вот чиновничество от такой системы безусловно пострадает. Если вся информация будет сведена в единый центр, никому не придется больше бегать за справками, собирать бумажки, подписывать разрешения в разных инстанциях. Идентифицировал себя через ближайший терминал – и вся нужная информация под рукой. Электронной системе взятки не нужны...

На данный момент вживление микрочипов только начинает распространяться. Первыми эту технологию оценили владельцы домашних животных. В Западной Европе и США домашним питомцам уже несколько десятилетий вживляют под кожу микрочип с информацией о владельце и адресе его проживания. Если такое животное потерялось, шансов найти его гораздо больше. Сейчас такую услугу начинают предлагать и в ветеринарных клиниках России, но пока проблема в том, что считыватели распространены мало. Тем не менее, технология показала свою полезность, и теперь вживление микрочипов планируют сделать обязательным в американской армии. Наверное, этому примеру последуют и другие армии мира, а затем

и гражданские организации. Сама по себе технология прогрессивная, просто необходимо преодолеть некоторый психологический барьер. Начинается все с использования микрочипов в носимых идентификаторах – карточках, загранпаспортах, это есть уже сейчас – и лишь затем будет сделан шаг к вживляемым чипам. Их нельзя потерять и сложно подделать. Представьте себе, что вместо подписи того или иного документа,



вместо предъявления билета или передачи денег за покупку вам будет достаточно поднести к соответствующему терминалу руку или палец, и даже прикоснуться ни к чему не понадобится. На случай, если кто-то в испуге скажет, что тогда вместо кражи паспортов и кредитных карточек у людей будут руки отрывать, нужно делать идентификаторы такого типа, чтоб они действовали только в составе живого тела и моментально меняли состояние при извлечении, причем необратимо. Для расследования преступлений в этом случае поможет серийный номер чипа, который должен определяться только специальным оборудованием, дорогим и недоступным для потенциальных злоумышленников. База данных таких серийных номеров должна вестись очень четко и быть доступной только спецслужбам. Кто-то сочтет, что такая бесконтактность рискованна и создает почву для преступлений против личности, но ведь сегодняшняя ситуация ничем не лучше: кто мешает потенциальному грабителю вытащить у вас документы и потребовать вознаграждение за их возвращение? Или вытянуть из кармана мобильник и получить доступ к базе телефонных номеров ваших знакомых? Или вытащить у вас кредитные карточки и пойти с ними по магазинам, потренировавшись подделывать подпись, или делая покупки через интернет? Или просто подстеречь на выходе из банка или сберкассы и обчистить карманы?

Естественно, единая система идентификации и единая сеть терминалов будет работать корректно только в том случае, если идентификатор будет присвоен каждому человеку, а терминалы будут распространены повсеместно и будут полностью совместимы. Терминалы могут быть общественного пользования, а могут быть личными. Какие-то устройства могут оставаться независимыми – например, плеер, радиоприемник, но основная масса устройств будет объединена в общую сеть, и услуги будут предоставляться централизованно.

Разумеется, до этого еще очень далеко. Да и конкретная реализация может отличаться в ту или иную сторону – кто сейчас может с гарантией предсказать, куда заведет нас технический прогресс? Кому-то такая система покажется тоталитарной, недемократичной: дескать, человек в ней полностью контролируется, все его действия можно отследить... Это не так. Воля у человека останется своя, решения принимать он будет сам, и подобная система не превратит его в послушного робота. Просто в целом деятельность всех и вся станет несколько прозрачнее, чем сейчас. Честный человек такой разницы может вообще не почувствовать. Интересно, что почувствуете вы? ■

