Этические проблемы новых технологий: конкретные примеры

С ростом значения ИКТ в мире растет и понимание необходимости признавать этические аспекты новых технологий. Более того, высокая скорость технологических изменений требует, чтобы мы продумывали использование новых технологий и их потенциальное влияние на стадии разработки, а не тогда, когда последствия становятся очевидными, а мы еще не готовы реагировать на них. Рассматривая технологии завтрашнего дня в свете задач инфоэтики, общество сможет лучше предвидеть их последствия и развивать их таким образом, чтобы использовать преимущества, снижая возможный вред.

Представленные ниже конкретные примеры (кейс-стади) анализируют некоторые из таких технологий и указывают на связанные с ними вопросы, вызывающие беспокойство с точки зрения инфоэтики.

Семантическая сеть и другие метаданные

Что такое «Семантическая сеть»?

Интернет был задуман как инструмент, с помощью которого люди могли бы обмениваться текстами, изображениями и другой информацией. Однако экспоненциальный рост контента делает Интернет все менее пригодным для работы. Поисковые машины стремятся смягчить эту проблему за счет предоставления средств навигации, но решение, которое они предлагают, не является кардинальным. Чтобы сделать Интернет полностью пригодным для навигации, требуются взаимодействующие друг с другом метаданные, или данные о данных. Эти метаданные могут служить также и для того, чтобы Интернет стал более машиночитаемым и позволил компьютерам из «тупых» инструментов превратиться в интеллектуальных агентов. Семантическая сеть[27] обещает предоставить такие метаданные.

[27] Семантическая сеть – это официальный проект WWW-консорциума (World Wide Web Consortium), созданный Тимом Бернерс-Ли (Tim Berners-Lee) – изобретателем Сети.

Как работает Семантическая сеть

Интернету было уже почти 30 лет, когда он вдруг стал популярной средой для информации и коммуникации[28]. Несмотря на то, что с самого начала он базировался на стандартных компьютерных языках, или кодах (TCP/IP, SMTP и др.), стимулом для бурного развития стали безвозмездные языки Всемирной сети (Сети), а именно HTML и HTTP, а также тот факт, что HTML чрезвычайно дружествен для пользователей. Эти два языка позволили установить «слабую связь» между машинами, участвующими в обмене информацией, т.е. любой клиент Сети, занимающийся поиском информации, мог обращаться к любому веб-серверу, который предоставлял информацию в удаленном доступе и в устраивающей потребителя форме. Использование Интернета пережило колоссальный подъем, и этот феномен подстегнул создание нового контента, что, в свою очередь, дало толчок росту обмена информацией.

С учетом больших объемов сетевого контента Семантическая сеть призвана «создать универсальную среду для обмена данными»[29], используя те же свойства слабой связи для программируемых данных, которая была использована для предоставленных людьми данных с HTML.

Этот новый язык должен обеспечивать предсказуемость растущего обмена в киберпространстве и непосредственно анализировать контент, а словари метаданных – предоставлять большую точность при доступе к компьютерам.

Семантическая сеть сочетает набор компьютерных языков[30] для предоставления машиночитаемых описаний веб-контента. Эти метаданные могут создавать люди или компьютеры, и они должны предоставлять контекст контента, не требуя от человека или машины анализировать этот контент. Семантическая сеть маркирует информационный объект, обрабатывает его данные и присваивает ему некое контекстное значение, основанное на анализе связей данного объекта с другими элементами контента. Это позволяет машинам проводить поиск по веб-сайтам и выполнять задачи в соответствии с заданными стандартами.

Несмотря на то, что само название отсылает нас к Сети, этот проект призван дать машинам возможность обрабатывать данные по целому ряду интернет-приложений.

[28] History of the Internet (История Интернета – запись в Wikipedia) – http://en.wikipedia.org/wiki/Internet_history (просмотр 8 ноября 2006 г.).

[29] http://www.w3.org/Consortium/activities#SemanticWebActivity.

[30] Например, Resource Description Framework (RDF), Web Ontology Language (OWL) и Extensible Markup Language (XML).

Последствия и задачи

Богатство контента, имеющегося в информационных сетях и в Интернете в особенности, полезно только тогда, когда люди могут на самом деле найти и получить доступ к интересующей их информации. Семантическая сеть позволяет людям использовать компьютеры в качестве агентов для поиска требуемого контента на основе широкого набора критериев, в числе которых – статус контента как общественного достояния или интеллектуальной собственности, альтернативные источники контента в разных форматах или на разных языках и даже существование доказательств, служащих для опровержения взгляда, предложенного в контенте.

Богатство контента тесно связано с взрывным развитием Интернета, которое часто приписывают принципу «нейтралитета сети». Этот принцип декларирует равную обработку всех элементов трафика. Странно, но Семантическая сеть смогла пойти наперекор этому нейтралитету, вооружив участвующие стороны инструментами для фильтрации интернет-контента на основе ассоциированных метаданных: ISP, маршрутизаторы или поисковые машины могли использовать эти метаданные для проведения различий между типами контента, обеспечивать предпочтения по обработке какому-то определенному трафику и ставить барьеры для входа новым услугам или провайдерам контента. В этом отношении машиночитаемые метки Семантической сети могли маркировать контент для дискриминации и сократить возможности пользователей по созданию и обмену материалами.

Более того, многие утверждают, что, если Семантическая сеть будет предоставлять пользователям возможность доступа только к тому контенту, который им нужен, то она может разрушить общественный диалог. Теория гласит, что полное участие в жизни общества невозможно без форума, на котором каждый человек имеет возможность высказать свое мнение, но Семантическая сеть и другие технологии позволяют пользователям полностью адаптировать под свой опыт и получать только тот контент, который они однозначно запрашивают. Другими словами, Семантическая сеть способствует изоляции конечного пользователя и тем самым косвенно разрушает форум. Таким образом, существует мнение, что Семантическая сеть способна нанести вред самой идее взаимосвязи, которую она призвана продвигать[31].

[31] Cass R. Sunstein, «The Daily We», Boston Review (Summer 2000), http://www/bostonreview.net/BR26.3/sunstein.html. Другие,однако, готовы оспаривать идею, что даже кажущийся низким уровень открытости для разных взглядов в Сети (15%) может создать условия для более широкого, чем когда-бы то ни было, общественного диалога. См. Eszter Hargittai, «Cross-Ideological Conversations among Bloggers» («Беседы с блоггерами с разных идеологических позиций»), http://crookedtimber.org/2005/05/25/cross-idelological-conversations-among-bloggers/ просмотр 8 ноября 2006 г. (описание работы Eszter Hargittai, Jason Gallo и Sean Zehnder по анализу перекрестных связей между либеральными и консервативными политическими блогами).

С точки зрения теории машины должны быть запрограммированы для распределения информации по категориям и присвоения ей определенных значений, для того, скажем, чтобы персональные данные можно было отличить от прогноза погоды и пометить как требующие гарантий защиты прайвеси. В этом смысле существует риск, связанный с созданием инструментов только для обмена информацией без одновременного кодирования для присвоения более высоких значений данным, относящимся к человеку. Защита прав человека может потребовать, чтобы программирование помещало персональные данные на более высокий уровень.

И все же не следует преувеличивать опасности Семантической сети. В конце концов, эти недостатки возможны и без метаданных и не обязательно должны проявиться в случае с метаданными.

Подводя итоги, можно сказать, что Семантическая сеть будет поддерживать задачу продвижения доступа к информации, значительно облегчая идентификацию, систематизацию и использование существующего контента.

Управление цифровой идентичностью

В предыдущей части мы говорили о том, как метаданные позволяют осуществлять постоянно усложняющийся обмен информацией. Развитие коммуникации между машинами создает вероятность появления благоприятных или неблагоприятных последствий этого процесса, таких как снижение расходов при заключении коммерческих сделок или опасность вирусных атак.

В этом разделе рассматривается возникновение необходимости в средствах управления цифровой идентичностью, позволяющих лучше контролировать потоки персональной информации. Изучение этого материала позволит перейти к следующей части, в которой показывается, как посредством биометрии метаданные могут «вычислить» конкретную физическую личность, которая стоит за различными цифровыми данными.

Что такое «управление цифровой идентичностью»

Если говорить просто, то управление цифровой идентичностью – это управление цифровой информацией, касающейся конкретного человека. Иногда такую информацию называют «персональными данными» или «персонально идентифицируемой информацией». Второй термин более точно определяет, что данные могут быть привязаны к конкретной личности.

Изначально архитектура Интернета не предполагала механизма для проверки или аутентификации идентичности пользователей. Раз-

работчики Сети работали в другое время и в других условиях, отличных от современной интернет-среды, а сообщество интернет-пользователей в то время состояло из объединенных общими целями и интересами, пользующихся взаимным доверием специалистов-компьютерщиков. Интернет, который они создали, отражал их культуру.

В результате бурного развития Сети участниками такого взаимодействия стало огромное количество пользователей, и не удивительно, что существовавшая когда-то в Интернете атмосфера доверия изменилась и люди начали относиться к этому пространству с растущим недоверием. Иными словами, Интернет пережил своего рода урбанизацию: все больше и больше людей пользуются его услугами, однако сообщество в «традиционном» понимании распалось, и теперь люди понимают, что, находясь в Интернете, они должны быть настороже. Компьютерные специалисты говорят сегодня: «Оглядываясь назад, мы понимаем, что должны были включить в Интернет уровень аутентификации. Сегодня, когда Сеть так разрослась и столько торговых сделок совершается через Интернет, возможности для мошенничества колоссальны»[32].

Статистика электронной коммерции подтверждает факт такого сдвига. Опубликованные в прошлом году данные показали резкий спад числа потребителей, чувствующих себя уверенно при совершении электронных коммерческих сделок[33]. Люди научились задаваться вопросом, является ли человек или организация на другом конце сделки именно тем, за кого этот человек или организация себя выдает, и люди хотят знать, смогут ли они привлечь эту другую сторону к ответственности, если что-то пойдет не так. Отвечая на электронное письмо или заполняя онлайновую форму, не рискует ли человек стать жертвой мошенничества?[34]

[32] Интервью с Паулем Тревитиком (Paul Trevithick) – руководителем проекта Eclipse Foundation's Higgins Trust Framework, август 2005 г.

[33] Riva Richmond, «Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds», Wall Street Journal, 23 июня, 2005, стр. B3, отчет об исследовании Гартнера 5000 онлайновых потребителей. В статье говорится, что более 42% онлайновых покупателей и 28% людей, осуществляющих в онлайне банковские операции, отказываются от этих возможностей по причинам безопасности и недостаточной защиты прайвеси.

[34] Дэвид Бэнк (David Bank) и Рива Ричмонд (Riva Richmond) дают следующее объяснение в Wall Street Journal, 18 июля, 2005: «Ловя рыбку в мутной воде», мошенники рассылают электронные письма, один вид которых убеждает в том, что они происходят из пользующегося доверием источника, такого как Citibank или eBay. Щелкните на ссылку в письме и попадете на веб-сайт, на котором вас попросят дать номера своих счетов, пароли и прочие личные, не подлежащие огласке сведения. После этого начинается «сбор урожая», когда хакеры взламывают серверы, на которых сидят официальные веб-сайты. Наберите адрес официального сайта, и вас переадресуют на его аналог».

В то же время интернет-пользователи жалуются на то, что им приходится запоминать пароли и заполнять кучу всяких бланков, чтобы взять в аренду машину, купить книгу или совершить какую-то другую онлайновую сделку. И, хотя это надоевшее дело многих раздражает, людей уже «приучили» предоставлять о себе информацию таким способом и делать это, не задумываясь[35].

Специалисты в данной области говорят, что средства управления цифровой идентичностью сделают онлайновый обмен информацией намного более безопасным и удобным, поскольку эта технология помогает установить более жесткий контроль над цифровой информацией, касающейся личности[36].

На сегодняшний день массовые потребители не освоили эту технологию, потому что она пока не представлена в приемлемой для них форме. Microsoft еще не оправился от прошлого опыта, когда пытался внедрить подобные средства[37], и другие технологические компании взяли на заметку один факт: люди не хотят, чтобы одна-единственная мощная компания находилась в центре их доверительных отношений или получила монопольное право распоряжаться их персональными данными.

Именно поэтому разработчики технологий[38] концентрируют свои усилия на создании ориентированных на пользователей способов управления цифровой идентичностью. В этой новой парадигме человек сам будет выбирать себе «провайдера идентичности», который будет оперировать его персональными данными, в ряде случаев и только с разрешения владельца передавая эти данные другому лицу или организации в процессе заключения сделки. В то же время новая система будет проверять и идентичность второго участника сделки.

Принцип работы управления цифровой идентичностью

Модель, ориентированная на пользователя, состоит из двух основных частей: одна управляет обменом

[35] На этом всегда акцентирует внимание Ким Кэмерон (Kim Cameron) – архитектор идентичности и доступа компании Microsoft. Он напоминает коллегам по отрасли, что люди – не дураки, просто им выдали плохие инструменты для онлайнового взаимодействия.

[36] См., например, Kim Cameron «Identity Weblog», http://www/identityblog.com/, Dick Hardt «Identity 2.0», http://www.identity20.com/ и другие источники, доступные на http://www/identitygang.org/individuals.

[37] За последние годы рынок практически отверг системы управления идентичностью «Passport», разработанные Microsoft. Рынок также категорически отказался от предшественника «Passport» – системы «Hailstorm».

[38] OpenID, Sxip, the Liberty Alliance, Shibboleth, Passel и другие игроки в данной отрасли присоединились к Microsoft в поиске средств управления идентичностью, которые будут приняты рынком.

информацией об идентичности, когда та проходит между исходным и конечным компьютерами или устройствами, а вторая помогает пользователю оперировать принадлежащей ему информацией об идентичности на его собственном компьютере. Работающая на отрезке пути между устройствами новая система представляет собой некий набор правил по обмену информацией[39] (которые называются компьютерными протоколами) в виде упакованных запечатанных опознавательных знаков. Пользователь может по желанию пользоваться услугами любого провайдера идентичности для хранения своей личной информации и присвоения ей меток (маркеров); также он может работать с разными провайдерами (например, одного использовать для управления данными по кредитным картам; другого – для управления основной персональной информацией, к которой относятся имя, фамилия и дата рождения; третьего – для обработки медицинских карт и т.п.). Провайдеры идентичности могут быть резидентными (располагаться на компьютере пользователя) или находиться в другом месте, доступном через Интернет.

Так, например, когда человек хочет совершить онлайновую сделку, компьютер или устройство на другом конце (на языке отрасли это называется «полагающаяся сторона») указывает своему «агенту», какой пакет информации требуется. После этого агент запросит метку, содержащую требуемые данные, от одного или более провайдеров идентичности, которым данный человек доверил хранение этой информации. Провайдер идентичности передаст метку «полагающейся стороне». Человек каждый раз может контролировать такой обмен, или же он может сделать это однажды, а затем разрешить обмен в автоматическом режиме.

Вторая часть системы – это то, что происходит на компьютере или устройстве самого человека. Вместо того чтобы запоминать пароли или набирать текст при заполнении онлайновой формы заказа, человек, участвующий в электронной коммерции, может просто выбрать визуальное представление или иконку конкретного пакета, который ему нужен (например, иконку, обозначающую банковские операции, медицинскую или налоговую информацию). Когда пользователь выберет эту иконку, его агент инициирует запрос провайдеру идентичности на выдачу цифровых меток доверенной стороне, как описано выше. Агент будет в состоянии работать с разными устройствами, будь то ПК, сотовый телефон или другие мобильные устройства. Этот агент будет единственным компонентом системы цифровой идентичности, в

[39] Консорциум в составе Microsoft, IBM и других технологических фирм разработал стандарты для такого обмена как часть более крупного набора стандартов для веб-услуг.

которой пользователь должен будет авторизоваться непосредственно (например, путем сканирования отпечатка пальца).

В качестве доверенного посредника агент идентичности человека будет находиться в центре коммуникации и иметь доступ ко всей информации об идентичности, которой обмениваются пользователи. Он раскроет метку и переведет требования с языка одной системы в формат, распознаваемый другой системой. Для обеспечения максимальной защиты прайвеси этот доверенный посредник сведет, в идеале, к минимуму объем раскрытой в процессе транзакции персональной информации. Во многих случаях это может потребовать трансформации информации в метке в альтернативную метку, соответствующую конкретному запросу. Например, посредник сможет взять из метки информацию о том, что человек родился в такой-то день (к примеру, 20 июля 1969 года), и перевести ее так, что в новом запросе будет указан лишь один факт – человеку действительно больше 21 года.

Стремясь претворить теорию на практике, Microsoft планирует развернуть производство системы «Cardspace» – дружественной для пользователя системы обмена метками с визуальными иконками, напоминающими карточки, которые люди обычно носят в бумажниках: водительские удостоверения, кредитные карты и т.п. Согласно плану эта система будет включена в новую версию Windows, известную как Windows Vista[40], но система цифровой идентичности будет также доступна и в обновленных версиях Windows XP. Microsoft проводила частную кампанию в целях убедить крупных игроков электронной коммерции, таких как Amazon и eBay, принять эти новые услуги в обмен на упрощенный доступ к пользователям Microsoft. Поскольку довольно много людей уже работают в Windows XP, распространение этих новых услуг не будет зависеть от степени популярности более новой версии Windows Vista. С учетом того факта, что Windows XP работает сегодня на сотне миллионов машин, эти инструменты управления цифровой идентичностью могут с большой долей вероятности прижиться.

Тем временем IBM и Novell объявили в феврале 2006 г. о намерении предложить новый программный код, позволяющий встраивать аналогичные средства управления цифровой идентичностью, используя программы с открытым исходным кодом. Проект под названием «Higgins» позволит разным средствам управления идентичностью взаимодействовать между собой[41]. Вместо того, чтобы оперировать самими цифровыми идентичностями,

[40] Планируется, что Windows Vista получит массовое распространение в начале 2007 г.

[41] Управляет системой Higgins сообщество открытого кода Eclipse Foundation.

Higgins сочетает разные системы, делая возможным обмен информацией между ними по заданию пользователей[42]. Привлекательной видится перспектива мобильности в системах оценки репутации, которая позволит человеку «перенести» репутацию, которую он заслужил в сообществе eBay[43], в мир Second Life[44]. Технические требования к такой мобильности находятся в начальной стадии разработки.

Последствия и задачи

Новые средства управления цифровой идентичностью обещают положить конец «ловле рыбки в мутной воде» и, возможно, также решат проблему спама. Так как агент идентичности может помочь минимизировать данные, раскрываемые коммерсанту или другому партнеру, с которым человек имеет дело, технология может способствовать большей приватности, поскольку сводит к минимуму количество организаций, имеющих доступ к личным данным индивида. Пожалуй, самым важным является то, что распределенная архитектура системы должна уменьшить ее уязвимость перед атакой, поскольку теоретически данные не сосредоточены в одном месте.

Если система может таким образом защитить персональные данные, управление цифровой идентичностью обладает множеством возможных преимуществ для общества, включая предотвращение злонамеренного поведения и превращение Интернета в более удобный для коммерции форум. С этой точки зрения технология способствует сохранению неприкосновенности частной жизни, безопасности и установлению более высокого уровня жизни.

Итак, средства, позволяющие осуществлять обмен персональными данными на основе индивидуальных предпочтений, могут способствовать социальным взаимодействиям. Пауль Тревитик, руководитель проекта Higgins, подчеркивает преимущества ориентированного на пользователя уровня сети, который «дает людям больше контроля над своими цифровыми идентичностями в самых разных компьютерных контекстах (таких как электронная почта, мгновенный обмен сообщениями, электронная коммерция, общие сетевые ресурсы и справочники предприятий), и особенно тех, в которых участвуют социальные сети»[45]. В этом смысле средства управления цифровой идентичностью

[42] Интервью с Джоном Клиппингером (John Clippinger) – старшим научным сотрудником Центра Беркмана «Интернет и общество» (Berkman Center for Internet and Society) при Гарвардской юридической школе (Harvard Law School), осень 2005 г.

[43] http://pages.ebay.com/services/forum/feedback.html – описание системы репутации eBay (просмотр 8 ноября 2006 г.).

[44] http://secondlife.com/whatis/ – описание трехмерного виртуального мира Second Life (просмотр 8 ноября 2006 г.).

[45] Интервью с Паулем Тревитиком (Paul Trevithik), 20 сентября 2005 г.

могут благоприятствовать развитию свободы собраний.

С другой стороны, существование систем управления цифровой идентичностью может представлять серьезный риск для неприкосновенности частной жизни и безопасности. Как уже отмечалось выше, в предлагаемой архитектуре агент персональной идентичности будет выступать в роли доверенного посредника в новой системе цифровой идентичности; однако ныне существующие технологии не гарантируют, что агент персональной идентичности не будет вступать в сговор с другими сторонами сделки (т.е. провайдерами идентичности и полагающимися сторонами).

Кроме того, вполне возможно, что рынок не поддержит множество провайдеров идентичности и что услуги по провайдингу идентичности будут сосредоточены в одном месте. Проще говоря, пользователям может показаться неудобным или слишком дорогим решение разделять свои данные и поручать их элементы разным провайдерам идентичности. Или же полагающиеся стороны будут неохотно признавать провайдеров идентичности, в результате чего доминировать на рынке станет ограниченное число таких провайдеров. Так или иначе, контролировать весь массив персональных данных будет ограниченное число провайдеров идентичности. Более того, принимая во внимание особенности существующей системы, у провайдеров идентичности и полагающихся сторон есть технические возможности для сговора. Другими словами, непонятно, как игроки в инфраструктуре управления идентичностью будут подотчетны пользователям и информационному обществу в целом[46]. Конечно, рынок может подстегнуть развитие технологий, архитектура которых гарантирует честное поведение, а закон вполне сможет стимулировать эту инициативу[47].

Некоторые считают, что основная забота инфоэтики – разобраться в том, что произойдет, если крупный игрок – правительство или мегакорпорация – узурпирует распределенную ориентированную на пользователя систему и использует свой глобальный уникальный идентификатор, нарушая тем самым принцип ориентированности на пользователя, повсеместно провозглашаемый разработчиками. Другими словами, сегодня не существует внутренней технологической защиты на случай возможного использования таких инструментов в будущем. Если бы эти инструменты были бы злонамеренно, в целях дискриминации, принуждения и блокирования коммуникации применены, на всем

[46] Mary Rundle and Ben Laurie, «Identity Management as a Cybersecurity Case Study» («Управление идентичностью – кейс-стади кибербезопасности»), Berkman Center Publications Series, сентябрь 2005, стр. 8.

[47] Microsoft заняла твердую позицию в вопросе законодательства по прайвеси в 2006 г.

пространстве информационного общества права человека и связанные с ними задачи инфоэтики оказались бы в большой опасности.

Масштаб таких последствий не следует преуменьшать, учитывая возможность революции в области взаимодействия между машинами или в сфере веб-услуг, к которой может привести управление цифровой идентичностью. Дейл Оулдс (Dale Olds), ведущий специалист Novell в этой области, указывает, что целью проекта Higgins может стать разработка дополнительной технологии, которая могла бы *автоматически* передавать информацию от определенной цифровой идентичности (или личности) индивида, когда он заходит на веб-сайт[48]. Именно в этом случае инструменты управления цифровой идентичностью могут быть наиболее влиятельными: позволяя машинам автоматически обмениваться персональными данными от имени человека, упомянутые инструменты устранят самые серьезные препятствия на пути развития веб-услуг. Поэтому наделение машин такими возможностями может привести к перевороту в межмашинных взаимодействиях.

Наделение машин подобными возможностями указывает на, пожалуй, самое значительное и потенциально опасное последствие: дело уже не в том, *что люди могут делать* с помощью данных инструментов, но в том, *как машины будут обращаться с людьми*, обладая настолько хорошо организованными персональными данными. Ким Кэмерон (Kim Cameron) – главный архитектор Microsoft по идентичности и доступу акцентирует внимание на этом прогнозе:

«Более общие аспекты того, как интеллект Сети реагирует на нашу личность, волнует меня все больше, когда я задумываюсь, что будет через 20 лет… Помимо злоупотребления властью существуют и другие равно неприятные варианты будущего, связанные с потенциальными отношениями между человечеством и машинным интеллектом. Я понимаю, что люди не склонны обсуждать этот вопрос, потому что пока это – проблема слишком отдаленного будущего, однако взаимное влияние этой пары может привести к действительно пугающим последствиям»[49].

Биометрия

В то время как система управления цифровой идентичностью расширяет словарь метаданных с целью осу-

[48] Robert Weisman, «Harvard, tech firms push data privacy: Goal is to let Net users control the personal» («Гарвард: технические фирмы продвигают идею прайвеси данных, чтобы Сеть могла контролировать персональную информацию»), Boston Globe, 27 февраля, 2006.

[49] Переписка по электронной почте с Ким Кэмерон, осень 2005 г. (приводится с разрешения автора).

ществления автоматизированного обмена персональными данными, ее прототип из реального мира – биометрия – занимается применением метаданных к физическому пространству. Поскольку обе имеют дело с человеком, возникает лингвистическое смешение виртуального и реального миров, поскольку для описания и того, и другого используются одни и те же базовые метаданные.

Что такое «биометрия»

Биометрия – это новая технология, которая измеряет и анализирует уникальные характеристики индивидов, включая физические и поведенческие параметры. Следующие характеристики часто называют биометрическими:

- ДНК;
- типы лица;
- отпечатки пальцев;
- походка;
- радужная оболочка глаза.
- типы сетчатки глаза;
- запах;
- подпись;
- почерк;
- голос.

Несмотря на то, что, как известно, биометрия была известна в Китае еще в XIV веке[50], она считается новой технологий, потому что сбор, оценка и анализ биометрических данных все чаще автоматизируются и представляются в цифровой форме. Как таковая, биометрия может сочетаться с другими технологическими достижениями – например, метаданными (поскольку биометрические данные могут обрабатываться и передаваться машинами); управлением цифровой идентичностью (поскольку оба направления оперируют персональными данными) и датчиками (поскольку биометрические измерения часто осуществляются сенсорными устройствами).

Основной движущей силой развития биометрии в последние годы было стремление добиться безопасности, как со стороны частного сектора бизнеса (желающего, например, ограничить доступ к коммерческой тайне), так и со стороны правительства (желающего, например, ограничить передвижение преступников или лиц, подозреваемых в совершении преступлений). Многие правительства активно поощряли научно-исследовательские и конструкторские работы в данной области после террористических атак на США 11 сентября 2001 г.

Принцип работы биометрии

Биометрия человека регистрируется в системе, когда одна или несколько его физических или поведенческих характеристик записываются устройством. Затем результаты измерения обрабатываются по численному алгоритму, который переводит их в цифровую форму. Полученные данные заносятся в базу. В этот момент человека можно

[50] Статья в Wikipedia по биометрии (http://en.wikipedia.org/wiki/Biometrics), просмотр 7 февраля 2006 г.

считать «зарегистрированным», независимо от того, знает он об этом или нет. Каждая следующая попытка системы провести аутентификацию биометрии данного человека требует новой записи данных и ее оцифровки. Затем это цифровое представление будет сопоставлено с тем, что уже существует в базе данных, и проверено на предмет совпадения.

Последствия и задачи

В 1997 г. Международная организация гражданской авиации (ICAO) приступила к разработке «глобального гармонизированного проекта включения информации биометрической идентификации в паспорта и другие машиночитаемые документы…»[51] Этот проект был одобрен членами ICAO в 2003 г. Поскольку внедрение такого проекта требует больших усилий, полная программа осуществляется в настоящее время ICAO для завершения указанной гармонизации.

188 государств–членов ICAO обязаны будут выполнять данное глобальное требование в отношении электронных проездных документов: в конечном итоге, статья 22 Чикагской конвенции призывает подписавшие ее государства «принять все практически выполнимые меры для предотвращения нежелательных задержек самолетов, экипажей, пассажиров и грузов, в особенности в отношении законов по иммиграции, карантину, таможне и таможенным пошлинам». ICAO заявила, что проект поможет государствам-участникам «внедрить по всему миру стандартизированную систему подтверждения идентичности»[52].

Как уже упоминалось выше, главный этап в ориентированной на пользователя системе управления идентичностью предполагает первичную аутентификацию пользователя для его электронного агента – чтобы последующие запросы основывались на этом подтверждении. Вполне возможно, что универсальные биометрические стандарты ICAO для машиночитаемых проездных документов превратятся в глобальный механизм для санкционированного правительством доказательства идентичности – и в то же время будут служить для первичной аутентификации. Подобная признанная во всем мире система цифровой идентичности видится как окончательная гарантия того, что любой человек является именно тем, за кого он себя выдает, и что запросы, основанные на этой идентичности, были подлинными.

Легко понять, почему международная система склонна принять такой под-

[51] Веб-сайт ICAO: http://www.icao.int. Для получения дополнительной информации о данной организации и краткого описания проекта см. http://www.netdialogue.org/initiatives/icaomrtd/.

[52] Пресс-релиз ICAO от 28 мая 2003 г.

ход. В конце концов, всеобщий уникальный идентификатор представляется окончательной гарантией при управлении цифровой идентичностью и по этой причине будет способствовать развитию онлайновых транзакций; он также сможет помочь в обеспечении порядка и защиты от кибератак. Кроме того, он предоставит глобальный метод для претворения в жизнь других международных обязательств по мониторингу действий отдельных людей на благо стабильности налоговой системы, сферы финансовых услуг, защиты окружающей среды и т.п.[53] Короче говоря, всеобщий уникальный идентификатор мог бы стать эффективным решением задачи по присвоению человеку официальной цифровой индивидуальности в информационном обществе.

Чтобы система смогла обеспечить ситуацию, при которой каждый человек имеет одну и только одну присвоенную ему государством идентичность, она нуждается в центральном администрировании[54]. Вполне предсказуемо, что взять на себя эту роль может быть предложено некоему международному агентству. В свете того, что международные организации не застрахованы от коррупции, доверить одной глобальной организации настолько уязвимую информацию – значит рискнуть здоровьем информационного общества. Проще говоря, международные институты не вооружены механизмами, предотвращающими злоупотребление властью.

Более того, управляемая из центра система идентичности может стать главной мишенью для атак. Ни одна организация не в состоянии технически обеспечить безопасность своих систем. Гораздо менее рискованный подход заключается в предотвращении централизации этих данных.

Если международная система действительно включала бы широкое использование биометрии или какого-то другого глобального идентификатора, такое решение стало бы концом анонимности. Стало бы возможным создать подробный отчет о действиях каждого человека, включая информацию о том, куда человек пошел, на что потратил деньги, с кем общался, что читал и т.п.[55]

Наряду со смертью анонимности мы сможем наблюдать и такое явление,

[53] Обсуждение данных инициатив представлено в работе Мэри Рандл и Бена Лаури (Mary Rundle and Ben Laurie) «Identity Management as a Cybersecurity Case Study» («Управление идентичностью как кейс-стади кибербезопасности»), Berkman Center Publication Series, сентябрь 2005.

[54] Stephen T. Kent and Lynette I. Millett, Editors, «IDs – Not that Easy: Questions About Nationwide Identity Systems» («Удостоверения личности – все не так просто: вопросы о национальных системах идентификации»), Computer Science and Telecommunications Board: Committee on Authentication Technologies and Their Privacy Implications, Washington, DC: National Academy Press, 2002, Chapter 2.

[55] Конечно, такое досье можно составить и без биометрии или других глобальных уникальных идентификаторов. Профилирование данных – это растущий бизнес и он имеет большое будущее благодаря тем технологиям, о которых мы расскажем ниже.

как информационная асимметрия: каждое движение человека будет отслеживаться, при этом он может не знать о таком наблюдении. Помимо нарушения прайвеси, такое положение дел плохо сочетается с соблюдением других фундаментальных свобод, таких как право на собрания или право на поиск, получение информации и на обмен ею, особенно учитывая тот факт, что страх попасть под наблюдение может служить серьезным сдерживающим фактором.

Наконец, биометрические процедуры, такие как идентификация по лицу, становятся со временем более точными. Однако ложные совпадения по биометрии могут привести к обвинению человека в преступлении, поднимая тем самым инфоэтический вопрос о том, что же, собственно, составляет доказательство, если человек считается невиновным, пока вина его не доказана.

Радиочастотная идентификация (RFID)

Что такое RFID

RFID – это технология, позволяющая осуществлять обмен данными с небольшого недорогого беспроводного устройства, известного как RFID-чип, снабженного компьютерным чипом и антенной. RFID может просто передавать свой уникальный идентификационный номер, а также дополнительные данные о конкретном объекте (например, дату упаковки продукта, цену, завод-изготовитель и т.п.) или лице (фамилия и имя, состояние здоровья и т.п.). Несмотря на то, что эта технология используется с 1980-х годов, она получила сегодня широкое распространение благодаря достижениям в сетевых коммуникациях, миниатюризации и компьютеризации.

Одной из главных функций технологии RFID сегодня является отслеживание продукции. Сеть Wal-Mart и Министерство обороны США известны как главные инициаторы прогресса в этой сфере, поскольку они потребовали от своих крупнейших подрядчиков, чтобы те использовали RFID-чипы[56]. Основным мотивирующим фактором являются каналы поставок и управление материально-техническим снабжением. Когда лента конвейера загружается продукцией, каждый элемент которой имеет RFID-чип, весь груз может быть проконтролирован во вре-

[56] По сообщению Тодда Спрэнглера (Todd Sprangler), «Wal-Mart – крупнейший в мире продавец в сфере розничной торговли – говорит об удвоении числа своих магазинов, использующих RFID, и доведении общей численности до 1000 в январе 2007 г., тем самым доведя до 600 число компаний-поставщиков, использующих эту технологию совместно с Wal-Mart. («Wal-Mart Plans to Add RFID to 500 More Stores» («Wal-Mart планирует ввести RFID еще в 500 магазинах»), Extreme RFID, 12 сентября, 2006). В 2003 г. Министерство обороны США объявило о начале политики, требующей от поставщиков использовать RFID-чипы к 2005 г. (U.S. Department of Defense Press release No. 775-03, 23 октября, 2003, http://www/defenselink.mil/releases/2003/nr20031023-0568.html).

мя его прохождения через считывающее устройство – например, во время погрузки или разгрузки. В розничной торговле RFID-чипы должны полностью заменить штрихкоды, поскольку новая технология позволяет присваивать метки на уровне составных элементов[57].

Итак, технология RFID применяется на транспорте для безопасности пассажиров и удобства поездок. Авиакомпании надеются использовать RFID для сокращения расходов и повышения надежности обработки багажа с прогнозируемой экономией в 700 млн долларов США в год[58]. Продемонстрировав рыночную эффективность RFID-чипов при отзыве бракованной продукции, Michelin в 2003 г. приступила к тестированию чипов, встроенных в шины, чтобы заставить производителей автомобилей более прилежно соблюдать американские стандарты для покрышек; с тех пор вся отрасль переняла эту практику[59]. Тем временем автомобильная промышленность приняла коллективное решение внедрить RFID-чипы в автомобили для того, чтобы установленные вдоль дорог датчики могли считывать информацию. Эта инициатива стала ответом на государственные инициативы по снижению дорожно-транспортных происшествий и заторов на дорогах в целях соответствия экологическим стандартам[60]. Многие системы на платных автомагистралях имеют оснащенные RFID электронные контрольно-пропускные пункты, которые позволяют транспорту быстро проезжать мимо, не образуя пробки у КПП. Эти нововведения применяются на ряде мест в Австралии, Канаде, Чили, Франции, на Филиппинах, в Португалии, Сингапуре и США. Системы общественного транспорта в Гонконге, Лондоне, Москве, Нью-Йорке, Париже, Перте, Тайбэе и других городах внедрили проездные билеты с RFID-чипами.

[57] Как уже предсказывалось несколько лет назад, RFID-чипы могли бы убрать очереди у касс, сделав так, что покупатели проходили бы со своими покупками через считывающее устройство, и их чек был бы автоматически подсчитан в момент их выхода из магазина (http://en.wikipedia.org/wiki/rfid – просмотр 6 октября 2006 г.).

[58] Эндрю Прайс (Andrew Price) – менеджер проекта RFID для IATA (Международной ассоциации воздушного транспорта) – выступление на саммите RFID Journals's Aerospace (26–28 сентября 2006 г.).

[59] Данные требования по маркировке шин сформулированы в TREAD Act, принятым Конгрессом США в 2000 г. после событий с шинами Firestone, установленными на Ford Explorers. Дополнительная информация по RFID-чипам в колесах представлена на http://www.rfidjournal.com/article/articleview/2043/2/1 (просмотр 11 октября 2006 г.).

[60] Приняв проект «Dedicated Short Range Communications», международная автомобильная промышленность дала согласие на коротко- и средневолновой беспроводной протокол, созданный специально для использования в автомобилях (http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm – информация Министерства транспорта США, http://www.ictsb.org/ITSSG/Documents/Mandate_M270.pdf – обзор мандата Еврокомиссии в области оперативного управления движением автотранспорта («Road Transport Telematics») (Мандат 270, опубликован 24 апреля 1998 г. Канцелярией генерального директора III).

RFID-чипы также используются в предметах, которые люди носят на себе или с собой, и они позволяют отслеживать перемещение конкретных людей или проверять их личность. Несколько корпораций приступили к внедрению RFID-чипов в форменную одежду сотрудников или служебные бейджи, что позволяет работодателю в любой момент знать, где находится его сотрудник, или ограничить доступ в определенные сектора здания[61]. В 2005 г. Cisco стала продавать RFID-серверы, работающие с RFID-чипами, вставленными в форменную одежду для определения местонахождения сотрудника[62]. В целях иммиграционного контроля многие страны внедряют RFID-чипы в паспорта для выполнения требований ICAO по бесконтактным машиночитаемым проездным документам. (См. соответствующую дискуссию в примере по биометрии.)[63]

RFID-чипы применялись также в области здравоохранения: в 2003 г. они были встроены в персональные бейджи в двух больницах Сингапура[64], чтобы знать, кто с кем контактировал, и помочь таким образом избежать распространения атипичной пневмонии. Информация хранилась в течение 21 дня (инкубационный период для этого заболевания составляет 10 дней), а затем стиралась для сохранения конфиденциальности[65].

RFID-чипы вживляют и в людей. На сегодняшний день эти устройства по размеру соответствуют зернышку риса и могут работать до 20 лет[66]. В области здравоохранения пациентам могут вживлять чипы, где хранятся их медицинские

61 Это применение технологии началось еще в 1989 г., когда Olivetti Research внедрил Roy Want's Active Badge. Использование этих бейджей оказалось непрактичным до начала широкого использования Интернет в промышленно развитых странах.

62 «Cisco slammed for RFID staff tracker» («Cisco подверглась критике за RFID – слежку за сотрудниками»), Iain Thomson, Vnunet.com, 4 мая 2005 г. (http://www/vnunet.com/vnunet/news/2127277/cisco-slammed-rfid-staff-tracker (просмотр 3 октября 2006 г.).

63 Малайзия выпустила первые снабженные RFID-чипами паспорта в 1998 г. (http://www/wikipedia.org) – просмотр 6 октября 2006 г. На конференции «Computers, Freedom and Privacy» («Компьютеры, свобода и прайвеси») в июне 2005 г. были продемонстрированы способы взлома технологии RFID, установить которую планировал Госдепартамент США. Вскоре после этого события приостанавливается план выдачи паспортов с RFID-чипами; после очевидно ошибочно осуществленного кодирования Госдепартамент США выпустил в марте 2006 г. первую партию этих документов с RFID-чипами в качестве пилотного проекта. См. Marc Perton «US Issues First RFID Passports» («США выпускают первые паспорта с RFID-чипами»), Engadget, http://www.engadget.com/2006/03/13us-issues-first-rfid-passports/.

64 В пилотном проекте принимали участие Alexandra Hospital и National University Hospital.

65 «Singapore Fights SARS with RFID» («Сингапур борется с атипичной пневмонией с помощью RFID»), RFID Journal, 4 июня, 2003, http://www.rfidjournal.com/article/article-view/446/1/1 – просмотр 23 октября 2006 г.

66 «I've got you under my skin» («Ты у меня под кожей»), The Guardian, Technology section, 10 июня, 2004, http://technology.guardian.co.uk/online/story/0,3605,1234827,00.html (просмотр 11 октября 2006 г.).

данные – таким образом эту информацию можно легко считать и связать с конкретным индивидом, особенно если он сам не в состоянии ее сообщить[67]. Имплантаты могут также быть использованы на рабочих местах: ряд работодателей применял их, чтобы не допустить проход сотрудника на сверхсекретные объекты. В 2004 г. имплантант поставили нескольким сотрудникам Министерства юстиции Мексики в целях запрета доступа на определенные объекты и в качестве средства слежения на случай их похищения[68]. Может быть, в попытке проверить реакцию общества на вживление первых имплантатов в людей один ночной клуб предложил эти устройства своим VIP-клиентам в Барселоне и Роттердаме для упрощения идентификации и оплаты напитков[69]. Вживляемые в человека чипы позиционируются на рынке как средства иммиграционного контроля, и генеральный директор одной ведущей компании так рекламировал этот товар: «Это то же самое, что не поддающийся разрушению паспорт, который вы можете всегда носить с собой». И еще он добавил: «что же касается поддельных документов, то технология VeriChip обеспечивает безопасность и прайвеси человека, а также большую безопасность наших границ…»[70]

Имплантанты RFID также хорошо сочетаются с другими технологиями. Например, RFID с биотермическими датчиками может измерять температуру у животных. Эта технология была предложена как способ мониторинга и борьбы с распространением вируса птичьего гриппа H5N1[71]. В рамках совместной пилотной программы организации Digital Angel Corporation[72] и Brazilian

67 Корпорация VeriChip позиционирует свои имплантанты VeriMed как устройства, позволяющие идентифицировать пациентов и их медицинские карты. См. http://www.verimedinfo.com/content/intro/patients (просмотр 3 октября 2006 г.).

68 http://www/verichipcorp.com/images/GSN_Mar06.pdf.

69 См. раздел «VIP» на веб-сайте Baha Beach Club в Барселоне, http://www/bajabeach.es/ (просмотр 11 октября 2006 г.).

70 «VeriChip Highlights Role Implanted Chip May Play in a Government Immigration and Guest Worker Program» («VeriChip рассказывает о роли вживленного чипа в государственном регулировании иммиграции и программе приема гастарбайтеров»), U.S. Newswire, 9 июня, 2006, http://releases.usnewswire.com/GetRelease.amsp?id=67264 (просмотр 16 июня 2006 г.).

71 Ephraim Schwartz, «RFID tags for chickens? Digital Angel says tracking temperature of poultry could be early warning system for avian flu» («RFID-чипы для кур? «Цифровой Ангел» говорит, что контроль температуры домашних птиц может быть ранним предупреждением птичьего гриппа»), InfoWorld, 5 декабря 2005 г. (http://www/infoworld.com/products/print_friendly.jsp?link=/article/05/12/05/HNchickenflu_1.html), просмотр 11 октября 2006 г.

72 Digital Angel Corporation – корпорация с мажоритарным пакетом акций у Applied Digital Inc., которая является также родительской компанией VeriChip Corporation. Среди дочерних компаний – Signature Industries – ведущий разработчик и производитель оборудования GPS для поиска и спасения (торговая марка SARBE), которое принято на вооружение армиями многих стран.

Agriculture Research Corporation (Embrapa) осуществляли вживление биотермических RFID-чипов в домашний скот для предотвращения распространения ящура. Опубликованный компанией пресс-релиз гласил: «При сканировании RFID-сканером и использовании в сочетании с программой базы данных биотермический чип может помимо измерения температуры предоставить мгновенный доступ к специальной информации, такой как принадлежность животного, его возраст, медицинская история (если имеется) и контакты с другими животными»[73].

Помимо этого, реагирующие на движение RFID-чипы используются для мониторинга уровней активности и привычных движений пожилых людей и людей с хроническими заболеваниями. Журналы с данными о движениях людей могут использоваться для создания картины привычек людей, сигнализировать, если эти привычки меняются (например, если человек прекращает принимать пищу, лекарства или перестает вставать с постели)[74].

Для слабовидящих и слепых людей компания En-Vision America разработала умные этикетки с RFID-чипами, которые работают с устройствами считывания, использующими технологию синтеза речи. В чип занесена информация с этикетки продукта, и эта информация произносится вслух в момент считывания ее ридером. Такие «интеллектуальные» этикетки могут использоваться на рецептах: аптеки могут прикреплять их к лекарствам, чтобы пациент, используя ридер, получал озвученную информацию, которая содержится на этикетке, например, свое имя, наименование препарата, тип препарата, рекомендуемую дозировку, противопоказания, общие инструкции по применению, номер рецепта, контактную информацию врача[75].

Эти сферы применения могут создать впечатление, что технология RFID – просто сегмент рынка; однако она получила широкое распространение. Еще в начале 2006 г. было зарегистрировано использование нескольких сотен миллионов RFID-чипов в упаковке продуктов питания, и более 70 миллионов чипов постоянно использовались для маркировки животных[76]. Последние оптовые цены на пассивные RFID-чи-

[73] http://digitalangelcorp.com/about_pressreleases.asp?RELEASE_ID=217 для пресс-релиза корпорации Digital Angel от 25 апреля 2006 г., объявляющего о заключении соглашения с правительством Бразилии.

[74] Pacific Health Summit's Health and Information Technology and Policy Briefing Book, Health Information Technology and Policy Workshop, июнь 2006, стр. 6.

[75] http://www/envisionamerica.com/scriptalk.htm (просмотр 3 октября 2006 г.).

[76] «Food and Livestock RFID – Where, Why, What Next?» («Продукты питания и домашний скот с RFID – где, зачем и что дальше?»), IDTechEx, 10 февраля 2006 г. (http://www.idtechex.com/products/en/articles/00000434.asp), просмотр 11 октября 2006 г.

пы составляли примерно 0,7 доллара США. Тем временем ряд компаний занялся разработкой новых форм, которые можно будет прямо печатать на бумаге, антеннах и других предметах[77]. Учитывая такое широкое использование RFID-чипов, специалисты предсказывают, что к 2010 году ежегодно в обращении будут находиться более 500 миллиардов RFID-чипов[78].

Принцип работы RFID

RFID-устройство может быть встроенным или иметь вид небольшой «бирки» с уникальным электронным номером и возможностью хранить дополнительную информацию. Устройство снабжено ретранслятором и цифровым чипом (микросхемой) памяти. Устройство работает вместе с отдельной антенной-считывателем или ридером, снабженным приемопередатчиком и декодером; ридер излучает сигнал, который активизирует RFID-устройство, и оно может переслать на устройство данные, зашифрованные в ее чипе. В отличие от штрих-кодов, которые повсеместно используются на товарах, RFID-чипы не требуют, чтобы ридер находился в зоне прямой видимости. Как уже было предложено выше, чип может использоваться в качестве этикетки или может быть встроен[79].

RFID-чипы делятся на 3 категории: пассивные, полуактивные и активные. Пассивные чипы не имеют встроенного источника питания; даже слабый электрический ток, создаваемый в антенне входящим радиосигналом, дает достаточно энергии для того, чтобы активизировать чип и позволить ему передать ответ. Другими словами, антенна питается и предает ответный сигнал от входящего сигнала. Пассивные RFID-чипы могут настолько малы, что их практически не видно. Например, к

[77] Такие компании, как PolyIC и Philips разрабатывают чипы из полимерных полупроводников, которые, в случае их коммерческого производства, можно будет печатать. Они будут также намного дешевле кремниевых чипов. См. «Philips Demos Polymer HF Tags» («Philips демонстрирует полимерные ВЧ чипы»), Mary Catherine O'Connor, RFID Journal, 7 февраля, 2006; http://www.rfidjournal.com/article/articleprint/2139/-1/1; просмотр 11 октября 2006 г.

[78] Loring Wirbel, «RFID tags ubiquitous by 2010, MIT prof predicts» (К 2010 году RFID-чипы будут использоваться повсеместно – предсказывает профессор МТИ»), My-ESM, 15 сентября, 2004. Были опасения, что дискуссии о порядке лицензирования и об интеллектуальном праве замедлят распространение RFID-технологии. Компания Intermec является держателем ряда патентов на RFID, в то время как промышленная ассоциация EPCglobal разработала стандарт «UHF Class 1 Generation 2» (2-е поколение, Gen-2). Было решено, что Gen-2 не будет нарушать патенты Intermec, но может возникнуть необходимость выплаты роялти в пользу Intermec в зависимости от способа считывания чипа. См. Mark Roberti, «EPCglobal Ratifies Gen 2 Standard» (EPCglobal ратифицирует стандарт Gen-2), RFID Journal, 16 декабря, 2004, http://www.rfidjournal.com/article/articleview/1293/1/1 (просмотр 11 октября 2006 г.).

[79] http://www/glandi.com/epacking/htm.

началу 2006 года, самые маленькие устройства этого типа были размером 0,15 мм x 0,15 мм (без антенны) и тоньше листа бумаги; несмотря на отсутствие внутреннего источника питания, они могут быть считаны ридером, находящимся на расстоянии в несколько метров.

Полуактивный чип, напротив, содержит маленькую батарейку, что исключает необходимость получения энергии от входящего сигнала. Полуактивный чип активизируется только при обнаружении им сигнала[80] от запрашивающего устройства.

Активные RFID-чипы работают по принципу радиомаяка. Имея собственный источник питания, они действуют на более дальние расстояния (до десяти метров) и обладают большей памятью, чем пассивные чипы; кроме того, они могут принимать, запоминать и хранить дополнительную информацию, полученную от внешнего передатчика. В настоящее время самые маленькие активные чипы имеют батарейку со сроком службы до 10 лет, стоят несколько долларов и имеют размер маленькой монеты[81]. (Конечно, через 10 лет такие размеры чипов и антенн, скорее всего, будут казаться просто огромными).

Последствия и задачи

Пока RFID-технологии остаются нейтральными, но их широкомасштабное применение, несомненно, будет иметь разнообразные инфоэтические последствия. Подобно управлению цифровой идентичностью и биометрии технология RFID создает серьезные проблемы для неприкосновенности частной жизни.

Такие вопросы возникают даже в том случае, когда технология используется только для маркировки потребительских товаров. Например, если большая часть покупок человека снабжена RFID и личность человека можно установить (благодаря кредитной карте, которой он оплачивает свои покупки), то становится возможным получение информации о частной жизни этого конкретного лица. Огромные массивы данных со временем накапливаются, позволяя создать детальную картину расходов, совершаемых человеком. Добавьте эти данные к тем, которые говорят о том, куда человек ездит на своей снабженной RFID-чипом машине, и картина получится еще более детальной.

Кэтрин Альбрехт (Katherine Albrecht) – директор группы защиты неприкосновенности частной жизни потребителей Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) – предупреждает, что RFID-чипы на потребительских товарах могут передавать данные даже после покупки, что позво-

[80] http://www/glandi.com/epacking/htm.
[81] Там же.

ляет полиции использовать каждый чип как радиомаяк[82].

Как уже отмечалось выше, действительно, можно установить связь между RFID-чипами и отдельными людьми, вовлеченными в процесс их использования. В настоящее время особую тревогу в связи с использованием RFID-чипов на рабочих местах вызывает вопрос о том, информируют ли компании надлежащим образом свой персонал относительно сбора, использования и хранения данных, полученных с оснащенных RFID-чипами бейджей. Хотя компании обычно говорят, что эти чипы им нужны для контроля над доступом в здания, последние исследования, проведенные корпорацией RAND, позволяют предположить, что компании США используют RFID-данные и для получения информации о местонахождении сотрудников в случае эвакуации, и для расследования краж, и для контроля над соблюдением сотрудниками правил поведения на работе (таких как обеденный и другие перерывы)[83].

Из всех обследованных компаний ни одна не информировала своих сотрудников об этих дополнительных возможностях применения чипов, оставляя их в убеждении, что RFID-чипы использовались исключительно для контроля над доступом. В общем, четких писаных правил на этот счет не существовало, и ни в одной из компаний не было ограничений, связанных со сроком хранения данных; скорее наоборот, они все хранили записи в течение неограниченного времени. Учитывая, что адекватные и справедливые информационные нормы должны предусматривать право сотрудников изучать и корректировать данные записи об их деятельности, авторы исследования проницательно предостерегают, что такое решение может оказаться неэффективным, так как сотруднику будет сложно реконструировать свои действия за определенный день по прошествии некоторого времени. Исследователи делают важный вывод: по мере того, как технологии осуществляют сбор и анализ данных о деятельности людей на все более высоком уровне, нормы практического применения новых информационных технологий нуждаются в пересмотре[84].

В связи с пристальным вниманием Европейского Союза к защите пер-

[82] Лекция Кэтрин Альбрехт в Гарвардском Университете 7 апреля 2006 г. (http://www.nocards.org/.

[83] Edward Balkovich, Tora K. Bikson, and Gordon Bitko, «9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace» («С 9 до 5: Знаете ли вы, что ваш босс знает, где вы? Кейс-стади использования RFID-чипов на рабочих местах»), TR-197-RC, 36 pp. Исследование проводит сравнение практик шести компаний частного сектора с численностью персонала более 1500 человек.

[84] Там же.

сональных данных правительства государств-членов ЕС более подробно проинформировали компании о правилах использования RFID. Так, в Великобритании Информационная комиссия опубликовала примеры передового опыта в своем Кодексе о трудовых отношениях, призывая компании избегать «подавляющих или унизительных» форм мониторинга сотрудников. Национальная комиссия по информатике и праву (Commission nationale de l'informatique et des libertes) во Франции рекомендовала компаниям полностью информировать сотрудников обо всех случаях использования данных, полученных с оснащенных RFID-чипами идентификационных бейджей. Эта организация также рекомендует открывать работникам доступ к их личным делам[85].

Работодатели говорят, что защита и общественная безопасность оправдывают использование RFID-чипов. Однако в дополнение к угрозе для прайвеси сотрудников и личной независимости чипы могут дать работодателям возможность держать своих сотрудников в страхе и лишать возможности пользования своими законными правами, такими как, например, право на коллективные действия в профессиональных союзах. Обнаружив эти обстоятельства, Британский генеральный союз (GMD) заявил в 2006 г., что практика некоторых центров розничной дистрибуции требовать от своих сотрудников ношения RFID-чипов является негуманной. Протестуя против наблюдения за сотрудниками во время перерывов, Union Network International – международная федерация профсоюзов сектора услуг со штаб-квартирой в Женеве (Швейцария) – организовала кампанию против такого использования RFID[86].

Что же касается использования RFID для предотвращения распространения заболеваний, то нам представляется, что система, подобная той, что была использована в Сингапуре во время вспышки атипичной пневмонии в 2006 г., могла бы использоваться более широко в случае пандемии этого заболевания (как, например, во время вспышки заболевания, вызванного мутацией птичьего гриппа). Для отслеживания возможного заражения власти могли бы использовать RFID-чипы в идентификационных карточках в сочетании с RFID-ридерами, установленными у входов в здания[87]. Даже если такие меры весьма целесообразны в деле охраны здоровья населения, защита прайвеси и свободы собраний потребует серьезного внимания к тем

[85] Andrew Bibby, «Invasion of the Privacy Snatchers» («Нашествие похитителей неприкосновенности частной жизни»), Financial Times, 8 января 2006 г.

[86] Там же.

[87] Для получения краткого отчета по новым планам строительных кодов в США см. ниже исследование по геопространственной сети и технологии LBS.

возможностям организации контроля, которые дает эта технология.

В особых случаях ношение RFID-идентификаторов людьми может требоваться по закону, однако для некоторых людей они могут стать практической необходимостью, обеспечивающей полноценное участие в жизни общества. Это может произойти даже если использование RFID не является формально необходимым – примером может служить ситуация с кредитными картами, без которых взрослому населению промышленно-развитых стран сложно совершать разного рода покупки. Если рынок потребовал, чтобы человек имел RFID-идентификатор для участия в коммерческой деятельности, но это условие не было в обязательном порядке утверждено правительством, будет сложно жаловаться на то, что государство нарушает права граждан, требуя участвовать в подобной системе, – если только люди не заявят, что правительство, разрешая рынку диктовать такое требование, нарушило свои обязательства по защите их автономии.

Можно представить, что такое требование будет де-юре или де-факто распространяться на вживляемые в человека имплантанты, и тогда непонятно, будет ли у людей право отказаться от этих мер.[88] Например, биотермические RFID-чипы, использовавшиеся для идентификации зараженных вирусом домашних животных, могут также применяться для помещения людей на карантин в целях ограничения распространения болезнетворных микроорганизмов. Отдельные люди, возможно, будут против такого вмешательства в свой организм (к примеру, по религиозным соображениям), таким образом, могут сложиться условия, когда интересами отдельных людей нужно будет пренебречь в интересах здоровья населения в целом.

Некоторые обозреватели указывают на то, что оказание поддержки инфраструктурам RFID входит в круг интересов национальной безопасности. Как отмечает Дезире Милошевич (Desiree Milosevic), правительства начинают рассматривать эту технологию в свете геополитических интересов, стимулируя тем самым «гонку контроля».

Однако на сегодня существуют более насущные проблемы, связанные с RFID-чипами. Недавно проведенное исследование, связанное с использованием чипов в кредитных карточках, показало, что информация о держателе карты может быть считана небольшим сделанным в

[88] Весной 2006 г. штат Висконсин (США) был в числе первых штатов, принявших закон, запрещающий требовать от человека вживления микрочипа. «Wisconsin Bans Forced Human Chipping» («Висконсин налагает запрет на насильственное вживление чипов в человека»), Free Market News Network, 1 июня, 2006. Многие другие штаты последовали этому примеру.

домашних условиях ридером, собранным из радиодеталей и компьютерных элементов, достать которые не составляет труда. Поскольку такие устройства могут читать чипы даже через бумажник или одежду, факт, что кто-то считает эту информацию, просто пройдя с ридером в местах скопления людей, не может не вызывать беспокойства. И хотя основные организации, выпускающие карты, заявляют, что большинство карт с RFID-чипом имеют достаточную защиту, все использованные в исследовании карты были выпущены недавно, и при этом ни одна из них не оказалась достаточно надежной[89].

RFID-датчики, имплантированные в человеческое тело, также подверглись критике за свою ненадежность. В июле 2006 г. хакеры продемонстрировали, что могут «клонировать» имплантант VeriChip и атрибутировать считанную идентификационную информацию совершенно другому устройству[90].

Если закрыть глаза на эти проблемы, то широкомасштабное использование RFID может способствовать решению самых разных инфоэтических задач. Осуществив революцию в каналах поставок и значительно повысив производительность труда, технология RFID может способствовать повышению качества жизни, большей свободе и безопасности. Основанные на RFID системы идентификации, при условии их надежности, сокращают потребность в других методах обеспечения безопасности, облегчая доступ к транспортным средствам и общественным ресурсам. Имплантированные RFID-чипы облегчают медицинское обследование, обеспечивая мгновенный доступ к точной медицинской информации о человеке. Список преимуществ этой технологии может быть очень длинным.

Несмотря на очевидные недостатки этой технологии, рыночный спрос на нее, тем не менее, велик со сто-

[89] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Ful, Ari Juels, and Tom O'Hare, «Vulnerabilities in First-Generation RFID-enabled Credit Cards» («Недостатки кредитных карточек с RFID-чипами первого поколения»), University of Massachusetts в сотрудничестве с RSA Labs, октябрь 2006. Эта работа стала первой публикацией нового консорциума с участием промышленных и академических работников, проводивших исследование RFID. Исследование финансируется Национальным научным фондом США. http://prisms.cs.umass.edu/%7Ekevinfu/papers/RFID-CC-manuscript.pdf (просмотр 23 октября 2006 г.).

[90] Хакеры – Аннали Ньюитц и Джонатан Вестхьюз – продемонстрировали эти недостатки на конференции HOPE Number Six в Нью-Йорке. Корпорация VeriChip заявила, что должна проверить эту информацию, но отметила, что взлом RFID-чипов – дело достаточно сложное. См. Donald Melanson, «VeriChip's human-implantable RFID chips clonable, sez hackers» («Хакеры говорят, что вживляемые в человека RFID-чипы VeriChip можно клонировать»), Engadget, 24 июля 2006 г. (http://www.engadget.com/2006/07/24/verichips-human-implantable-rfid-chips-clonable-sez-hackers/, просмотр 24 октября 2006 г.).

роны оптовиков и розничных продавцов, которые с ее помощью могут быстро формировать учетные списки. Скоро она будет востребована и покупателями, которые смогут совершать покупки без очередей, просто проходя через сканирующие устройства. Правительства принимают законы, касающиеся использования этой технологии, и стимулируют ее развитие в сфере общественных услуг. Учитывая серьезность соображений, заставляющих компании и органы местного управления использовать технологию радиочастотной идентификации, и слабость аргументов против такого использования, можно предположить, что RFID уже практически обеспечила себе место в информационном обществе ближайшего будущего.

Итак, в определенном смысле RFID-технология представляет собой микрокосм потенциальных возможностей и угроз для ИКТ. При условии продуманного и тщательно контролируемого внедрения эта технология открывает широкие перспективы для кардинального улучшения многих аспектов нашей жизни; если же использовать ее без адекватных мер по охране безопасности, неприкосновенности частной жизни и других свобод, она может привести к ужасающим последствиям.

Датчики

Что такое «датчики»

Датчики – это устройства, обнаруживающие присутствие биологических или химических веществ или физических раздражителей и формирующие соответствующий сигнал.

Датчики делятся на типы в зависимости от того, что они обнаруживают и уровень чего определяют: скорость, звук, объем, направление потока, газ, влажность, наклон, магнитные свойства, свет, кислород, положение, уровень кислотности, давление, расстояние, вращение или температуру[91].

Принцип работы датчиков

Датчики состоят из двух основных частей: сенсорного элемента и преобразователя. Сенсорная часть взаимодействует с окружающим миром и формирует ответ. Затем преобразователь конвертирует этот ответ в количественное выражение, которое можно интерпретировать.[92]

Датчики можно устанавливать на больших расстояниях, и тогда информация об окружающей среде в определенном месте будет определяться

[91] Web Sensor Portal, http://www/sensorportal.com/HTML/Sensor.htm (просмотр 7 ноября 2006 г.).

[92] Sensor Technology Exchange, http://www.sentix.org/info.htm (просмотр 7 ноября 2006 г.).

датчиком, расположенным на некотором расстоянии от объекта (например, на самолете, на космическом корабле, спутнике или корабле)[93]. Дистанционное измерение параметров окружающей среды обычно основано на излучении. Подобные датчики измеряют самые разные явления, такие как тепло, свет (визуальное отображение) и звук.

Датчики можно также устанавливать in situ, т.е. непосредственно в тех местах, где надлежит производить измерения. И хотя результаты замеров многих из таких датчиков можно получить только на месте, датчик способен также передавать информацию и по сети. В этом случае индивидуальный датчик, иногда называемый «pod» (приставка), состоит из нескольких компонентов, а именно:

1. Корпуса с сенсорным элементом и преобразователем.
2. Микроконтроллера с системными протоколами/коммуникационными стандартами, который взаимодействует с сенсорным устройством и осуществляет анализ данных по заданной схеме.
3. Радиоприемника, соединяющего приставку с окружением или сетью.
4. Системы питания, которая представляет собой, как правило, аккумулятор с солнечными панелями, рассчитанный на работу в течение нескольких лет.
5. Чехла, который должен быть легким, прочным, дешевым, легко надеваться, предохранять от воздействия солнечного излучения и воды, а также защищать от животных[94].

Все чаще датчики производят в виде микроэлектромеханических систем – MEMS. Датчики MEMS способны усиливать выходной сигнал, генерируемый сенсором, настраивая сенсор на считывание различных параметров окружающей среды, например, температуры, и выполнять ряд вычислений на основе его показаний. (Так, например, подобный сенсор может контролировать годность скоропортящегося продукта по мере его прохождения по каналу поставок, обеспечивая поддержание нужной температуры).

Недавно была опубликована статья, посвященная способам сокращения размеров беспроводных MEMS до микрометрического уровня – примерно до размера песчинки[95]. (Такие устройства иногда на-

93 http://en.wikipedia.org/wiki/Remote_sensor (просмотр 7 ноября 2006 г.).

94 Kevin A. Delin, Shannon P. Jackson, David W. Johnson, Scott C. Burleigh, Richard R. Woodrow, J. Michael McAuley, James M. Dohm, Felipe Ip, Ty P.A. Ferre, Dale F. Rucker, and Victor R. Baker, «Environmental Studies with the Sensor Web: Principles and Practice» («Исследования окружающей среды с помощью сенсорных сетей: принципы и применение на практике»), Sensors 2005, том 5, 103–117, стр. 106.

95 Michael J. Sailor and Jamie R. Link, «Smart dust: nanostructured devices in a grain of sand» («Умная пыль: нанотехнологии в песчинке»), Chemical Communications, vol. 11, p. 1375, 2005.

зывают «пылинки» или «умная пыль».) Как сообщается, финансирование научно-исследовательских и проектных работ в данной области осуществляет Министерство обороны США.

Противоположным примером могут служить датчики, установленные на крупных спутниках для предоставления веб-контента в форме изображений, которые затем могут быть совмещены с другими веб-сервисами, такими как автомобильные системы навигации, для создания новых полезных моделей в форме мэшапов («mash ups»)[96].

Последствия и задачи

Если датчики сами по себе могут быть нейтральны, сервис, который они предоставляют, и данные, которые они собирают, могут дать повод для беспокойства. Например, сенсоры, использующиеся для мониторинга лесных пожаров, можно незаметно устанавливать с другой стороны стены, чтобы выстроить приблизительную картину действий человека на основании инфракрасного излучения его тела[97].

Даже данные, полученные для явно благих целей, могут оказаться вредными, если их использовать для целей, нарушающих права человека. К примеру, если датчики изначально используются для обнаружения опасных болезней, то впоследствии их данные могут применяться для установления карантинной зоны, которая нарушает права определенного сегмента населения.

Итак, сбор данных и его основная цель могут быть социально приемлемыми, но перспектива побочного использования данных вызывает озабоченность. Например, полученные со спутника снимки, предоставляемые в онлайновом режиме такими сервисами, как Google, привели правительства стран в ужас. И дело вовсе не в том, что Google это сделал, и не в том, что было изображено на снимках, – просто власти задумались о последствиях попадания такой важной и незащищенной информации в руки потенциальных противников[98].

Чтобы решить подобные проблемы и рассмотреть их в целом, полезно взглянуть на датчики в свете инфоэтических задач. Датчики можно рассматривать как ценный вклад в обеспечение права человека на жизнь, свободу и безопасность. Например, многие датчики служат спасательными средствами – среди них датчики присутствия вредных хими-

[96] См. исследование infra по технологии LBS.

[97] Верховный Суд США запретил правоохранительным органам использовать эту форму технологии. См. Kyllov. United States, 533 U.S. 27 (2001), но общего запрета на ее использование другими лицами нет.

[98] См. Katie Hafner and Saritha Rai, «Governments Tremble at Google's Bird's-Eye View» (Правительства трепещут от представленных Google снимков «с высоты птичьего полета»), New York Times, 20 декабря 2005 г.

ческих веществ в воде или датчики слежения за развитием урагана. В целях предотвращения распространения вируса птичьего гриппа компания STMicroelectronics – вторая в Европе компания по производству чипов – и сингапурская компания Veredus Laboratories занялись разработкой лабораторного чипа, способного за один час проанализировать микроскопический образец крови и проверить его на наличие вируса. Вместо того чтобы отсылать образцы крови в лаборатории и в течение недели ждать результатов анализа, с помощью этого чипа можно будет быстро отобразить результаты на компьютерном мониторе в полевых условиях. По прогнозам авторов статьи в Financial Times, каждый одноразовый чип будет стоить не один десяток долларов[99].

Датчики также помогают оптимизировать производство и поставки продуктов питания, энергии и других жизненно важных ресурсов в промышленно развитых странах. В этом смысле их можно рассматривать как средство повышения уровня жизни и, следовательно, реализации права на жизнь, свободу и безопасность.

Что касается прав человека, то одной из самых важных остается проблема неприкосновенности частной жизни (прайвеси). Та информация, которую человек традиционно считает частной, может теперь быть получена датчиками, и человек может находиться в полном неведении относительно существования или присутствия этих датчиков. Данные о человеке, собранные датчиками, могут быть идентифицированы, при этом вряд ли он сможет заметить наблюдение или сделать выбор относительно использования информации; также маловероятно, что он будет иметь к ней доступ или будет уверен в ее надежном сохранении.

Конечно, датчики могут также содействовать соблюдению прайвеси – например, регистрируя нарушение границ частной собственности.

Если полученные датчиками данные используются в судебном заседании, человек может оказаться в крайне невыгодном положении, если попытается опровергнуть достоверность их как улик.

Не нарушает ли это принцип презумпции невиновности, право человека считаться невиновным, пока вина его не доказана?

Использование датчиков также ставит перед нами инфоэтические проблемы, связанные доступом к информации, являющейся общественным достоянием. Существуют разногласия по поводу совместного использования данных, предостав-

[99] Maija Palmer, «STMicro, Veredus plan quick-test bird-flu chip» («STMicro и Veredus планируют создание чипа для быстрого тестирования птичьего гриппа»), Financial Times, 19 января 2006 г.

ляемых сенсорами. Вопрос в том, принадлежат ли права на эти данные кому-то конкретно, или все они относятся к сфере общедоступной информации?

Стандартный интерфейс для работы с данными сенсоров мог бы способствовать их доступности. Информацию можно было бы получать как из центрального хранилища, так и непосредственно с самого датчика, подключенного к информационной сети. Как отмечал Дэвид Кларк (David Clark)[100], ведущий архитектор Интернета начиная с середины 70-х годов, «самым интересным с точки зрения политики является вопрос о том, будет ли существовать открытая инфраструктура для датчиков»[101].

В то время как подобные проблемы обычно рассматриваются с юридической точки зрения, ученые настороженно относятся к вопросам законодательного регулирования, потому что законы быстро устаревают и начинают мешать технологическому прогрессу. В качестве примера можно сказать, что мониторинг окружающей среды считается в целом необходимым для защиты населения от токсичных веществ и патогенных микроорганизмов, которые могут попадать в воздух, почву или воду определенного региона. Сенсорная технология позволяет осуществлять мониторинг дешево, избегая затрат на отправку команды для сбора образцов и последующих расходов, которые могут быть вызваны порчей образцов в результате транспортировки, хранения и лабораторного анализа. Тем не менее, многие стандартные процедуры по-прежнему предписывают собирать образцы для проведения лабораторных анализов вручную[102]. Следовательно, законодательство, регулирующее использование датчиков или любой другой технологии, должно предусматривать достаточную гибкость законодательных и административных процедур для того, чтобы развиваться параллельно с данной технологией.

Несмотря на все трудности, и уполномоченные лица, и специалисты в области технологии не должны избегать проблем, которые может поставить перед ними сенсорная тех-

[100] Кларк работал архитектором Главного протокола Интернет в 1981–1989 гг. В настоящее время – председатель Совета по вычислительной технике и телекоммуникации Национального научно-исследовательского совета США и старший научный сотрудник лаборатории вычислительных систем и искусственного интеллекта MIT.

[101] Интервью с Дэвидом Кларком в MIT, 11 ноября 2005 г.

[102] В обозримом будущем рынок полевых приборов для контроля над состоянием окружающей среды должен расти в среднем на 7% в год. Эта цифра могла бы быть намного больше, если бы закон и культура могли быстрее охватить все технологические изменения. Clifford K. Ho, Alex Robinson, David R. Miller, and Mary J. Davis, «Overview of Sensors and Needs for Environmental Monitoring» («Обзор датчиков и потребностей в мониторинге окружающей среды»), Sensors, 2005, том 5, 4–37, стр. 5, 7.

нология, и должны принимать меры для создания климата, благоприятного для решения этих проблем с позиций этики.

Геопространственная сеть и технология LBS (услуги на базе информации о местоположении)

Что такое «геопространственная сеть»

Если датчики дают нам количественную информацию о реальном мире и превращают ее в данные, которые считываются машинами, то геопространственная сеть преобразует этот процесс, применяя цифровые данные к определенным объектам реального мира. Путем сочетания данных, взятых из разных источников, геопространственные сервисы могут, к примеру, показать вам карту какого-либо города с отмеченными местами расположения ресторанов, сопроводив ее контактной информацией и отзывами.

Что такое «услуги на базе информации о местоположении»

Услуга на базе информации о местоположении (LBS) – следующий шаг на пути развития данной концепции. Она уже не просто предоставляет информацию о какой-то географической точке, а автоматически определяет местоположение пользователя и выдает информацию с учетом этого местоположения. Развивая предыдущий пример, скажем, что пользователь LBS сможет получить информацию обо всех ресторанах на определенном расстоянии от места, где он находится, а также указания о том, как до них добраться из этой точки[103].

Еще важнее то, что LBS может автоматически отследить местоположение человека и предоставить эту информацию другим людям. Подобное наблюдение делает возможным существование таких сервисов, как, например, Dodgeball.com, который уведомляет людей о том, что их друзья или знакомые находятся поблизости. LBS также позволяет автоматически, без действий со стороны водителя, вызвать скорую помощь на место автомобильной аварии. Некоторые родители покупают своим детям сотовые телефоны с LBS, чтобы всегда знать, где дети находятся. Все возможные области применения LBS еще только начинают вырисовываться.

[103] Система OnStar, например, показывает водителям направления движения, определяя местоположение автомашины и соединяя эту информацию с картами улиц и конечным пунктом движения машины – водитель должен знать, где именно он находится, чтобы воспользоваться этой услугой. См. http://www/onstar.com/us_english/jsp/index.jsp (просмотр 15 марта 2006 г.).

Принцип работы геопространственной сети и LBS

Концепция, лежащая в основе геопространственной сети, довольно проста: нужно лишь указать географическое положение, соответствующее определенному набору (виртуальных) данных, и задать механизм совмещения карт реального мира с этими данными. Чтобы показать карту города с отмеченными на ней ресторанами, геопространственой сети нужно лишь собрать адреса разных ресторанов и соединить их с картографической программой, которая поместит каждый ресторан на определенную улицу на карте или на другой форме географического отображения местности.

LBS устанавливает местоположение конкретного человека или машины. На простейшем уровне человек просто сообщает службе о своем местоположении. Есть и другой способ, при котором местоположение человека вычисляется автоматически. При наличии мобильного телефона местоположение человека может быть установлено по ближайшим к телефону вышкам сотовой связи. Для определения расстояния до этого телефона от каждой из вышек используется метод триангуляции. Точность, а, главное, доступность данного метода определения местоположения пользователя может варьироваться в зависимости от плотности сотовых вышек в данном районе. Система определения положения на базе спутниковой связи, такая как Глобальная система навигации и определения положения (GPS)[104], предоставляет альтернативный способ определения местоположения пользователя без привязки к сотовым вышкам (ведь большинство, если не все современные телефоны снабжены GPS-приемниками). Другой новинкой является подключение мобильных телефонов к установленным поблизости центрам Wi-Fi, которые позволяют, например, определить местоположение человека внутри здания.

Разрабатываются планы создания кодов, использующих технологию RFID и LBS-датчики. Как написано на веб-сайте Национального института стандартов и технологий США (NIST), «проект по развитию систем локализации и коммуникации на

[104] Статья в Wikipedia, посвященная GPS (просмотр 5 марта 2006 г.), гласит: «Министерство обороны США разработало систему… и группа спутников управляется 50-м Космическим звеном с базы ВВС Шривер… GPS предоставляется бесплатно для гражданских целей как общественное благо». Тем временем, «Россия имеет в своем распоряжении автономную систему GLONASS (систему глобальной навигации), имеющую, правда, по состоянию на 2004 г., только 12 активных спутников, что ограничивает сферу ее использования. На рассмотрении находятся планы реконструкции GLONASS для полномасштабного использования к 2008 г. Евросоюз разрабатывает Galileo в качестве альтернативы GPS и планирует ввести его в действие в 2010 г. Китай и Франция также заняты разработкой собственных спутниковых навигационных систем». http://en.wikipedia.org/wiki/GPS.

базе RFID-технологии, предназначенных для служб быстрого реагирования, определит возможность использования систем RFID-локализации в сочетании с существующей беспроводной сетью для предоставления службам быстрого реагирования возможностей для точного ориентирования в условиях слабого радиоприема, когда GPS-локализация и связь с внешними коммуникационными системами оказывается ненадежной. Исследование также призвано рассмотреть средства и потенциальные возможности включения критически важной информации о здании и людях в нем в RFID-чипы, установленные в определенных местах, в целях усиления безопасности и эффективности работы служб быстрого реагирования, а также для того, чтобы свести к минимуму зависимость от коммуникации с базами данных за пределами здания»[105].

Описание проекта в данном исследовании отмечает связь между технологиями: «Система… предназначена для использования возможностей технологии RFID-чипов в сочетании с последними достижениями в создании миниатюрных инерциальных датчиков для разработки недорогих систем слежения…»[106]

Другие области применения LBS связаны с использованием RFID-чипов, имплантированных в тело человека. Несмотря на то, что генеральный директор компании VeriChip подчеркивает, что чипы, которые он предлагает использовать в целях иммиграционного контроля, будут пассивными, на веб-сайте компании написано, что она выпускает также имплантируемые чипы, которые можно использовать как радиомаяки[107].

Последствия и задачи

Ассоциируя информацию с определенным географическим положением, данные технологии позволяют человеку пользоваться рядом своих прав. Например, они позволяют человеку быстро идентифицировать и определять местоположение людей в его социальной сети и предоставляют возможности для более широкого социального взаимодействия[108]. Тем самым, можно сказать, что они помогают человеку осуществлять свое право на собрания. Это право может служить для поддержки демократии и свободы в

[105] NIST, Отделение передовых сетевых технологий, http://www/antd.nist.gov/wctg/RFID/RFIDassist.htm, обновлено 03.03.06 и просмотрено 14 марта 2006 г.

[106] Leonard Miller, «Indoor Navigation for First Responders: A Feasibility Study» («Навигация в помещениях для служб быстрого реагирования: ТЭО»), NIST, 10 февраля 2006 г., стр. 7.

[107] Веб-сайт VeriChip: http://www/verichipcorp.com/ (просмотр 22 июня 2006 г.).

[108] См. www.Dodgeball.com (социальная сеть LBS, в которой пользователи отправляют текстовое сообщение на сотовый телефон для указания своего местоположения).

целом, поскольку граждане могут собираться, например, для составления обращения к правительству с призывом уважать их права.

Геопространственная сеть и LBS могут также считаться средствами, содействующими защите здоровья и безопасности людей, поскольку возможность оказания скорой помощи в чрезвычайных ситуациях часто зависит от способности определить местоположение человека. В этом смысле технология позволяет людям полнее использовать свое право на жизнь, свободу и безопасность.

Естественно, что у этой технологии есть и свои отрицательные стороны. С точки зрения неприкосновенности частной жизни людей может беспокоить, что их местоположение находится под наблюдением. Если речь идет о подавляемой малочисленной части населения, наблюдение за местоположением может привести к дискриминации, и знание – стать причиной угнетения. И так же как сервисы определения местоположения могут помочь людям собираться вместе, они могут и помешать им собираться или устраивать собрания, в зависимости от того, кто получил доступ к данным и какие средства они могут применить, чтобы не допустить это собрание. Даже угроза наблюдения за местом сбора может насторожить людей и предотвратить собрание.

Эти противоречивые возможности заставляют задуматься о том, кто же все-таки должен обладать информацией о местоположении человека. Структура нынешней системы LBS позволяет провайдеру этой услуги определять местоположение человека и делиться информацией с другими; однако из этого не следует, что провайдер должен иметь возможность или разрешение устанавливать местоположение человека в любой момент времени или использовать имеющуюся у него информацию по своему усмотрению.

Аналогично мерам защиты, принятым для управления цифровой идентичностью, один из подходов к решению данной проблемы может включать использование доверенных третьих лиц, которые могли бы предоставлять минимум необходимой информации о местоположении человека и делать это таким образом, чтобы информацию нельзя было связать с другими данными. Например, программа может предложить человеку выбрать, когда и кому открывать информацию о своем местонахождении. И все же, у человека может и не быть возможности выбора, когда LBS объединится с датчиками и биометрией (например, технологией распознавания лиц) для определения местонахождения индивидов. Следовательно, машины должны быть запрограммированы на более аккуратную работу с персональными данными.

Что касается других развивающихся технологий, решения, связанные с законодательством и компьютер-

ными кодами, определят, кто будет обладать правом собственности на эту информацию и контролем над ней. При этом должны быть установлены юридические и технологические механизмы защиты, гарантирующие приемлемое для общества (включая малочисленные группы населения) использование информации о местонахождении конкретного человека. Такое комбинированное решение могло бы помочь информационному обществу пожинать плоды технологий, не платя большие инфоэтические «проценты».

Сети с ячеистой структурой

К существующему интернет-контенту могут прибавиться крупные массивы данных, сгенерированных RFID-приборами, датчиками и LBS-устройствами, особенно после того, как стандарты обеспечат им возможность взаимодействия. Для такого огромного объема данных потребуется более обширная коммуникационная сеть, связывающая все технологии воедино. Сети с ячеистой структурой представляются идеальным решением на начальном этапе подобного проекта.

Что представляют собой сети с ячеистой структурой

В ячеистых сетях устройства, активизированные сетью (компьютеры или мобильные телефоны), устанавливают произвольную равноправную связь. Соединение характеризуется как автоматически конфигурируемое, самовосстанавливающееся, масштабируемое, надежное и недорогое[109].

Принцип работы ячеистых сетей

Ячеистые сети работают за счет устройств, определяющих взаимное присутствие и договаривающихся друг с другом о создании сети для передачи сообщений. Вместо того, чтобы проходить через контролируемые из центра хабы, данные, которыми обмениваются в ячеистой сети, проходят по многоканальному специализированному пути, причем каждый пункт или «узел» на этом пути функционирует как маршрутизатор для передачи сообщений на другие ближайшие узлы. Задействованный узел может быть мобильным или фиксированным, проводным или беспроводным.

Основным преимуществом ячеистой сети является ее специализированный характер: ячеистая сеть может формироваться между узлами, не требующими инфраструктуры, и зависит исключительно от возможностей каждого отдельного узла соединяться с другим узлом. Так, например, ячеистая сеть позволит спасательной команде, работающей на месте разлива отравляющих веществ, сформировать соб-

[109] Статья по ячеистым сетям в Wikipedia, http://en/wikipedia.org/wiki/Mesh_network (просмотр 11 марта 2006 г.).

ственную сеть для обмена информацией.

Точно так же ячеистая сеть, использующая радио или другие технологии беспроводной связи, может быть развернута на местности, на которой отсутствует инфраструктура проводной связи из-за особенностей данной местности или по другим причинам. Если сеть должна быть подключена к Интернету, такое соединение можно установить одним дополнительным узлом с соответствующим соединением – хотя чем больше количество узлов с соединением, тем выше надежность и скорость передачи данных. Таким образом, ячеистая сеть может предоставить слаборазвитым регионам некоторое ограниченное число интернет-соединений. Для связи с удаленными районами к сети нужно просто добавлять узлы[110].

Ячеистые сети отличаются способностью предоставлять множество разнообразных маршрутов для передачи данных, и такая избыточность делает эти сети надежными даже в случае выхода из строя какого-либо узла[111]. Несмотря на то, что в бизнесе представление об избыточности неотделимо от неэффективности, в ячеистых сетях ситуация прямо противоположна: (1) узлы сами по себе довольно дешевы; (2) установка их проста (узел определяется автоматически и задействуется сетью), и (3) плотная сеть из беспроводных узлов позволяет осуществлять связь с использованием более слабых сигналов (Lower-powered communication)[112].

Ячеистые сети имеют и другие сферы применения. Датчики могут использовать слабосильные ячеистые сети для отправки прямых сообщений на другие устройства в сети или, например, передавать определенный ответный сигнал в случае обнаружения разлива химических отравляющих веществ. Поскольку ячеистые сети используют метод распределенного управления и сообщения не должны проходить через центральный узел, системы становятся самонаводящимися.

110 В традиционной беспроводной ячеистой сети все устройства работают на одном и том же коммуникационном канале; в более развитой сети это может создать перегрузку и снизить пропускную способность канала. Решить эту проблему можно за счет использования множественных каналов, предотвращающих интерференцию. См. Richard Draves et al., Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks (2004), http://research.microsoft.com/mesh/papers/multiradio.pdf.

111 Этот метод аналогичен методу работы Интернета и других сетей, использующих равноправную маршрутизацию.

112 Сила электромагнитного сигнала обратно пропорциональна квадрату расстояния от источника сигнала. Как следствие, для передачи сигнала на множество коротких расстояний требуется сигнал меньшей силы, чем для прямой передачи на большие расстояния.

Последствия и задачи

Создание сетей с ячеистой структурой – относительно молодая технология, нуждающаяся в стандартизации: в настоящее время существует более 70 конкурирующих схем формирования сетей и коммуникации устройств. Профессиональная ассоциация IEEE проводит политику внедрения стандартов, и это позволяет предположить, что данная проблема будет решена в ближайшем будущем. Как и в случае других технологий, стандарты касательно ячеистых сетей должны устанавливаться открыто – такая политика отвечает общим интересам, так как не позволяет могущественным организациям внедрять стандарты, которые могут привести к их неправомерному лидированию на рынке.

Ячеистые сети потенциально способны разрушить контроль над контентом. В более традиционной интернет-топологии практически весь контент передается через интернет-провайдеров (ISP), которые могут его фильтровать либо в интересах правительства (например, для предотвращения доступа к нелегальному контенту), либо в своих собственных интересах (ограничивая пропускную способность канала для передачи контента от конкурента). Напротив, ячеистая сеть допускает создание обширного пула пользователей, которые соединяются друг с другом в произвольной манере, без обязательного использования ISP или другого центрального хаба. Таким образом, эта технология позволяет пользователям свободно обмениваться информацией – в полном соответствии с правом на свободу слова.

В то же время, сокращая потребность в ISP для установления локальных соединений, ячеистые сети могут концентрировать потенциал в тех ISP, которые обслуживают относительно малое количество узлов, отвечающих за соединение с опорной интернет-сетью. Эти ISP могут иметь и развивать возможность фильтровать контент и манипулировать ситуацией в своих интересах. Более того, любой сбой в коллективном интернет-соединении может иметь последствия для всей группы пользователей ячеистой сети. С учетом этих аспектов ячеистые сети должны сохранить точки множественного соединения с опорной сетью, контролируемые разными организациями с целью предотвращения монопольного поведения.

Дэвид Кларк (David Clark) отмечает: «Ячеистые сети поднимают вопросы политики в области распределения спектра частот, структуры промышленности и пр. Идет в некотором роде классическая борьба, в ходе которой ответственные лица используют закон как преграду для изменений»[113].

[113] Интервью с Дэвидом Кларком в MIT, 11 ноября 2005 г.

Помимо конкуренции особенностью ячеистых сетей является их небезопасность. При отсутствии контрольных пунктов, через которые должны проходить все данные, вредные вирусы могут распространяться по всем компьютерам сетевого сообщества. Опасность такого заражения может сделать более настойчивым требование эффективного управления цифровой идентичностью и другими подобными технологиями, что усиливает инфоэтический аспект.

Технические средства диктуют правила игры

Интервью с Дуэйном Хендриксом[114]

Ключевым фактором, объясняющим интеграцию Интернета в нашу жизнь, является его проникновение во все ее сферы. Там, где Интернета нет, нет и современной жизни; в этом смысле физическая составляющая управления Интернетом приобретает особое значение. Хотя на сегодняшний день Интернет дошел по проводам (медным, коаксиальным, волоконным) до каждого пользователя, многие из его сервисов станут вскоре особо ценными благодаря отсутствию привязки к сети. Интернет превращается в вездесущий элемент современной жизни, а беспроводной доступ станет вскоре таким же естественным, как воздух.

В каком-то смысле беспроводные соединения устанавливать проще, чем их проводные аналоги, поскольку они не нуждаются в физической инфраструктуре: меньше проводов надо прокладывать, меньше землевладельцев убеждать. Но если провод, проложенный в земле, везде одинаков, то беспроводной спектр – везде разный. В таких странах, как США, спектр радиочастот был аккуратно поделен и практически весь контролируется. А в таких странах, как Китай, ситуация прямо противоположная. Политика других государств сочетает оба подхода[115].

Дуэйн Хендрикс – специалист в области спектров частот – считает, что «деление спектра радиочастот на отгороженные стеной охранные зоны – пережиток прошлого. Лицензируя спектр частот, политики внедрили понимание, что спектр – это ограниченный ресурс, доступ к которому должен строго контролироваться или регламентироваться. Технологические изменения, которые начались в начале 50-х годов XX века, показали нам ошибочность подобной точки зрения.

[114] Дуэйн Хендрикс (Dewayne Hendricks) является Генеральным директором Dandin Group.

[115] См. «Focus on Wireless: Special Study on Wireless Spectrum» (Цель: беспроводная связь – специальное исследование беспроводного спектра) – http://www/netdialogue.org/casestudy/ – создан совместно с исследовательским подразделением Microsoft Corporation. В этом кейс-стади изучен спектр 5ГГц и его возможности для международного использования. На этих веб-страницах Net Dialogue представляет информацию об использовании 5ГГц в мире, перспективы законодательного регулирования этого спектра и стандарты, которые могут быть использованы для него в будущем.

Дуэйн отмечает, что с изобретением программного обеспечения и когнитивного радио, а также концепций типа «spectrum underlay» (или overlay), «информационное общество уже может рассматривать спектр радиочастот как динамически распределенный ресурс, доступ к которому определяется потребностями и особенностями устройств, использующих его в конкретный момент времени».

Дуэйн считает, что лучшей иллюстрацией этого феномена является спектр любительских радиочастот, который используется уже в течение почти 100 лет. Все эти годы любительское радио работало на «общедоступной» частоте и никому не вредило – даже наоборот, стимулировало развитие среды, благоприятной для инноваций. Проводя такую параллель, Дуэйн утверждает, что еще более недавнее создание нелицензированных спектров частот показало всем, что получается, когда государство делает общедоступную частоту доступной для бесконечного числа устройств».

Рассуждая о будущем, Дуэйн сказал: «Трудно сказать, куда заведет нас «общедоступный спектр». Если бы всего 3 года назад кто-то предсказал, что крупнейшие индустриальные города мира будут покрыты «облаками» Wi-Fi, никто бы ему не поверил». И, тем не менее, сегодня ситуация именно такова.

В заключение Дуэйн заметил: «Я думаю, что политики имеют более чем достаточно информации, позволяющей им переосмыслить свои позиции в области спектров частот и серьезно подумать над вопросом открытого спектра».

Вычисления на основе Grid-технологий

Сети с ячеистой структурой и другие сетевые технологии делают возможным подключение к Интернету практически бесконечного количества устройств во всем мире. Конечно, многие из этих устройств обладают очень низким уровнем вычислительной мощности и сравнительно небольшим объемом памяти. Для того, чтобы они смогли адекватно функционировать в информационном обществе, им нужно предоставить доступ к дополнительным ресурсам. Такой возможностью обладают Grid-технологии.

Что такое «вычисления на основе Grid-технологий»

Вычисления на основе Grid-технологий позволяют устройствам, подключенным к сети, объединять вы-

[116] http://creativecommons.org/licenses/by/2.0

числительные мощности и совместно использовать емкости для хранения данных, и в результате работать в качестве единого суперкомпьютера. За счет объединения ресурсов машины, соединенные в Grid-систему, могут выполнять вычисления, которые были бы невозможны или заняли бы слишком много времени, если бы использовался один компьютер. Такая компьютерная кооперация позволяет постоянным пользователям выполнять масштабные задачи, такие как моделирование мировой финансовой системы или прогнозирование изменения климата. Машина, подключенная к такой системе, может также получать доступ к данным, которые она не может хранить в собственной памяти из-за их большого объема.

Grid-систему можно организовать так, чтобы она функционировала в качестве утилиты, а вычислительные ресурсы могут при этом предоставляться «по требованию», как предоставляются во всех развитых странах вода и электричество[117].

В виде идеи **вычисления на основе Grid-технологий** существуют уже несколько десятилетий, первые концепции появились в 60-е годы как «совместное использование компьютерного времени». Однако только в последние 5 лет достижения в области компьютерной обработки данных, совершенствование памяти и сетевых решений позволили оценить преимущества этой технологии. С распространением Интернета, широкополосных сетей, а также недорогих и высокопроизводительных компьютеров, использующих открытые стандарты, концепция **вычислений на основе Grid-технологий** получила более широкое признание[118].

Вычисления на основе Grid-технологий позиционируются на рынке как метод повышения компьютерной эффективности. Например, веб-сайт Sun Microsystems среди преимуществ **Grid-технологий** называет их способность «снижать расходы», «сокращать время, необходимое для выхода на рынок», «обеспечивать более высокое качество и поощрять инновации» и просто «делать то, что раньше было невозможно»[119].

Корпорация IBM также утверждает, что использование **вычислений на основе Grid-технологий** выгодно

[117] В 1965 г. разработчики операционной системы Multics (предшественницы Linux) представили проект «вычислительного процесса как утилиты». См. http://gridcafe.web.cern.ch/gridcafe/Gridhistory/history.html (просмотр 7 марта 2006 г.). Термин «Grid-технология» происходит от метафоры, используемой в начале 1990-х гг. для обозначения вычислительных возможностей, которые также просты для доступа, как объединенная электрическая сеть (electric power grid).

[118] Daniel Minoli, A Networking Approach to Grid Computing («Сетевой подход к вычислениям на основе Grid-технологий»), Hoboken, N.J: John Wiley & Sons, Inc. 2005, p. 3.

[119] http://www.sun.com/software/grid/, просмотр 5 марта 2006 г.

компании, так как позволяет ей «быстрее достигать результатов… делает возможным сотрудничество и способствует большей гибкости производства… Помогает эффективно распределять ресурсы в соответствии с изменяющимися потребностями бизнеса… Повышает производительность… Позволяет управлять текущими капитальными инвестициями…». Технологии развиваются под лозунгами «Оптимизация инфраструктуры… облегченный доступ к данным и более продуктивное сотрудничество… Эластичная, легко доступная инфраструктура…»[120].

Oracle рекламирует свои услуги следующим образом: «**Grid-технологии** позволяют вам создать единую IT-инфраструктуру, воспользоваться которой может каждое из ваших производственных подразделений. Программа Oracle 10g ориентирована специально на **вычисления на основе Grid-технологий** и предоставляет услуги более высокого качества, при этом делая производственный процесс гораздо более дешевым» [121].

Принцип работы вычислений на основе Grid-технологий

Как объясняется на веб-сайте GridCafe Европейской организации по ядерным исследованиям (CERN), Grid имеет 5 основных характеристик:

1. **совместное использование глобальных ресурсов;**
2. **безопасность;**
3. **распределение нагрузки;**
4. **независимость от расстояния и**
5. **открытые стандарты**[122].

Можно сказать, что компьютеры, участвующие в вычислениях на основе Grid-технологий, совместно используют вычислительные ресурсы и ресурсы памяти, распределяя их между организациями, расположенными в разных географических регионах на разных доменах. Отдельные компьютеры в сети предоставляют информацию о том, когда они могут предложить свободные вычислительные мощности или память, и устройства, нуждающиеся в этих ресурсах, могут ими воспользоваться. Когда данный процесс запущен, вычислительные потребности определенного пользователя подразделяются на дискретные задачи и распределяются между машинами в сети. Каждая отдельная машина работает над своей задачей и затем отправляет назад результат для рекомбинации его с результатами, полученными от других участников процесса. Как утверждает CERN, «это больше, чем простой обмен

120 http://www-1.ibm.com/grid/about_grid/benefits.shtml, просмотр 5 марта 2006 г.
121 http://www.oracle.com/technology/tech/grid/index.html, просмотр 27 января 2006 г.
122 http://gridcafe.web.cern.ch/gridcafe/challenges/challenges.html, просмотр 5 марта 2006 г.

файлами, это – прямой доступ к удаленному софту, компьютерам и данным. Технология может также предоставить вам доступ и возможность управления удаленными датчиками, телескопами и другими устройствами, которые вам не принадлежат»[123].

Безопасность можно рассматривать как сочетание 4 аспектов: доступа, авторизации, аутентификации и отчетности. Для доступа участники должны определить, какие ресурсы (программы, компьютеры или данные), кем и в какое время будут использоваться, а также что с ними будут делать. Механизм авторизации проверяет, соответствует ли определенная задача установленным условиям совместного использования. В процессе аутентификации проверяется идентичность участника (провайдера ресурса или пользователя). И, наконец, отчетность предполагает выставление счета за пользование ресурсом; этот аспект все больше превращается в проблему, поскольку вычисления на основе Grid-технологий из чисто экспериментальной лабораторной технологии стремительно превращаются в технологию широкого коммерческого использования[124]. Чиновники и технологи усиленно ищут решение этих проблем, и возможно, что оно будет связано с технологиями управления цифровой идентичностью и сертификацией компьютеров.

Равномерность нагрузки в Grid обусловлена необходимостью эффективно распределять ресурсы. Вместо людей, старающихся оптимизировать ресурсы, мириады программ-посредников позволяют машинам «договариваться» друг с другом на рынке вычислительных услуг и ресурсов памяти. При этом одни из них берут на себя роль агентов (рассказывающих о пользователях, данных и ресурсах), а другие – роль брокеров (предоставляющих доступ к этим услугам и взимающих плату за них). Метаданные (данные о данных) позволяют осуществлять такой обмен, указывая «как, когда и кем определенный набор данных был собран, в каком формате они доступны, и в какой точке (или точках) мира они хранятся…»[125] Нельзя не отметить, что развитие вычислений на основе Grid-технологий тесно связано с прогрессом семантической сети и управления цифровой идентичностью.

Независимость от расстояния подразумевает способность обмениваться Grid-ресурсами с компьютерами из самых разных и удаленных друг от друга мест наиболее эффек-

[123] http://gridcafe.web.cern.ch/gridcafe/challenges/challenges.html, просмотр 5 марта 2006 г.

[124] http://gridcafe.web.cern.ch/gridcafe/challenges/challenges/access.html, просмотр 5 марта 2006 г.

[125] http://gridcafe.web.cern.ch/gridcafe/gridatwork/middleware.html, просмотр 6 марта 2006 г.

тивным образом и обрабатывать задания без задержки.

Аналогично Интернету, представляющему собой «сеть сетей», Grid должен стать объединением перекрывающих друг друга Grid-сетей, функционирующих в соответствии со стандартами приложений, которыми они обмениваются. Чтобы решить эту задачу, сотни участников проекта из разных стран мира (компании, научные организации, исследовательские институты и пр.) совместно работали над определением стандартов. Наверное, самым значительным результатом этой работы по стандартизации стало слияние региональных организаций – сторонников внедрения Grid – в Глобальный Grid-форум (Global Grid Forum)[126] в 2001 г. В настоящее время эта группа работает над стандартом «Открытая архитектура Grid-сервисов», который, как ожидается, станет основным стандартом функционирования Grid[127]. В дополнение к этому общему архитектурному стандарту компания Globus Alliance выпустила программный пакет с открытым кодом «Globus Toolkit»[128], чтобы содействовать развитию Grid и совместимых с ним приложений.

Что полностью отсутствует в базовых характеристиках, так это принцип «нейтралитета сети», который гласит, что не должно быть никакой дискриминации по отношению к разным типам информации, курсирующей по сети. Этот принцип считался необходимым в первые десятилетия существования Интернета и был основан на концепции, гласящей, что эффективность и инновации будут развиваться лучше, если сеть будет служить исключительно для передачи информации. Основная идея заключалась в том, чтобы «интеллект находился по обе стороны» (т.е. там, где осуществляется соединение пользователей), но сама сеть при этом должна была оставаться информационно нейтральной, чтобы не создавать препятствий для коммуникации[129]. Однако в последние годы многие компании разработали технологию, способную эффективно различать разные

126 Члены Глобального Grid-форума по состоянию на 2005 г. http://www/gridforum.org, просмотр 5 марта 2006 г.

127 http://www/gridforum.org/documents/GFD.30pdf, просмотр 7 марта 2006 г.

128 Globus Alliance работает над фундаментальными Grid-технологиями для Globus Toolkit. Globus Alliance была создана в 1996 г. как проект Globus на базе Университета Южной Калифорнии и Университета Чикаго (США). Известная сегодня как Globus Alliance, эта группа включает Royal Institute of Technology (Швеция), University of Edinburgh, National Center for Supercomputing Applications (Иллинойс, США) и Univa Corporation (Иллинойс, США). Спонсорами являются различные федеральные агентства США, такие как DARPA, DOE, NASA, NSF, а также коммерческие партнеры – IBM и Microsoft.

129 «End of Arguments in System Design» («Конец спорам по разработке систем»), J.H. Saltzer, D.P. Reed and D.D. Clark, MIT Laboratory for Computer Science, 1984 (http://www.reed.com/Papers/endtoend.pdf, просмотр 22 июня 2006 г.).

типы трафика (голос, видео или текстовые данные). Естественно, эти компании стали выступать за отказ от нейтралитета сети ради улучшения качества услуг.

На международном уровне этот аргумент в пользу качества услуг был эффективно поддержан Международным союзом электросвязи (International Telecommunication Union), который приступил к реализации инициативы по разработке глобальных стандартов для сетей следующего поколения, призванной внедрить эти возможности повсюду в мире. Интересно, что Глобальный Grid-форум и инициативная группа совместно изучают перспективы взаимодополняющего использования данных технологий[130].

Свободное программное обеспечение (Free Software): доступ к информации и знаниям

Георг Греве[131]

Информация и знания всегда были основой развития человека. Они формировали облик общества, помогали строить мир и становились причиной войн. Информация и знания, сосредоточенные в руках нескольких людей, могут поработить целые народы, но мудрое использование знаний может, напротив, принести людям свободу.

Информационно-коммуникационные технологии кардинально изменили правила доступа и к информации, и к знаниям. Оцифровка впервые сделала возможной передачу информации по всей планете в реальном времени, без потерь и практически бесплатно.

Программное обеспечение лежит в основе упомянутых перемен и определяет эволюцию на современном этапе. Программное обеспечение кодирует правила, в соответствии с которыми происходит обмен информацией и ее конвертирование в знания. «Софт» определяет, кто и на каких условиях может это делать – ведь отчасти именно доступ к программному обеспечению и контроль над ним обусловливает сегодня наличие знаний и власти. Вот почему проблемы, связанные с программным обеспечением, являются такими противоречивыми и социально значимыми.

Программное обеспечение, однако, может быть сконфигурировано так, чтобы дать всем пользователям возможность управлять своими компьютерами и предоставить право определять, как им взаимодействовать с другими пользователями в этой новой, виртуальной среде. Чтобы

[130] Так, например, ITU и Global Grid Forum провели совместную встречу в Женеве, Швейцария, в октябре 2006 г. http://www.itu.int/ITU-T/worksem/grid/index.html (просмотр 22 июня 2006 г.).

[131] Георг Греве (Georg Greve) является президентом Европейского фонда свободного ПО (Free Software Foundation Europe).

люди могли в полной мере реализовать это право, программное обеспечение должно предоставлять 4 фундаментальные свободы: свободу неограниченного пользования информацией, независимо от цели; свободу изучать программное обеспечение и принципы его работы; свободу вносить изменения в программное обеспечение для адаптации его в соответствии с потребностями; свободу копировать и распространять программное обеспечение в оригинальной или модифицированной форме.

Правила пользования программным обеспечением, защищенным правом собственности, могут привести к тому, что многие будут зависеть от немногих. Правила свободного «софта» дают равные и независимые возможности всем игрокам, и поэтому всеобщее желание сделать доступ к информации и знаниям открытым для всех, представляется нам вполне естественным[132].

Последствия и задачи

Со временем Grid-технологии могут изменить подход к работе с компьютером. Вместо того чтобы требовать наличия у каждого человека мощного компьютера, эта технология поощряет использование недорогих «неинтеллектуальных терминалов», каждый из которых обладает ресурсами, достаточными лишь для решения рутинных задач и координации коммуникации с центральным вычислительным ресурсом. Такие терминалы, как правило, намного дешевле стандартного компьютера и поэтому являются, в определенном смысле, способом предоставления доступа к вычислительным мощностям даже самым бедным регионам мира (особенно при совместном использовании с ячеистыми сетями).

Такой оптимистический взгляд предполагает, что пользователи, живущие в бедных регионах, смогут получить доступ к объединенному вычислительному ресурсу. Однако в случае, если Grid-вычисления будут осуществляться на коммерческой основе, невозможность оплатить их может исключить жителей многих регионов мира из числа пользователей; если же сделать данный ресурс принципиально некоммерческим по структуре, то субсидирование этой технологии должна будет взять на себя какая-либо организация.

В то время как над проблемой распределения доходов предстоит еще долго работать, теоретически Grid-технология уже сегодня обещает небывалую эффективность. Миллиарды устройств имеют либо незадействованные, избыточные, либо не-

[132] Дополнительная информация по свободному ПО представлена на веб-страницах Free Software Foundation Europe и Проекта GNU (http://www/fsfeurope.org; http://www/gnu.org).

достаточные вычислительные ресурсы, и эта технология позволяет направлять ресурсы туда, где они в данное время необходимы. Так же как в случае с другими потенциально эффективными технологиями, применение Grid-вычислений обещает резко повысить уровень жизни и в результате поддержать право человека на жизнь, свободу и безопасность.

Понятно, что на практике возникнет много проблем касательно отчетности и безопасности системы, которые потребуют решения. Grid-вычисления в рамках одной организации – дело гораздо более простое, чем открытая Grid-система, использующая Интернет.

Масштабная Grid-система также не лишена инфоэтических недостатков. Угроза для безопасности, заложенная в обмене вычислительной мощностью и данными, потребует внедрения системы управления цифровой идентичностью и других соответствующих технологий, что, в свою очередь, выведет на первый план этические проблемы, связанные с данными технологиями. Более того, если аутентификация будет носить централизованный характер или находиться в чьих-то руках, это теоретически может привести к дискриминации отдельных групп пользователей сети.

Также Grid-архитектура подразумевает необходимость различения контента. Технология, которая используется в настоящее время для такого различения, позволит правительствам и интернет-провайдерам проводить «глубокую пакетную проверку», а это значит, что упомянутые структуры смогут контролировать и, вероятно, блокировать отправку определенной информации. Нет сомнений, что это представляет собой угрозу для свободы слова.

Подобные негативные перспективы уравновешивают преимущества, которые дают большая вычислительная мощность, доступность данных и возможность хранения крупных массивов информации, присущие Grid-технологиям.

Как и другие подобные технологии, Grid-вычисления сами по себе нейтральны и могут использоваться для решения разных задач. И сегодня лица, уполномоченные принимать решения, должны найти подходы, минимизирующие негативные инфоэтические последствия, и сориентировать информационное общество на использование Grid-систем в благих целях.

Чтение и библиотеки: два замечания[133]

Дэвид Вайнбергер[134]*, автор блога «Йохо» (Joho the Blog), 6 марта 2006 г.*

Не могу дождаться момента, когда мы перейдем на чтение электронных книг. Поскольку все они будут доступны в Сети, чтение станет процессом социальным. Книжные клубы станут безграничными, глобальными, повсеместными и разнообразными, как сама Сеть.

Только вообразите, что вы, автор, сможете увидеть, какие фрагменты в вашей книге читатели подчеркивают и где они оставляют пометки на полях. Только представьте, что у автора будет возможность им ответить.

Я не могу дождаться этого момента.

***

Если все наши работы будут доступны онлайн, нам понадобится лишь одна библиотека…

Зачем иметь множество библиотек, если мы сможем пройти по нужной ссылке и получить все, что нам нужно? Да, библиотека будет распределенной, а ее разделы будут продублированы в интересах безопасности (все-таки история Александрийской библиотеки кое-чему нас научила), но ведь это – просто техническая деталь.

Когда все наши работы будут оцифрованы, областная библиотека превратится в обыкновенный гиперсписок.

Новейшие вычислительные технологии

Закон Мура гласит, что вычислительная мощность одного чипа будет удваиваться каждые 18 месяцев[135]. Каждый раз, когда нам кажется, что мы приближаемся к пределу этого экспоненциального роста и имеющаяся технология достигла своего «потолка», появляется но-

[133] http://www/hyperorg.com/blogger/mtarchive/reading_and_libraries_two>note.html#comments.

[134] Дэвид Вайнбергер (David Weinberger) – научный сотрудник Центра Беркмана «Интернет и общество» (Berkman Center for Internet and Society) при Гарвардской юридической школе (Harvard Law School).

[135] Wikipedia, Moore'Law, http://en.wikipedia.org/wiki/Moore%27s_Law (просмотр 26 февраля 2006 г.).

вая технология, позволяющая продолжать наращивание компьютерной мощности.

Существует несколько технологий, открывающих новые перспективы для роста вычислительной мощности, невозможного при использовании существующих интегральных схем[136]. В этом разделе мы вкратце расскажем о некоторых из этих технологий и затем проанализируем общий результат их внедрения – наращивание компьютерной мощности.

Нанотрубки и трехмерные вычисления

Все существующие интегральные схемы принципиально двухмерны; по мере усложнения чипов и увеличения числа их субкомпонентов, необходимость работать в двух измерениях с фиксированным количеством уровней межчиповой коммуникации ограничивает рост вычислительной мощности.

Используя при вычислениях три измерения, мы сможем преодолеть это ограничение. Хотя это возможно при использовании кремниевых транзисторов, существуют и другие транзисторы, более подходящие для трехмерного процессора. Нанотрубки – каркасные цилиндрические структуры, состоящие исключительно из атомов углерода – могут стать более приемлемым средством для трехмерных вычислений. Однако эта технология пока не является коммерчески доступной, поскольку производственные технологии, позволяющие интегрировать нанотрубки в готовые схемы, еще не созданы.

Молекулярные и биологические вычисления

Другие технологии, призванные заменить транзисторы, лежащие в основе современных устройств, используют совершенно новые вычислительные элементы. Молекулярные компьютеры используют отдельные молекулы в качестве вычислительных устройств, позволяя представлять данные в виде определенной конфигурации молекул и производить вычисления путем изменения молекулы. Подобным же образом биологические компьютеры используют живые клетки в качестве компьютеров, при этом вычислительные функции клетки определяются ее собственной ДНК-структурой. В настоящее время обе эти технологии находятся на стадии изучения[137].

Оптические и квантовые вычисления

В традиционном компьютере каждый элемент обрабатывает один фрагмент данных в каждый определенный момент времени. Новей-

[136] Ray Kurzweil, «The Singularity Is Near» («Оригинальность уже близка»), раздел 3 (2005).
[137] Там же.

шие технологии могут позволить одному вычислительному элементу одновременно просчитывать множество таких фрагментов.

Оптические вычисления позволяют проводить такую параллельную обработку, кодируя данные в потоке света. При использовании призменной технологии потоки света могут проходить через одно и то же устройство одновременно, не создавая интерференции. Один-единственный оптический вычислительный элемент, который выполняет вычисления, видоизменяя поток света, может, таким образом, обрабатывать несколько элементов данных одновременно.

Квантовые вычисления используют недетерминированную природу частиц для того, чтобы представить каждое из возможных состояний частицы и в результате сгенерировать частицу в определенном состоянии, которое соответствует решению проблемы.

Оптические и квантовые вычисления имеют общий недостаток, связанный с особенностями их функционирования: каждая из этих технологий эффективна только для выполнения однотипных вычислений при обработке большого массива данных. Именно поэтому данные технологии идеально подходят для решения определенных задач, таких как цифровая обработка изображений, где требуется просчитать каждый фрагмент изображения. Что же касается их применения для менее масштабных вычислений, то здесь возникают трудности. Однако внедрение Grid-вычислений может открыть дополнительные возможности для широкого параллельного использования подобных вычислительных технологий.

Последствия и задачи

Несмотря на то, что большинство технологий, описанных в данном разделе, не появится на рынке в ближайшие несколько лет, они представляют собой многообещающие альтернативы существующим методам вычислений. Реализация каждой включает определенные технические проблемы, которые следует решить, чтобы сделать технологию жизнеспособной; однако ни одна из этих проблем не представляется непреодолимой. Таким образом, можно с уверенностью предположить, что хотя бы одна из описанных технологий будет способствовать значительному росту вычислительных взможностей.

В целом, появление этих технологий говорит о том, что информационное общество далеко еще не достигло пределов своего развития. Компьютеры грядущего, несомненно, будут продолжать сокращаться в размерах, становясь все более мощными и все более зависимыми от сети, а стремительный прогресс Интернета, который 15 лет назад воспринимался как любопытная новинка, а теперь стал доминирую-

щей парадигмой современной жизни, дает понять, что информационное общество находится в самом начале своего пути.

Подобный рост вычислительных мощностей может внести значительный вклад в решение инфоэтических задач. Например, мощные компьютеры могли бы выполнять переводы на самые разные языки, помогая объединению людей из разных языковых групп и стимулируя лингвистическое разнообразие. Кроме того, эти ресурсы могли бы сделать коммуникацию более доступной, предоставляя вычислительные ресурсы для Grid-систем и, таким образом, позволяя пользователям недорогих маломощных устройств получать доступ к информации, которая была сгенерирована другими людьми и хранится на других компьютерах.

С другой стороны, новые технологии порождают новые возможности для слежения и контроля. Сегодня подобный шпионаж представляется сравнительно далекой перспективой, однако в будущем такие технологии будут способны анализировать огромные массивы данных, собранных поисковыми машинами, провайдерами, видеокамерами и другими пунктами сбора данных. В связи с этим опять следует подчеркнуть, что слежение может серьезно помешать реализации прав человека. Особенно это касается тех прав, что призваны предотвратить злоупотребление властью, поскольку наблюдение может нарушать право на невмешательство в частную жизнь, а также свободу собраний и мнений.

Эти технологии могут также сильно повлиять на геополитику, т.к. структуры, которые получат к ним доступ раньше других, будут иметь значительное преимущество над остальными. Таким образом, использование технологий может представлять угрозу для права человека на жизнь, свободу, безопасность и т.п.; но оно также может способствовать позитивным переменам, которые приведут к улучшению правовой ситуации.

Чтобы подготовиться к появлению этих технологий, сулящих невероятные перспективы, информационное общество должно уделять больше внимания существующим на сегодняшний день относительно небольшим программам, которым предстоит проложить дорогу к будущим возможностям, и прилагать все усилия к тому, чтобы технологии создавались и использовались с учетом уважения прав человека.

Таблица
Краткий перечень инфоэтических проблем

Технология	Возможные положительные последствия	Возможные отрицательные последствия
Семантическая сеть	• Расширяет доступ к информации. • Может приводить к поляризации и нарушению общественного диалога, хотя эта вероятность считается спорной. • Повышает эффективность (способствует экономическому развитию и, следовательно, повышению уровня жизни, что, по мнению многих людей, непосредственно связано с правом человека на жизнь, свободу и безопасность).	• Может облегчить блокирование доступа к различным типам контента. • Может способствовать тому, что люди не захотят делиться контентом (из-за угрозы для определенного контента или конкуренции со стороны новых участников). • Может поставить людей на один уровень с предметами.
Управление цифровой идентичностью	• Может содействовать защите частной жизни и безопасности. • Может способствовать свободе собраний, помогая людям находить других людей со схожими интересами. • Может способствовать большей экономической эффективности и развитию бесплатных веб-сервисов (т.е. содействовать росту экономики и, следовательно, повышению уровня жизни, который, по существующему мнению, непосредственно связан с правами человека на жизнь, свободу и безопасность).	• Делает возможным сговор между провайдерами идентичности и третьей стороной и составление досье на пользователей. • Может легко превратиться в систему государственного контроля. • Может способствовать дискриминации. • Может поставить людей в зависимость от машин, действующих от их имени как агенты. • Может увеличить угрозу несанкционированного раскрытия или потери защищенной информации.
Биометрия	• Может помочь создать систему отчетности, что, по мнению некоторых, непосредственно связано с правами человека на жизнь, свободу и безопасность. • Может дать государству новые возможности по оказанию услуг населению (напри-	• Применение вместе с технологией управления цифровой идентичностью может стать обязательным условием участия в жизни информационного общества. • Может привести к созданию международной системы централизованного ад-

	мер, ускорить процедуру проверки паспортов в аэропортах). Некоторые считают, что это будет способствовать соблюдению прав человека	министрирования, при этом международные организации не смогут предотвратить злоупотребление властью. • Может создать условия для масштабного наблюдения, нарушая, таким образом, право на невмешательство в частную жизнь, свободу собраний и слова и т. д.
RFID	• Может способствовать эффективной работе каналов поставок (повышая уровень жизни, что, по мнению многих людей, непосредственно связано с правами человека на жизнь, свободу и безопасность). • Может повысить уровень безопасности, увеличивая возможности принуждения к выполнению законов.	• Может влиять на свободу убеждений, если имплантанты будут необходимы для участия в информационном обществе. • Может создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.
Датчики	• Могут использоваться в качестве средств спасения, что напрямую связано с правами человека на жизнь, свободу и безопасность. • Могут оптимизировать производство и распределение (внеся вклад в экономическую эффективность и, следовательно, помогая реализовать права человека на жизнь, свободу и безопасность).	• Могут добавить неясность в ситуацию с информацией, являющейся общественным достоянием, доступом к информации и средствам коммуникации. • Могут стать причиной серьезного беспокойства по поводу государственного суверенитета и безопасности. • Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.
Геопространственная сеть и LBS	• Может помочь людям в осуществлении права на свободу собраний. • Расширяя возможности служб спасения, укрепляют права человека на жизнь, свободу и безопасность.	• Может нарушать право на невмешательство в частную жизнь, давая возможность отслеживать местонахождение. • Может приводить к дискриминации и нарушению права на свободу собраний и слова, давая возможность отслеживать местонахождение.

Сети с ячеистой структурой	• Могут снять ограничения на контент (например, фильтрацию информации и выделение канала). • Могут помочь слабо развитым регионам получить доступ к средствам коммуникации.	• Могут сосредоточить власть в точках соединения опорного Интернета. • Могут привести к внедрению аутентификации, имеющей такие же побочные последствия, как и управление цифровой идентичностью (в особенности в отношении права на невмешательство в частную жизнь).
Grid-технологии	• Могут предоставлять малоимущему населению вычислительные мощности, память для хранения данных и средства поиска информации. • Повышают эффективность работы за счет оптимизации распределения ресурсов.	• Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы. • Могут приводить к дискриминации и другим ограничениям за счет перекрытия доступа.
Новейшие вычислительные технологии	• Рост вычислительной мощности поможет эффективно осуществлять перевод на разные языки и объединять людей. • При использовании вместе с Grid-системами могут расширить возможности доступа к информации.	• Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы. • Могут нарушить геополитический баланс (предоставляя возможность расшифровки секретных сведений).